The Weak Rank Principle: Lower Bounds and Applications

Michal Garlík*
Imperial College London

Svyatoslav Gryaznov†
Imperial College London

Hanlin Ren‡
Institute for Advanced Study

Iddo Tzameret§
Imperial College London

Abstract

Given two symbolic matrices X and Y of dimensions $m \times n$ and $n \times m$, respectively, the *rank principle* states that when $m = n+1$ and A is a scalar matrix of rank $n+1$, the equation $XY = A$ is unsatisfiable. When m is arbitrarily larger than n and A has rank exceeding n, we obtain the *weak rank principle*. We study this principle as an algebraic generalisation of the weak pigeonhole principle (WPHP), asserting that m pigeons cannot be injected into n holes, extending its counting argument to an algebraic setting. As a strengthening of WPHP, it admits proof complexity lower bounds in settings where none are known for WPHP, yet we show that these still yield applications analogous to those of WPHP. In particular, using new generalised types of random restrictions, which may be interesting by themselves, this allows us to resolve a number of open problems in proof complexity, including the construction of proof complexity generators for Polynomial Calculus Resolution over the two-element field ($\mathsf{PCR}_{\mathbb{F}_2}$), new generators for Sherali–Adams (SA), and hardness results for circuit lower bound statements against $\mathsf{PCR}_{\mathbb{F}_2}$, as detailed below.

Generators for $\mathsf{PCR}_{\mathbb{F}_2}$: We prove exponential size lower bounds for several encodings—both algebraic and CNF—of the weak rank principle in PCR over $\mathbb{F}_2$, where no such bounds are known for the WPHP in the regime with arbitrarily many pigeons. In particular, we obtain $2^{\Omega(n)}$ size lower bounds for both algebraic and standard CNF encodings, including the *bamboo-tree encoding*, which is the most useful and corresponds to a circuit encoding, as considered by Alekhnovich, Ben-Sasson, Razborov, and Wigderson (*SIAM J. Comput.*, 2004) and Razborov (*Ann. Math.*, 2015). Our bounds hold for every matrix A in $XY = A$, implying that the rank principle forms a proof complexity generator with nearly quadratic stretch. Using a standard iteration technique we amplify the stretch to $2^{n^{\Omega(1)}}$, meaning we obtain a function generator. This resolves an open problem posed by Alekhnovich *et al.* (*SIAM J. Comput.*, 2004) and Razborov (*Ann. Math.*, 2015) concerning the construction of proof complexity generators with good stretch for $\mathsf{PCR}_{\mathbb{F}_2}$.

Generators for SA: Since in SA even the *strong* pigeonhole principle is easy, we develop a new size lower-bound technique showing that the weak rank principle, encoded as a bamboo-tree CNF, serves as a proof complexity generator for SA. Our method introduces a new relaxed notion of degree and a new corresponding pseudoexpectation tailored specifically to the rank principle (and incompatible with the pigeonhole principle).

Circuit lower bound formulas: We show that $\mathsf{PCR}_{\mathbb{F}_2}$ does not admit short proofs of lower-bound statements against Boolean circuits, nor against weak models of algebraic circuits such as non-commutative algebraic branching programs. This settles an open problem raised by Razborov (*Ann. Math.*, 2015) concerning the provability of such lower bounds in $\mathsf{PCR}_{\mathbb{F}_2}$.

Rank principle as an axiom: Finally, we demonstrate the centrality of the weak rank principle by showing that it is *necessary* for proving NC^2 circuit lower bounds and *sufficient* for proving $\mathsf{AC}^0[p]$ lower bounds.

*michal.garlik@gmail.com
†svyatoslav.i.gryaznov@gmail.com
‡h4n1in.r3n@gmail.com
§iddo.tzameret@gmail.com

Contents

1 Introduction

Proof complexity provides both a concrete and conceptual framework for studying computational lower bounds. On the one hand, it seeks to develop combinatorial and algebraic techniques for proving unconditional lower bounds on the lengths of proofs, with relations to complexity class

separations. On the other hand, it offers a setting for formulating and exploring metamathematical questions—for example, which proof systems can efficiently establish which lower bounds in computational complexity theory.

For concrete proof-size lower bound questions, it remains a long-standing open problem to establish superpolynomial size lower bounds against sufficiently strong proof systems, such as textbook propositional logic (i.e., Frege systems). Such lower bounds are unknown even against significantly weaker fragments, such as those operating with $\mathsf{AC}^0[2]$ circuits. Nonetheless, the development of theoretical frameworks and techniques aimed at tackling such lower bounds remains a highly active and vibrant area of research.

