On the Binary and Boolean Rank of Regular Matrices

Ishay Haviv
The Academic College of Tel Aviv-Yaffo, Tel Aviv, Israel

Michal Parnas
The Academic College of Tel Aviv-Yaffo, Tel Aviv, Israel

──── **Abstract** ────

A $0,1$ matrix is said to be regular if all of its rows and columns have the same number of ones. We prove that for infinitely many integers k, there exists a square regular $0,1$ matrix with binary rank k, such that the Boolean rank of its complement is $k^{\widetilde{\Omega}(\log k)}$. Equivalently, the ones in the matrix can be partitioned into k combinatorial rectangles, whereas the number of rectangles needed for any cover of its zeros is $k^{\widetilde{\Omega}(\log k)}$. This settles, in a strong form, a question of Pullman (Linear Algebra Appl., 1988) and a conjecture of Hefner, Henson, Lundgren, and Maybee (Congr. Numer., 1990). The result can be viewed as a regular analogue of a recent result of Balodis, Ben-David, Göös, Jain, and Kothari (FOCS, 2021), motivated by the clique vs. independent set problem in communication complexity and by the (disproved) Alon-Saks-Seymour conjecture in graph theory. As an application of the produced regular matrices, we obtain regular counterexamples to the Alon-Saks-Seymour conjecture and prove that for infinitely many integers k, there exists a regular graph with biclique partition number k and chromatic number $k^{\widetilde{\Omega}(\log k)}$.

1 Introduction

For a $0,1$ matrix M of dimensions $n \times m$, consider the following three notions of rank.

- The (standard) *rank* of M over $\mathbb{R}$, denoted by $\mathrm{rank}_{\mathbb{R}}(M)$, is the minimal k for which there exist real matrices A and B of dimensions $n \times k$ and $k \times m$ respectively, such that $M = A \cdot B$ where the operations are over $\mathbb{R}$.
- The *binary rank* of M, denoted by $\mathrm{rank}_{\mathrm{bin}}(M)$, is the minimal k for which there exist $0,1$ matrices A and B of dimensions $n \times k$ and $k \times m$ respectively, such that $M = A \cdot B$ where the operations are over $\mathbb{R}$. Equivalently, $\mathrm{rank}_{\mathrm{bin}}(M)$ is the smallest number of monochromatic combinatorial rectangles in a *partition* of the ones in M.
- The *Boolean rank* of M, denoted by $\mathrm{rank}_{\mathbb{B}}(M)$, is the minimal k for which there exist $0,1$ matrices A and B of dimensions $n \times k$ and $k \times m$ respectively, such that $M = A \cdot B$ where the operations are under Boolean arithmetic (namely, $0 + x = x + 0 = x$, $1 + 1 = 1 \cdot 1 = 1$, and $x \cdot 0 = 0 \cdot x = 0$). Equivalently, $\mathrm{rank}_{\mathbb{B}}(M)$ is the smallest number of monochromatic combinatorial rectangles in a *cover* of the ones in M.

Note that every $0,1$ matrix M satisfies $\mathrm{rank}_{\mathrm{bin}}(M) \geq \mathrm{rank}_{\mathbb{R}}(M)$ and $\mathrm{rank}_{\mathrm{bin}}(M) \geq \mathrm{rank}_{\mathbb{B}}(M)$.

The above notions of rank play a central role in the area of communication complexity, introduced in 1979 by Yao [31]. In the communication problem associated with a $0, 1$ matrix M of dimensions $n \times m$, one player holds a row index $i \in [n]$ and another player holds a column index $j \in [m]$, and their goal is to decide whether $M_{i,j} = 1$ while minimizing the worst-case number of communicated bits. For the deterministic setting, the well-known log-rank conjecture of Lovász and Saks [24] suggests that the communication complexity of the problem is polynomially related to $\log_2 \text{rank}_{\mathbb{R}}(M)$ (see, e.g., [25]). For the non-deterministic setting, it is not difficult to see that the minimum number of bits that should be communicated is precisely $\lceil \log_2 \text{rank}_{\mathbb{B}}(M) \rceil$. For the *unambiguous* non-deterministic setting, where each input is required to have at most one accepting computation, the minimum number of bits that should be communicated is precisely $\lceil \log_2 \text{rank}_{\text{bin}}(M) \rceil$.

For a $0, 1$ matrix M, let $\overline{M}$ denote the complement matrix obtained from M by replacing the ones by zeros and the zeros by ones. A result of Yannakakis [30] implies that every $0, 1$ matrix M with $\text{rank}_{\text{bin}}(M) = k$ satisfies

$$\text{rank}_{\mathbb{B}}(\overline{M}) \leq \text{rank}_{\text{bin}}(\overline{M}) \leq k^{O(\log k)}. \tag{1}$$

The challenge of determining the largest possible value of $\text{rank}_{\mathbb{B}}(\overline{M})$ for a $0, 1$ matrix M with $\text{rank}_{\text{bin}}(M) = k$ has attracted intensive attention in the literature, mostly with the equivalent formulation of the clique vs. independent set problem introduced in [30] (see [20, Chapter 4.4]). The first non-trivial bound was given by Huang and Sudakov [19] who provided, building on a construction of Razborov [28], a family of such matrices M satisfying $\text{rank}_{\mathbb{B}}(\overline{M}) \geq \Omega(k^{6/5})$ (see [11] for extended constructions). The constant $6/5$ in the exponent was improved to $3/2$ by Amano [1] and then to 2 by Shigeta and Amano [29]. The first super-polynomial separation was obtained by Göös [13], who provided a family of such matrices M satisfying $\text{rank}_{\mathbb{B}}(\overline{M}) \geq k^{\Omega(\log^{0.128} k)}$. This was then improved in a work of Ben-David, Hatami, and Tal [3] to $\text{rank}_{\mathbb{B}}(\overline{M}) \geq k^{\Omega(\log^{0.22} k)}$. In a recent breakthrough, it was shown by Balodis, Ben-David, Göös, Jain, and Kothari [2] that the bound can be further improved to $\text{rank}_{\mathbb{B}}(\overline{M}) \geq k^{\widetilde{\Omega}(\log k)}$, which matches the upper bound in (1) up to $\log \log k$ factors hidden in the $\widetilde{\Omega}$ notation. Note that the result of [2] strengthens an earlier result of Göös, Pitassi, and Watson [15], who provided a near optimal separation between the binary rank of a $0, 1$ matrix and the deterministic communication complexity of the problem associated with it.

Interestingly, the above problem is closely related to a graph-theoretic problem proposed by Alon, Saks, and Seymour in 1991 (see [21]). For a graph G, let $\chi(G)$ denote its chromatic number, and let $\text{bp}(G)$ denote its biclique partition number, that is, the smallest number of edge-disjoint bicliques (i.e., complete bipartite graphs) needed for a partition of the edge set of G. A classic result of Graham and Pollak [16] asserts that the complete graph K_n on n vertices satisfies $\text{bp}(K_n) = n - 1$. Inspired by this result, Alon, Saks, and Seymour conjectured that every graph G satisfies $\text{bp}(G) \geq \chi(G) - 1$. The conjecture was disproved by Huang and Sudakov in [19], where it was shown that for infinitely many integers k there exists a graph G satisfying $\text{bp}(G) = k$ and $\chi(G) \geq \Omega(k^{6/5})$. These graphs were used there to derive the aforementioned separation between $\text{rank}_{\text{bin}}(M)$ and $\text{rank}_{\mathbb{B}}(\overline{M})$ for $0, 1$ matrices M (see [19, Section 4]). In a work of Bousquet, Lagoutte, and Thomassé [6], the two problems were shown to be essentially equivalent, allowing the authors of [2] to derive, for infinitely many integers k, the existence of a graph G satisfying $\text{bp}(G) = k$ and $\chi(G) \geq k^{\widetilde{\Omega}(\log k)}$. As in the matrix setting, the gap is optimal up to $\log \log k$ factors in the exponent.

A $0, 1$ matrix M is said to be *d-regular* if every row and every column in M has precisely d ones. In 1986, Brualdi, Manber, and Ross [7] proved that for every d-regular $0, 1$ matrix M of dimensions $n \times n$ where $0 < d < n$, the rank of M over the reals is equal to that of

its complement, that is, $\mathrm{rank}_{\mathbb{R}}(M) = \mathrm{rank}_{\mathbb{R}}(\overline{M})$. Following their work, Pullman [27] asked in 1988 whether every such matrix M satisfies $\mathrm{rank}_{\mathrm{bin}}(M) = \mathrm{rank}_{\mathrm{bin}}(\overline{M})$. In 1990, Hefner, Henson, Lundgren, and Maybee [18] conjectured that the answer to this question is negative (see [18, Conjecture 3.2]). The question was asked again in 1995 in a survey by Monson, Pullman, and Rees [26] (see [26, Open problem 7.1]).[1] Note that for the Boolean rank, such a statement does not hold in general. For example, the 1-regular identity matrix I_n satisfies $\mathrm{rank}_{\mathbb{B}}(I_n) = n$ and yet $\mathrm{rank}_{\mathbb{B}}(\overline{I_n}) = (1 + o(1)) \cdot \log_2 n$ (see [12]).

1.1 Our Contribution

The current work aims to determine the largest possible gap between the binary rank of *regular* $0,1$ matrices and the Boolean rank of their complement. Our main result is the following.

▶ **Theorem 1.** *For infinitely many integers k, there exists a square regular $0,1$ matrix M satisfying $\mathrm{rank}_{\mathrm{bin}}(M) = k$ and $\mathrm{rank}_{\mathbb{B}}(\overline{M}) \geq k^{\widetilde{\Omega}(\log k)}$.*

Theorem 1 can be viewed as a regular analogue of the aforementioned result of Balodis et al. [2], showing that their near optimal separation between $\mathrm{rank}_{\mathrm{bin}}(M)$ and $\mathrm{rank}_{\mathbb{B}}(\overline{M})$ can also be attained by regular matrices M. Since every $0,1$ matrix M satisfies $\mathrm{rank}_{\mathrm{bin}}(\overline{M}) \geq \mathrm{rank}_{\mathbb{B}}(\overline{M})$, Theorem 1 settles, in a strong form, the question of Pullman asked in [27, 26] (and the variants of the question mentioned there) and confirms the conjecture of Hefner et al. [18]. We remark that regular matrices M with $\mathrm{rank}_{\mathbb{B}}(\overline{M})$ larger than $\mathrm{rank}_{\mathrm{bin}}(M)$ can also be derived from [19] (see Section 1.2 for details). While these matrices are sufficient to answer the original question of [27, 26], they only achieve a polynomial gap between the quantities.

The proof of Theorem 1 relies on a modification of the construction of [2] to the regular setting. It involves an extension of the query-to-communication lifting theorem in non-deterministic communication complexity proved by Göös, Lovett, Meka, Watson, and Zuckerman [14], as well as a two-source extractor studied by Bouda, Pivoluska, and Plesch [4] and by Kothari, Meka, and Raghavendra [22]. For an overview of the proof, see Section 1.2.

As alluded to before, matrices M with $\mathrm{rank}_{\mathrm{bin}}(M)$ much smaller than $\mathrm{rank}_{\mathbb{B}}(\overline{M})$ are known to imply graphs G with $\mathrm{bp}(G)$ much smaller than $\chi(G)$, and thus yield counterexamples to the Alon-Saks-Seymour conjecture (see [6]). Although the conjecture is false in general, it is of interest to identify classes of graphs that satisfy a polynomial version of the conjecture. In particular, it was asked in [2] whether the chromatic number of perfect graphs is polynomially upper bounded in terms of their biclique partition number (see [30] for a related question; see also [23, 5, 10]). As an application of Theorem 1, we show that this is not the case for the class of regular graphs. Namely, we show that the near optimal separation achieved in [2] between the biclique partition number and the chromatic number can also be attained by regular graphs.

▶ **Theorem 2.** *For infinitely many integers k, there exists a simple regular graph G satisfying $\mathrm{bp}(G) = k$ and $\chi(G) \geq k^{\widetilde{\Omega}(\log k)}$.*

1.2 Overview of Proofs

Our goal is to obtain regular $0,1$ matrices M for which the binary rank of M is much smaller than the Boolean rank of $\overline{M}$. We first observe that a polynomial gap between the two quantities, for a regular matrix, can be derived from a construction of Huang and

---

[1] The question of [27, 18, 26] was originally formulated using the notion of *non-negative integer rank*, which coincides with the binary rank for $0,1$ matrices (see, e.g., [17, Lemma 2.1]).

Sudakov [19]. Indeed, it can be verified that the (simple) graphs G given in [19], which satisfy $\mathrm{bp}(G) = k$ and $\chi(G) \geq \Omega(k^{6/5})$, are regular, hence their adjacency matrices are regular as well. The following simple claim implies that these adjacency matrices achieve a polynomial gap between the binary rank and the Boolean rank of the complement.

▷ **Claim 3.**   For every simple graph G, the adjacency matrix M of G satisfies that $\mathrm{rank}_{\mathrm{bin}}(M) \leq 2 \cdot \mathrm{bp}(G)$ and $\mathrm{rank}_{\mathbb{B}}(\overline{M}) \geq \chi(G)$.

Proof. For a simple graph G on the vertex set $[n]$, put $k = \mathrm{bp}(G)$, and consider the k bipartitions $(A_1, B_1), \ldots, (A_k, B_k)$ of the k edge-disjoint bicliques that form a partition of the edge set of G. Observe that for every $i \in [k]$, the sets $A_i \times B_i$ and $B_i \times A_i$ form combinatorial rectangles of ones in the adjacency matrix M of G, and that these $2k$ rectangles form a partition of the ones in M, hence $\mathrm{rank}_{\mathrm{bin}}(M) \leq 2 \cdot k$.

Next, put $m = \mathrm{rank}_{\mathbb{B}}(\overline{M})$, and let $A_1 \times B_1, \ldots, A_m \times B_m$ be m combinatorial rectangles that form a cover of the ones in $\overline{M}$, i.e., the zeros in M. For every $i \in [m]$, let C_i denote the set of elements $j \in [n]$ satisfying $(j, j) \in A_i \times B_i$. Since G is simple, the elements on the diagonal of M are all zeros, hence the sets C_i for $i \in [m]$ cover all vertices of G. Since $A_i \times B_i$ is a rectangle of zeros in M, it also follows that C_i is an independent set in G. This implies that $m \geq \chi(G)$, and we are done.   ◁

The matrices M that are known to achieve super-polynomial separations between $\mathrm{rank}_{\mathrm{bin}}(M)$ and $\mathrm{rank}_{\mathbb{B}}(\overline{M})$, however, are apparently far from being regular [13, 3, 2]. Their constructions rely on a powerful technique, known as *query-to-communication lifting*, that enables to deduce separation results in communication complexity from separation results in the more approachable area of query complexity. The proofs of the separation results of [13, 3, 2] involve two main steps, as described below.

In the first step, one provides a family of Boolean functions $f : \{0,1\}^n \to \{0,1\}$ with a large gap between two certain measures of Boolean functions, namely, the unambiguous 1-certificate complexity of f and the 0-certificate complexity of f (see Section 2.3). These measures can be viewed as query complexity analogues of the binary rank of a matrix and the Boolean rank of its complement. It is shown in [2] that the gap between the two measures can be nearly quadratic.

In the second step, the separation is "lifted" from query complexity to communication complexity. This is done by considering, for some gadget function $g : \{0,1\}^\ell \times \{0,1\}^\ell \to \{0,1\}$, the communication problem in which two players get inputs from $\{0,1\}^{\ell \cdot n}$ and aim to determine the value of the composed function $f \circ g^n : \{0,1\}^{\ell \cdot n} \times \{0,1\}^{\ell \cdot n} \to \{0,1\}$, defined by $(f \circ g^n)(x,y) = f(g(x_1,y_1), g(x_2,y_2), \ldots, g(x_n,y_n))$ for all $x, y \in \{0,1\}^{\ell \cdot n}$. Here, the vectors $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$ are viewed as concatenations of n blocks of size ℓ. Query-to-communication lifting results typically show that for some gadget g, a gap between certain query complexity measures of f implies a gap between the suitable communication complexity measures of the composed function $f \circ g^n$. For the non-deterministic setting, it is shown in [14] that if the gadget g is the inner product function on vectors of length $\ell = \Theta(\log n)$, then a gap between the unambiguous 1-certificate complexity and the 0-certificate complexity for f implies a gap between the unambiguous non-deterministic communication complexity and the co-non-deterministic communication complexity for $f \circ g^n$ (see also [13, Appendix A]). The analysis uses the fact that the inner product function forms a two-source extractor, as shown by Chor and Goldreich [9].

Let M denote the matrix associated with the communication problem of $f \circ g^n$ for the function f constructed in [2] and the inner product function g. The lifting result of [14] implies that M attains a near optimal separation between $\mathrm{rank}_{\mathrm{bin}}(M)$ and $\mathrm{rank}_{\mathbb{B}}(\overline{M})$. However, it

can be seen that the matrix M is not regular at all. For example, the row and the column of M that correspond to the all-zero vector consist of only ones or only zeros, depending on the value of f on the all-zero vector.

We turn to describe how we obtain regular matrices M with a similar gap between $\mathrm{rank}_{\mathrm{bin}}(M)$ and $\mathrm{rank}_{\mathbb{B}}(\overline{M})$. We first observe that to construct a regular matrix M, it suffices to replace the inner product function in the above construction by a different gadget function g. Specifically, it turns out that if g is unbiased in a strong sense, namely, it is unbiased even while fixing one of its two inputs, then the matrix M associated with $f \circ g^n$ is regular for any function f (see Section 4.1). Hence, to obtain the desired separation on regular matrices, we provide an extension of the query-to-communication lifting theorem of [14] which allows the gadget function g to be not only the inner product function but any low-discrepancy function. We note that such an extension was speculated already in [14, Remark 1] and was actually established for the deterministic and probabilistic settings in a recent work of Chattopadhyay, Filmus, Koroth, Meir, and Pitassi [8]. Building on the approach of [14] and on tools supplied in [8], we prove that such an extension holds for the non-deterministic setting as well (for a precise statement, see Theorem 7). We proceed by showing that a slight variant g of the inner product function, studied in [4] and in [22], is unbiased in the required sense and has low discrepancy. Then, to prove Theorem 1, we apply our generalized query-to-communication lifting theorem to the family of functions f provided in [2] with this gadget g.

Let us mention that our generalized lifting theorem is not essential for the proof of Theorem 1. It turns out that the matrix M obtained using the aforementioned gadget function g has a sub-matrix that corresponds to a composition with the standard inner product function, hence the lower bound on $\mathrm{rank}_{\mathbb{B}}(\overline{M})$ can also be derived from the lifting result of [14]. Yet, the generality of our lifting theorem can be used to obtain a separation between $\mathrm{rank}_{\mathrm{bin}}(M)$ and $\mathrm{rank}_{\mathbb{B}}(\overline{M})$ using various other gadget functions, and we believe that it might find additional applications.

We finally use the regular matrices given in Theorem 1 to provide regular counterexamples for the Alon-Saks-Seymour conjecture and to prove Theorem 2. It is shown in [6] that a matrix M with $\mathrm{rank}_{\mathrm{bin}}(M)$ much smaller than $\mathrm{rank}_{\mathbb{B}}(\overline{M})$ can be transformed into a graph G with $\mathrm{bp}(G)$ much smaller than $\chi(G)$. This transformation, however, does not preserve the regularity. In fact, a natural attempt to produce a regular graph G from a regular matrix M using the approach of [6] results in a graph that is not even simple (because it has loops). Moreover, certain steps of the argument of [6] identify subgraphs of this graph G with a biclique partition number much smaller than the chromatic number, but those subgraphs are not necessarily regular even if G is. We overcome these difficulties by combining the approach of [6] with a couple of additional ideas, and show that any square regular matrix M with a large gap between $\mathrm{rank}_{\mathrm{bin}}(M)$ and $\mathrm{rank}_{\mathbb{B}}(\overline{M})$ can be transformed into a simple regular graph G with a similar gap between $\mathrm{bp}(G)$ and $\chi(G)$ (see Theorem 12).

1.3 Outline

The rest of the paper is organized as follows. In Section 2, we collect several definitions and results needed throughout the paper. In Section 3, we present our generalized query-to-communication lifting theorem in non-deterministic communication complexity. Its proof can be found in the full version of the paper. In Section 4, we present and analyze a certain gadget function, and combine it with the lifting theorem to prove Theorem 1. Finally, in Section 5, we obtain regular graphs that form counterexamples to the Alon-Saks-Seymour conjecture and confirm Theorem 2.

2   Preliminaries

2.1   Non-deterministic Communication Complexity

Let Λ be a finite set, and let $F : \Lambda \times \Lambda \to \{0,1\}$ be a function. In the communication problem associated with F, one player holds an input $x \in \Lambda$ and another player holds an input $y \in \Lambda$, and their goal is to decide whether $F(x,y) = 1$ by a communication protocol that minimizes the worst-case number of communicated bits. The $0,1$ matrix M associated with the function F is the matrix whose rows and columns are indexed by Λ, defined by $M_{x,y} = F(x,y)$ for all $x, y \in \Lambda$. Consider the following three non-deterministic communication complexity measures of a function F.

- The *non-deterministic communication complexity* of F, denoted by $\mathsf{NP}^{\mathsf{cc}}(F)$, is the smallest possible number of communicated bits in a non-deterministic communication protocol for F, that is, a protocol satisfying that $F(x,y) = 1$ if and only if there exists an accepting computation on (x,y). It holds that $\mathsf{NP}^{\mathsf{cc}}(F) = \lceil \log_2 \mathrm{rank}_{\mathbb{B}}(M) \rceil$.
- The *co-non-deterministic communication complexity* of F, denoted by $\mathsf{coNP}^{\mathsf{cc}}(F)$, is the non-deterministic communication complexity of the negation $\neg F$ of F, defined by $(\neg F)(x,y) = 1 - F(x,y)$ for all $x, y \in \Lambda$. It thus holds that $\mathsf{coNP}^{\mathsf{cc}}(F) = \lceil \log_2 \mathrm{rank}_{\mathbb{B}}(\overline{M}) \rceil$.
- A non-deterministic protocol is called *unambiguous* if it satisfies that each input has at most one accepting computation. The smallest possible number of communicated bits in such a protocol for F is referred to as the *unambiguous non-deterministic communication complexity* of F and is denoted by $\mathsf{UP}^{\mathsf{cc}}(F)$. It holds that $\mathsf{UP}^{\mathsf{cc}}(F) = \lceil \log_2 \mathrm{rank}_{\mathrm{bin}}(M) \rceil$.

2.2   Composed Functions

For integers n and ℓ, let $f : \{0,1\}^n \to \{0,1\}$ and $g : \{0,1\}^\ell \times \{0,1\}^\ell \to \{0,1\}$ be two functions. The function $g^n : \{0,1\}^{\ell \cdot n} \times \{0,1\}^{\ell \cdot n} \to \{0,1\}^n$ is defined by

$$g^n(x,y) = (g(x_1, y_1), g(x_2, y_2), \ldots, g(x_n, y_n))$$

for all $x, y \in \{0,1\}^{\ell \cdot n}$, where the vectors $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$ are viewed as concatenations of n blocks of size ℓ. The *composed function* $f \circ g^n : \{0,1\}^{\ell \cdot n} \times \{0,1\}^{\ell \cdot n} \to \{0,1\}$ is defined by $(f \circ g^n)(x,y) = f(g^n(x,y))$. For a set $I \subseteq [n]$ and a vector $x \in \{0,1\}^{\ell \cdot n}$, we let $x_I \in \{0,1\}^{\ell \cdot |I|}$ denote the projection of x to the blocks whose indices are in I. Note that when $I = \{i\}$ for some $i \in [n]$, we have $x_i = x_I$. For vectors $x, y \in \{0,1\}^{\ell \cdot n}$, we let $g^I(x_I, y_I)$ denote the projection of $g^n(x,y)$ to the indices of I.

2.3   Certificate Complexity

An n-variate *k-DNF* formula φ is a Boolean formula on n variables that can be written as a disjunction $\varphi = c_1 \vee \cdots \vee c_m$, where every c_i is a conjunction of at most k literals. The formula φ is said to be *unambiguous* if for every input $x \in \{0,1\}^n$ there is at most one $i \in [m]$ that satisfies $c_i(x) = 1$. For a Boolean function $f : \{0,1\}^n \to \{0,1\}$, consider the following query complexity measures.

- The 1-*certificate complexity* of f, denoted by $\mathsf{C}_1(f)$, is the smallest integer k for which f can be written as a k-DNF formula.
- The 0-*certificate complexity* of f, denoted by $\mathsf{C}_0(f)$, is $\mathsf{C}_1(\neg f)$, where $\neg f$ is the negation of f. Equivalently, $\mathsf{C}_0(f)$ is the smallest integer k for which f can be written as a k-CNF formula.
- The *unambiguous* 1-*certificate complexity* of f, denoted by $\mathsf{UC}_1(f)$, is the smallest integer k for which f can be written as an unambiguous k-DNF formula.

We need the following result that was proved in [2].

▶ **Theorem 4** ([2]). *For infinitely many integers r, there exists a Boolean function $f :$ $\{0,1\}^n \rightarrow \{0,1\}$ satisfying $\mathsf{UC}_1(f) = r$ and $\mathsf{C}_0(f) \geq \widetilde{\Omega}(r^2)$ where $r = n^{\Omega(1)}$.*

2.4 Discrepancy

▶ **Definition 5** (Discrepancy). *Let Λ be a finite set, let $g : \Lambda \times \Lambda \rightarrow \{0,1\}$ be a function, and let X, Y be independent random variables that are uniformly distributed over Λ. The* discrepancy *of g with respect to a combinatorial rectangle $R \subseteq \Lambda \times \Lambda$ is denoted by $\mathrm{disc}_R(g)$ and is defined by*

$$\mathrm{disc}_R(g) = \Big| \Pr\left[g(X,Y) = 0 \text{ and } (X,Y) \in R\right] - \Pr\left[g(X,Y) = 1 \text{ and } (X,Y) \in R\right] \Big|.$$

The discrepancy *of g, denoted by $\mathrm{disc}(g)$, is defined as the maximum of $\mathrm{disc}_R(g)$ over all combinatorial rectangles $R \subseteq \Lambda \times \Lambda$.*

3 Lifting from Certificate to Communication Complexity

In this section, we present our extension of the query-to-communication lifting theorem in non-deterministic communication complexity to general low-discrepancy functions. We start with a simple upper bound on the unambiguous non-deterministic communication complexity of a composed function.

▶ **Lemma 6.** *For all functions $f : \{0,1\}^n \rightarrow \{0,1\}$ and $g : \{0,1\}^\ell \times \{0,1\}^\ell \rightarrow \{0,1\}$, it holds that $\mathsf{UP}^{\mathsf{cc}}(f \circ g^n) \leq O\big(\mathsf{UC}_1(f) \cdot \max(\log_2 n, \ell)\big)$.*

Proof. Put $k = \mathsf{UC}_1(f)$. Then, the function f can be written as an unambiguous n-variate k-DNF formula $\varphi = c_1 \vee \cdots \vee c_m$ where $m \leq (2n)^k$. Consider the following non-deterministic protocol for the communication problem associated with the function $f \circ g^n$. Let $x, y \in \{0,1\}^{\ell \cdot n}$ be the inputs of the players. The first player selects non-deterministically an index $i \in [m]$ and sends it to the other player. Let $I \subseteq [n]$ denote the set of indices of the variables that appear in the clause c_i, and note that $|I| \leq k$. Then, the first player sends the projection x_I of x to the blocks of I, and similarly, the second player sends the projection y_I of y to the blocks of I. The players accept if and only if $c_i(g^I(x_I, y_I)) = 1$.

Observe that $(f \circ g^n)(x,y) = 1$ if and only if the protocol has an accepting computation on the inputs x, y. Observe further that the fact that φ is unambiguous implies that the protocol is unambiguous as well. Finally, the number of bits communicated by the protocol is $O(\log_2 m + k \cdot \ell) \leq O\big(k \cdot \max(\log_2 n, \ell)\big)$, completing the proof. ◀

We turn to state a lower bound on the co-non-deterministic communication complexity of composed functions $f \circ g^n$ for low-discrepancy functions g. Its proof can be found in the full version of the paper.

▶ **Theorem 7.** *For every $\eta > 0$ there exists $c > 0$ for which the following holds. Let ℓ and n be integers such that $\ell \geq c \cdot \log_2 n$, and let $g : \{0,1\}^\ell \times \{0,1\}^\ell \rightarrow \{0,1\}$ be a function satisfying $\mathrm{disc}(g) \leq 2^{-\eta \cdot \ell}$. Then, for every function $f : \{0,1\}^n \rightarrow \{0,1\}$, it holds that*

$$\mathsf{coNP}^{\mathsf{cc}}(f \circ g^n) \geq \Omega\big(\eta \cdot \mathsf{C}_0(f) \cdot \ell\big).$$

   The Binary and Boolean Rank of Regular Matrices

In what follows we consider the notion of strongly unbiased functions and show that compositions with such functions are associated with regular matrices. We then present a strongly unbiased function and analyze its discrepancy. Equipped with this function, we apply the lifting theorem from the previous section to prove Theorem 1.

4.1   Strongly Unbiased Functions

Consider the following definition.

▶ **Definition 8.** *Let ℓ be an integer. We call a function $g : \{0,1\}^\ell \times \{0,1\}^\ell \to \{0,1\}$ strongly unbiased if for every vector $x \in \{0,1\}^\ell$, the number of vectors $y \in \{0,1\}^\ell$ satisfying $g(x,y) = 1$ is $2^{\ell-1}$, and for every vector $y \in \{0,1\}^\ell$, the number of vectors $x \in \{0,1\}^\ell$ satisfying $g(x,y) = 1$ is $2^{\ell-1}$. Equivalently, g is strongly unbiased if the matrix associated with g is $2^{\ell-1}$-regular.*

The following lemma shows that compositions with strongly unbiased functions are associated with regular matrices.

▶ **Lemma 9.** *For all functions $g : \{0,1\}^\ell \times \{0,1\}^\ell \to \{0,1\}$ and $f : \{0,1\}^n \to \{0,1\}$, if g is strongly unbiased then the matrix associated with the composed function $f \circ g^n$ is regular.*

Proof. Let $g : \{0,1\}^\ell \times \{0,1\}^\ell \to \{0,1\}$ be a strongly unbiased function, let $f : \{0,1\}^n \to \{0,1\}$ be a function, and let M be the matrix of dimensions $2^{\ell \cdot n} \times 2^{\ell \cdot n}$ associated with the composed function $f \circ g^n$. Since g is strongly unbiased, it follows that for every vector $x \in \{0,1\}^{\ell \cdot n}$ and for every vector $a \in \{0,1\}^n$, precisely 2^{-n} fraction of the vectors $y \in \{0,1\}^{\ell \cdot n}$ satisfy $g^n(x,y) = a$. This implies that the row of the matrix M that corresponds to a vector $x \in \{0,1\}^{\ell \cdot n}$ consists of the evaluations of the function f on all vectors $a \in \{0,1\}^n$, where each such evaluation appears exactly $2^{-n} \cdot 2^{\ell \cdot n} = 2^{(\ell-1)n}$ times. In particular, the number of ones in this row is $2^{(\ell-1)n} \cdot |f^{-1}(1)|$. Since this number is independent of x, it follows that this is the number of ones in each row of the matrix M. By symmetry, this is also the number of ones in each column of M, implying that the matrix M is regular.   ◀

4.2   The Gadget Function

For an integer $\ell \geq 1$, define the function $g_\ell : \{0,1\}^\ell \times \{0,1\}^\ell \to \{0,1\}$ by

$$g_\ell(x,y) = x_1 + y_1 + \sum_{i=2}^{\ell} x_i \cdot y_i \pmod 2$$

for all $x,y \in \{0,1\}^\ell$. We first observe that g_ℓ is strongly unbiased.

▶ **Lemma 10.** *For every integer $\ell \geq 1$, the function g_ℓ is strongly unbiased.*

Proof. Consider the function g_ℓ for an integer $\ell \geq 1$. By definition, for every $x \in \{0,1\}^\ell$, it holds that for every $y' \in \{0,1\}^{\ell-1}$ exactly one of the two vectors $y \in \{0,1\}^\ell$ with suffix y' satisfies $g(x,y) = 1$. This implies that for every $x \in \{0,1\}^\ell$ precisely $2^{\ell-1}$ of the vectors $y \in \{0,1\}^\ell$ satisfy $g(x,y) = 1$. By symmetry, we also have that for every $y \in \{0,1\}^\ell$ precisely $2^{\ell-1}$ of the vectors $x \in \{0,1\}^\ell$ satisfy $g(x,y) = 1$, so we are done.   ◀

The following lemma claims that the functions g_ℓ have low discrepancy. We note that this can be directly derived from a bound on the discrepancy of the inner product function. Yet, we present in the full version of the paper a bound with a somewhat better multiplicative constant, borrowing an argument of Bouda, Pivoluska, and Plesch [4].

▶ **Lemma 11.** *For every integer $\ell \geq 1$, the discrepancy of the function g_ℓ satisfies*

$$\text{disc}(g_\ell) \leq 2^{-(\ell+1)/2}.$$

4.3 Proof of Theorem 1

We are ready to put everything together and to complete the proof of Theorem 1.

Proof of Theorem 1. By Theorem 4, for infinitely many integers r, there exists a Boolean function $f : \{0,1\}^n \to \{0,1\}$ satisfying $\mathsf{UC}_1(f) = r$ and $\mathsf{C}_0(f) \geq \widetilde{\Omega}(r^2)$ where $r = n^{\Omega(1)}$. For an integer ℓ, consider the function $g_\ell : \{0,1\}^\ell \times \{0,1\}^\ell \to \{0,1\}$ defined in Section 4.2. By Lemma 11, it holds that $\text{disc}(g_\ell) \leq 2^{-\eta \cdot \ell}$ for $\eta = 1/2$. Theorem 7 yields that there exists a constant c, such that for $\ell = \lceil c \cdot \log_2 n \rceil$, the composed function $f \circ g_\ell^n$ satisfies

$$\mathsf{coNP}^{\mathsf{cc}}(f \circ g_\ell^n) \geq \Omega(\mathsf{C}_0(f) \cdot \ell) \geq \widetilde{\Omega}(r^2). \tag{2}$$

By Lemma 6, it further holds that

$$\mathsf{UP}^{\mathsf{cc}}(f \circ g_\ell^n) \leq O(\mathsf{UC}_1(f) \cdot \ell) \leq \widetilde{O}(r), \tag{3}$$

where for the second inequality we have used our choice of ℓ and the fact that $r = n^{\Omega(1)}$.

To complete the proof, let M be the square $2^{\ell \cdot n} \times 2^{\ell \cdot n}$ matrix associated with the composed function $f \circ g_\ell^n$. By Lemma 10, the function g_ℓ is strongly unbiased, hence by Lemma 9, the matrix M is regular. Recalling that $\mathsf{UP}^{\mathsf{cc}}(f \circ g_\ell^n) = \lceil \log_2 \text{rank}_{\text{bin}}(M) \rceil$, it follows from (3) that $\text{rank}_{\text{bin}}(M) \leq 2^{\widetilde{O}(r)}$. Put $k = \text{rank}_{\text{bin}}(M)$, and combine (2) with the fact that $\mathsf{coNP}^{\mathsf{cc}}(f \circ g_\ell^n) = \lceil \log_2 \text{rank}_{\mathbb{B}}(\overline{M}) \rceil$ to obtain that $\text{rank}_{\mathbb{B}}(\overline{M}) \geq 2^{\widetilde{\Omega}(r^2)} \geq k^{\widetilde{\Omega}(\log k)}$. ◀

5 The Alon-Saks-Seymour Conjecture and Regular Graphs

In this section, we prove the following theorem.

▶ **Theorem 12.** *For every square regular $0,1$ matrix M, there exists a simple regular graph G satisfying $\text{bp}(G) \leq 33 \cdot \text{rank}_{\text{bin}}(M)^2$ and $\chi(G) \geq \text{rank}_{\mathbb{B}}(\overline{M})^{1/3}$.*

Applying Theorem 12 to the matrices given by Theorem 1 yields regular graphs that form counterexamples to the Alon-Saks-Seymour conjecture with a near optimal gap between the biclique partition number and the chromatic number. This confirms Theorem 2.

5.1 Biclique Covering

We start with some definitions that will be used throughout the proof of Theorem 12. All graphs considered here are undirected. They do not contain parallel edges but they may have loops. As usual, a graph is said to be *simple* if it contains no loops and no parallel edges. For a graph $G = (V, E)$, a *biclique of G* is a complete bipartite subgraph of G, that is, a pair (A, B) of sets $A, B \subseteq V$ where every vertex of A is adjacent in G to every vertex of B. For adjacent vertices x, y of G such that $x \in A$ and $y \in B$, we say that the biclique (A, B) covers the oriented edge (x, y). Note that although the edges of G are undirected, a biclique of G covers edges of G with some orientation.

For an integer t, a *t-biclique covering* of G is a collection of bicliques of G that cover every edge of G at least once and at most t times. The minimum size of such a covering is called the *t-biclique covering number of G* and is denoted by $\mathrm{bp}_t(G)$. For $t = 1$, a 1-biclique covering is also called a *biclique partition*, and we write $\mathrm{bp}(G) = \mathrm{bp}_1(G)$.

We need the following result of Bousquet, Lagoutte, and Thomassé [6].

▷ **Claim 13** ([6, Claim 28]). Let $H = (V, E)$ be a simple graph, and let $\mathcal{C}$ be a t-biclique covering of size k of H. Let $E' \subseteq E$ be the set of edges of H that are covered by $\mathcal{C}$ exactly t times. Then, the graph $H' = (V, E')$ satisfies $\mathrm{bp}(H') \leq (2k)^t$.

5.2   From Regular Matrices to Regular Graphs

We are ready to prove Theorem 12.

Proof of Theorem 12. Let M be an $n \times n$ regular $0, 1$ matrix, and let d denote the number of ones in each row and each column of M. Put $k = \mathrm{rank}_{\mathrm{bin}}(M)$ and $m = \mathrm{rank}_{\mathbb{B}}(\overline{M})$.

We first define a graph $H = (V, E)$ on the vertex set $V = [n] \times [n]$ in which every two (not necessarily distinct) vertices $(i_1, j_1), (i_2, j_2) \in V$ are adjacent if $M_{i_1, j_2} = 1$ or $M_{i_2, j_1} = 1$. Define $V_0 = \{(i, j) \in V \mid M_{i,j} = 0\}$ and $V_1 = \{(i, j) \in V \mid M_{i,j} = 1\}$. Note that $V = V_0 \cup V_1$, and notice that the vertices of H that have loops are precisely the vertices of V_1.

Let $H_0 = H[V_0]$ denote the subgraph of H induced on the vertices of V_0. Clearly, H_0 is a simple graph. The following lemma relates its chromatic number to the Boolean rank of $\overline{M}$.

▶ **Lemma 14.** *The graph H_0 satisfies $\chi(H_0) \geq m$.*

Proof. Put $r = \chi(H_0)$. Then, there exists a partition of V_0 into r independent sets $I_1, \ldots, I_r$ of H_0. For each $t \in [r]$, let A_t be the set of elements $i \in [n]$ for which there exists some $j \in [n]$ such that $(i, j) \in I_t$, and let B_t be the set of elements $j \in [n]$ for which there exists some $i \in [n]$ such that $(i, j) \in I_t$. Since I_t is an independent set in H_0, it follows that every pair $(i, j) \in A_t \times B_t$ satisfies $M_{i,j} = 0$. This implies that $A_t \times B_t$ is a combinatorial rectangle of zeros in the matrix M. Since the r given independent sets cover the entire set V_0, it follows that for every pair $(i, j) \in V_0$ there exists some $t \in [r]$ such that $(i, j) \in I_t$, and this t satisfies $(i, j) \in A_t \times B_t$. This shows that the rectangles $A_t \times B_t$ with $t \in [r]$ form a cover of the zeros of M, hence $r \geq \mathrm{rank}_{\mathbb{B}}(\overline{M}) = m$, as required. ◀

The next lemma provides a 2-biclique covering of H.

▶ **Lemma 15.** *There exists a 2-biclique covering $\mathcal{C}$ of H such that*
1. $|\mathcal{C}| = k$,
2. *for every adjacent distinct vertices $(i_1, j_1), (i_2, j_2)$ of H, if both $M_{i_1, j_2} = 1$ and $M_{i_2, j_1} = 1$ hold, then the edge that connects them is covered by $\mathcal{C}$ twice in the two opposite orientations, and if only one of them holds, then it is covered by $\mathcal{C}$ once, and*
3. *every loop of H is covered by $\mathcal{C}$ once.*

Proof. By $k = \mathrm{rank}_{\mathrm{bin}}(M)$, there exists a collection of k combinatorial rectangles $A_t \times B_t$ of ones, $t \in [k]$, that forms a partition of the ones of the matrix M. We define $\mathcal{C}$ as the collection of all bicliques of the form $C_t = (A_t \times [n], [n] \times B_t)$ for $t \in [k]$.

Let $(i_1, j_1), (i_2, j_2)$ be two (not necessarily distinct) vertices of H. If $M_{i_1, j_2} = 1$ then there exists a unique $t \in [k]$ such that $(i_1, j_2) \in A_t \times B_t$. This implies that the oriented edge $((i_1, j_1), (i_2, j_2))$ is covered by the biclique C_t and is not covered by any other biclique of $\mathcal{C}$. If, however, it holds that $M_{i_1, j_2} = 0$, then no $t \in [k]$ satisfies $(i_1, j_2) \in A_t \times B_t$, hence the oriented edge $((i_1, j_1), (i_2, j_2))$ is not covered by any biclique of $\mathcal{C}$.

We turn to show that $\mathcal{C}$ is a 2-biclique covering of H that satisfies the assertion of the lemma. By definition, we have $|\mathcal{C}| = k$, as required for Item 1. Let $(i_1, j_1), (i_2, j_2)$ be two distinct vertices of H. If the vertices are adjacent then $M_{i_1, j_2} = 1$ or $M_{i_2, j_1} = 1$. The above discussion implies that if both the conditions hold then the edge that connects them is covered twice in the two opposite orientations, whereas if only one of the conditions holds, then the edge is covered once, as required for Item 2. For a vertex (i, j) that has a loop, it holds that $M_{i,j} = 1$, hence the oriented edge $((i, j), (i, j))$ is covered once by $\mathcal{C}$, as required for Item 3. On the other hand, if the vertices $(i_1, j_1), (i_2, j_2)$ are not adjacent then $M_{i_1, j_2} = 0$ and $M_{i_2, j_1} = 0$, hence no oriented edge between them is covered by $\mathcal{C}$. It thus follows that $\mathcal{C}$ is a 2-biclique covering of H, and we are done. ◀

Let $\mathcal{C}$ be the 2-biclique covering of H given by Lemma 15. Consider the two subgraphs of H_0 defined by $H_0^{(1)} = (V_0, E_1)$ and $H_0^{(2)} = (V_0, E_2)$, where E_t is the set of edges of H_0 that are covered by $\mathcal{C}$ exactly t times for $t \in [2]$. Since the edge set of H_0 is $E_1 \cup E_2$, it follows that

$$\chi(H_0) \leq \chi(H_0^{(1)}) \cdot \chi(H_0^{(2)}). \tag{4}$$

To obtain the desired simple regular graph, we proceed by considering the following two cases according to the chromatic number of $H_0^{(2)}$.

Case 1. Suppose first that $\chi(H_0^{(2)}) \geq m^{1/3}$. Let $\mathcal{C}'$ be the collection of bicliques of H obtained from $\mathcal{C}$ by replacing every biclique $(A, B) \in \mathcal{C}$ by the three bicliques $(A \cap B, A \cap B)$, $(A \cap B, B \setminus A)$, and $(A \setminus B, B)$, where bicliques with an empty part can be avoided. Observe that these three bicliques cover precisely the same edges covered by (A, B) with the same multiplicities and orientations. Therefore, $\mathcal{C}'$ is a 2-biclique covering of H of size $|\mathcal{C}'| \leq 3k$ which satisfies Items 2 and 3 of Lemma 15. It further satisfies that each of its bicliques has either equal or disjoint parts. We let $\mathcal{C}'' \subseteq \mathcal{C}'$ denote the collection of bicliques of $\mathcal{C}'$ with equal parts. It clearly holds that $|\mathcal{C}''| \leq k$ and $|\mathcal{C}' \setminus \mathcal{C}''| \leq 2k$.

Every biclique of $\mathcal{C}''$ has the form (A, A) for some set $A \subseteq V$. For every $x \in A$, it covers a loop of x as an oriented edge (x, x), and for every distinct $x, y \in A$, it covers the edge that connects x and y in the two opposite orientations, namely, as (x, y) and as (y, x). This implies that all the vertices that appear in the bicliques of $\mathcal{C}''$ have loops in H and thus belong to V_1. Since the parts of the bicliques of $\mathcal{C}' \setminus \mathcal{C}''$ are disjoint, it follows that the bicliques of $\mathcal{C}''$ cover all the loops of H. Since $\mathcal{C}'$ is a 2-biclique covering of H that covers the loops once, it follows that no edge is covered by both $\mathcal{C}''$ and $\mathcal{C}' \setminus \mathcal{C}''$.

Let F be the graph obtained from H by removing the edges of the bicliques of $\mathcal{C}''$. Since the bicliques of $\mathcal{C}''$ cover all the loops of H, it follows that the graph F is simple. The collection $\mathcal{C}' \setminus \mathcal{C}''$ forms a 2-biclique covering of F, hence $\mathrm{bp}_2(F) \leq 2k$. Let $F^{(2)}$ denote the subgraph of F on V that includes all the edges that are covered by $\mathcal{C}' \setminus \mathcal{C}''$ twice. Since the bicliques of $\mathcal{C}''$ involve only vertices of V_1, it follows that $F^{(2)}$ has an induced subgraph isomorphic to $H_0^{(2)}$, implying that $\chi(F^{(2)}) \geq \chi(H_0^{(2)}) \geq m^{1/3}$.

Now, let G be the graph that contains two disjoint copies of $F^{(2)}$, with additional edges between the two copies according to the bicliques of $\mathcal{C}''$. More precisely, G is the graph on the vertex set $V \times [2]$ in which two vertices (x, b) and (y, b) for $b \in [2]$ are adjacent if x and y are adjacent in $F^{(2)}$, and two vertices $(x, 1)$ and $(y, 2)$ are adjacent if (x, y) is an oriented edge covered by the bicliques of $\mathcal{C}''$. The graph G is simple, because $F^{(2)}$ is simple and because no oriented edge is covered twice by $\mathcal{C}''$. We claim that G satisfies the assertion of the theorem.

Firstly, G has an induced subgraph isomorphic to $F^{(2)}$, hence it follows that $\chi(G) \geq \chi(F^{(2)}) \geq m^{1/3}$.

Secondly, we claim that $\mathrm{bp}(G) \leq 33 \cdot k^2$. To see this, use Claim 13 and $\mathrm{bp}_2(F) \leq 2k$ to obtain that $\mathrm{bp}(F^{(2)}) \leq (4k)^2$, that is, at most $(4k)^2$ bicliques are needed for a partition of the edges of each copy of $F^{(2)}$ in G. Consider further the bicliques $(A \times \{1\}, A \times \{2\})$ for $(A, A) \in \mathcal{C}''$, which form a partition with size at most k of the edges of G between the vertices of $V \times \{1\}$ and those of $V \times \{2\}$. It follows that $\mathrm{bp}(G) \leq 2 \cdot (4k)^2 + k \leq 33 \cdot k^2$.

Finally, we claim that G is regular with degree d^2. To see this, consider an arbitrary vertex $(i_1, j_1, b) \in V \times [2]$ in G. This vertex is adjacent to the vertices (i_2, j_2, b) for which the pairs (i_1, j_1) and (i_2, j_2) are adjacent in H and the edge that connects them is covered twice by $\mathcal{C}' \setminus \mathcal{C}''$. It is further adjacent to the vertices (i_2, j_2, b') with $b' \neq b$ for which the pairs (i_1, j_1) and (i_2, j_2) are adjacent in H and the edge that connects them is covered by $\mathcal{C}''$ (twice if they are distinct, and once otherwise). Since $\mathcal{C}'$ satisfies Items 2 and 3 of Lemma 15, it follows that the degree of (i_1, j_1, b) in G is precisely the number of pairs $(i_2, j_2) \in V$ satisfying $M_{i_1, j_2} = 1$ and $M_{i_2, j_1} = 1$. By the d-regularity of M, the latter is equal to d^2, so we are done.

Case 2. Suppose next that $\chi(H_0^{(2)}) < m^{1/3}$. We start by proving that there exists an independent set $S \subseteq V_0$ in the graph $H_0^{(2)}$ for which

$$\chi(H_0^{(1)}[S]) \geq m^{1/3}. \tag{5}$$

Indeed, the assumption implies that there exists a proper coloring of $H_0^{(2)}$ with fewer than $m^{1/3}$ colors. If the induced subgraph of $H_0^{(1)}$ on every color class of this coloring has chromatic number smaller than $m^{1/3}$, then one can obtain a proper coloring of $H_0^{(1)}$ whose number of colors is smaller than $m^{1/3} \cdot m^{1/3} = m^{2/3}$, which implies using (4) that $\chi(H_0) < m^{2/3} \cdot m^{1/3} = m$, in contradiction to Lemma 14. This implies that some color class $S \subseteq V_0$ of the coloring of $H_0^{(2)}$ satisfies (5).

Now, consider the 3-partite graph G' whose vertex set consists of three copies of V that are connected by three copies of the bicliques of $\mathcal{C}$ oriented in a cyclic manner. More precisely, the vertex set of G' is $V \times [3]$ and its edges are those of the bicliques $(A \times \{1\}, B \times \{2\})$, $(A \times \{2\}, B \times \{3\})$, and $(A \times \{3\}, B \times \{1\})$ for all $(A, B) \in \mathcal{C}$. By Lemma 15, no oriented edge of the bicliques of $\mathcal{C}$ is covered twice. It thus follows that G' is a simple graph and that each of its edges is covered by the above bicliques exactly once. By $|\mathcal{C}| = k$, it follows that $\mathrm{bp}(G') \leq 3k$. Further, Items 2 and 3 of Lemma 15 imply that the degree of every vertex $(i_1, j_1, b) \in V \times [3]$ of G' is precisely the sum of the number of pairs $(i_2, j_2) \in V$ satisfying $M_{i_1, j_2} = 1$ and the number of pairs $(i_2, j_2) \in V$ satisfying $M_{i_2, j_1} = 1$. Since the matrix M is d-regular, it follows that the graph G' is regular with degree $2nd$.

We next define a graph G as follows. The graph G is obtained from G' by removing all the edges whose both endpoints are in $S \times [3]$ and by adding the edges of the induced subgraph $H[S]$ of H on S to each of the three copies of S in G (i.e., $S \times \{b\}$ for $b \in [3]$). Since G' is a simple graph, using the fact that S is a subset of V_0, it follows that G is a simple graph as well. We claim that G satisfies the assertion of the theorem.

Firstly, since S is an independent set in $H_0^{(2)}$, the subgraph of G induced on every copy of S is isomorphic to $H_0^{(1)}[S]$. It thus follows from (5) that $\chi(G) \geq \chi(H_0^{(1)}[S]) \geq m^{1/3}$.

Secondly, we claim that $\mathrm{bp}(G) \leq 9k$. To see this, recall that $\mathrm{bp}(G') \leq 3k$, and consider some biclique partition with size at most $3k$ of the edges of G'. Replace each biclique $(A \times \{b\}, B \times \{b'\})$ of this partition, where $b \neq b'$, by the two bicliques

$$((A \setminus S) \times \{b\}, B \times \{b'\}) \quad \text{and} \quad ((A \cap S) \times \{b\}, (B \setminus S) \times \{b'\}).$$

This gives us a biclique partition with size at most $6k$ of all the edges of G' but those spanned by the vertices of $S \times [3]$. It remains to cover the edges of the three copies of $H[S]$ in G. Since S is an independent set in $H_0^{(2)}$, each edge of $H[S]$ is covered by $\mathcal{C}$ exactly once, so by restricting the bicliques of $\mathcal{C}$ to the vertices of S, we get a biclique partition of $H[S]$ with size at most k. This gives us a biclique partition with size at most k of the edges of $G[V \times \{b\}]$ for each $b \in [3]$, implying that $\mathrm{bp}(G) \le 6k + 3k = 9k$.

Finally, we claim that G is regular. To see this, recall that G' is regular and that G is obtained from G' by replacing the edges between the different copies of S by the corresponding edges inside the copies of S. Since those edges are covered exactly once by $\mathcal{C}$, this does not change the degrees of the vertices, yielding that the graph G is regular as well, and we are done. ◀

References

1. Kazuyuki Amano. Some improved bounds on communication complexity via new decomposition of cliques. *Discret. Appl. Math.*, 166:249–254, 2014.

2. Kaspars Balodis, Shalev Ben-David, Mika Göös, Siddhartha Jain, and Robin Kothari. Unambiguous DNFs and Alon-Saks-Seymour. In *IEEE 62nd Annual Symposium on Foundations of Computer Science (FOCS'21)*, pages 116–124. IEEE, 2021.

3. Shalev Ben-David, Pooya Hatami, and Avishay Tal. Low-sensitivity functions from unambiguous certificates. In *8th Innovations in Theoretical Computer Science Conference (ITCS'17)*, pages 28:1–28:23, 2017.

4. Jan Bouda, Matej Pivoluska, and Martin Plesch. Improving the Hadamard extractor. *Theor. Comput. Sci.*, 459:69–76, 2012.

5. Nicolas Bousquet, Aurélie Lagoutte, Frédéric Maffray, and Lucas Pastor. Decomposition techniques applied to the clique-stable set separation problem. *Discret. Math.*, 341(5):1492–1501, 2018.

6. Nicolas Bousquet, Aurélie Lagoutte, and Stéphan Thomassé. Clique versus independent set. *European J. Combinatorics*, 40:73–92, 2014.

7. Richard A. Brualdi, Rachel Manber, and Jeffrey A. Ross. On the minimum rank of regular classes of matrices of zeros and ones. *J. Combin. Theory Ser. A*, 41(1):32–49, 1986.

8. Arkadev Chattopadhyay, Yuval Filmus, Sajin Koroth, Or Meir, and Toniann Pitassi. Query-to-communication lifting using low-discrepancy gadgets. *SIAM J. Comput.*, 50(1):171–210, 2021. Preliminary version in ICALP'19.

9. Benny Chor and Oded Goldreich. Unbiased bits from sources of weak randomness and probabilistic communication complexity. *SIAM J. Comput.*, 17(2):230–261, 1988. Preliminary version in FOCS'85.

10. Maria Chudnovsky and Paul Seymour. Subdivided claws and the clique-stable set separation property. In *2019–20 MATRIX Annals*, volume 4, pages 483–487. Springer, 2021.

11. Sebastian M. Cioabă and Michael Tait. More counterexamples to the Alon-Saks-Seymour and rank-coloring conjectures. *Electron. J. Combinatorics*, 18(1), 2011.

12. D. de Caen, David A. Gregory, and Norman J. Pullman. The Boolean rank of zero-one matrices. *Proc. of the 3rd Caribbean Conference on Combinatorics and Computing*, pages 169–173, 1981.

13. Mika Göös. Lower bounds for clique vs. independent set. In *IEEE 56th Annual Symposium on Foundations of Computer Science (FOCS'15)*, pages 1066–1076, 2015.

14. Mika Göös, Shachar Lovett, Raghu Meka, Thomas Watson, and David Zuckerman. Rectangles are nonnegative juntas. *SIAM J. Comput.*, 45(5):1835–1869, 2016. Preliminary version in STOC'15.

15. Mika Göös, Toniann Pitassi, and Thomas Watson. Deterministic communication vs. partition number. *SIAM J. Comput.*, 47(6):2435–2450, 2018. Preliminary version in FOCS'15.

16 Ronald L. Graham and Henry O. Pollak. On the addressing problem for loop switching. *Bell Syst. Tech. J.*, 50(8):2495–2519, 1971.

17 David A. Gregory, Norman J. Pullman, Kathryn F. Jones, and J. Richard Lundgren. Biclique coverings of regular bigraphs and minimum semiring ranks of regular matrices. *J. Comb. Theory, Ser. B*, 51(1):73–89, 1991.

18 Kim A. S. Hefner, Teresa D. Henson, J. Richard Lundgren, and John S. Maybee. Biclique coverings of bigraphs and digraphs and minimum semiring ranks of {0, 1}-matrices. *Congr. Numer.*, 71:115–122, 1990.

19 Hao Huang and Benny Sudakov. A counterexample to the Alon-Saks-Seymour conjecture and related problems. *Combinatorica*, 32(2):205–219, 2012.

20 Stasys Jukna. *Boolean Function Complexity – Advances and Frontiers*, volume 27 of *Algorithms and Combinatorics*. Springer, 2012.

21 Jeff Kahn. Recent results on some not-so-recent hypergraph matching and covering problems. In *Extremal Problems for Finite Sets*, pages 305–353. Bolyai Soc. Math. Stud., 1994.

22 Pravesh K. Kothari, Raghu Meka, and Prasad Raghavendra. Approximating rectangles by juntas and weakly-exponential lower bounds for LP relaxations of CSPs. In *Proc. of the 49th Annual ACM Symposium on Theory of Computing (STOC'17)*, pages 590–603, 2017.

23 Aurélie Lagoutte and Théophile Trunck. Clique-stable set separation in perfect graphs with no balanced skew-partitions. *Discret. Math.*, 339(6):1809–1825, 2016.

24 László Lovász and Michael E. Saks. Lattices, Möbius functions and communication complexity. In *IEEE 29th Annual Symposium on Foundations of Computer Science (FOCS'88)*, pages 81–90, 1988.

25 Shachar Lovett. Recent advances on the log-rank conjecture in communication complexity. *Bull. EATCS*, 112, 2014.

26 Sylvia D. Monson, Norman J. Pullman, and Rolf Rees. A survey of clique and biclique coverings and factorizations of (0, 1)-matrices. *Bull. Inst. Combin. Appl.*, 14:17–86, 1995.

27 Norman J. Pullman. Ranks of binary matrices with constant line sums. *Linear Algebra Appl.*, 104:193–197, 1988.

28 Alexander A. Razborov. The gap between the chromatic number of a graph and the rank of its adjacency matrix is superlinear. *Discret. Math.*, 108(1–3):393–396, 1992.

29 Manami Shigeta and Kazuyuki Amano. Ordered biclique partitions and communication complexity problems. *Discret. Appl. Math.*, 184:248–252, 2015.

30 Mihalis Yannakakis. Expressing combinatorial optimization problems by linear programs. *J. Comput. Syst. Sci.*, 43(3):441–466, 1991. Preliminary version in STOC'88.

31 Andrew Chi-Chih Yao. Some complexity questions related to distributive computing. In *Proc. of the 11th Annual ACM Symposium on Theory of Computing (STOC'79)*, pages 209–213, 1979.