The Weak Pigeonhole Principle. A prominent example illustrating the broad reach of proof complexity is the *pigeonhole principle* (PHP for short), which is the (suitably encoded) statement that $m = n + 1$ pigeons cannot be mapped into n holes if each hole can accommodate at most one pigeon. The *weak pigeonhole principle* (WPHP) refers to the case where the number of pigeons is possibly much larger than the number of holes; namely, it is the collection of such statements for all pairs $m > n$, where m may be arbitrarily larger than n. In this regard, WPHP is logically weaker than PHP where $m = n + 1$.

The pigeonhole principle is perhaps the most influential example in proof complexity, serving as a driving force behind many lower bound techniques and frameworks. These include bottleneck counting [35], pigeonhole switching lemmas and k-evaluations [2, 51, 63], pigeon dance [39, 69], pseudo-width [65, 71], etc. As for upper bounds, already TC^0-Frege admits polynomial-size proofs of PHP (and hence WPHP); see [16, 20]. Despite this progress, a notable open problem posed by Razborov [73] remains unresolved: proving size lower bounds for WPHP against the polynomial calculus resolution (PCR) proof system (see Footnote 1 and discussion therein).

Beyond concrete lower bounds, the pigeonhole principle plays a central role in the development of theories in bounded arithmetic, which study the computational complexity of the concepts required to prove various statements within formal systems. In bounded arithmetic, the weak pigeonhole principle serves as an axiom from which important results—particularly those related to randomness in computation—can be derived. As early as 1981, Woods [82] observed that explicit counting of the number of elements in a finite set can often be replaced by applications of the pigeonhole principle for bounded formulas. Building on this idea, Paris, Wilkie, and Woods [61] introduced the weak pigeonhole principle, and showed that it often serves as a more suitable substitute for PHP in such contexts and that it is provable in bounded arithmetic T_2. Initial work by Wilkie (unpublished; see Krajíček [48, Theorem 7.3.7]), further developed by Thapen [79] and systematically pursued by Jeřábek [42–44], established WPHP as a useful axiom for reasoning about randomized computation.

WPHP and proof complexity generators. A concept closely related to the weak pigeonhole principle is that of a proof complexity generator. In fact, it is more directly connected to the *dual* weak pigeonhole principle (denoted dWPHP), which states that when n pigeons are mapped to $2n$ holes, at least one hole must remain empty. The notion of proof complexity generators was introduced independently by Alekhnovich, Ben-Sasson, Razborov, and Wigderson [4], and by Krajíček [49, 50]; see also the monograph [53] for a comprehensive treatment.

A *proof complexity generator* is any encoding of the statement that expresses that a point $b \in \{0,1\}^\ell$ is not in the image of a given polytime mapping $G : \{0,1\}^m \to \{0,1\}^\ell$, with $m < \ell$. The proof complexity of such statements depends on G and is sensitive to the encodings; indeed, [4] suggested three different encodings (see also Sokolov [76] for a discussion). We say that a proof complexity generator is *hard* against a proof system when for *every* point b there is no short proof that b is not in the image of G. This means that the proof system cannot prove that G is non-surjective. (Notice that even a single b for which the proof complexity generator is easy would constitute a proof of non-surjectivity, hence we insist that no such b exists; this point is explained further in Alekhnovich *et al.* [4].)

The hope is that for strong propositional proof systems, one can establish (at least conditionally) that there are no $\mathrm{poly}(\ell)$-size proofs that g is non-surjective, under the assumption that the mapping g is sufficiently pseudorandom (cf. [73]). Razborov in [73] proved the existence of hard

proof complexity generators for systems such as PCR and Res(k). However, as Razborov mentions, the important case of generators for PCR over $\mathbb{F}_2$ is completely open (the importance of this case is explained after stating Theorem 2.4).

WPHP and the provability of circuit lower bounds. WPHP and proof complexity generators also play a central role in the metamathematics of complexity theory—particularly in understanding which systems can efficiently prove circuit lower bounds. This connection was first observed by Razborov [69], who showed that WPHP reduces to circuit lower bound statements. Informally, this means that if WPHP is hard for some ("nice") proof system $\mathcal{P}$, then $\mathcal{P}$ cannot prove any circuit lower bound efficiently. This idea was employed by Razborov [69] and later by Raz [65]. The former established degree lower bounds for WPHP in polynomial calculus, and the latter established resolution size lower bounds. Both work then leveraged the above reduction to show that the statement "$\mathsf{NP} \not\subseteq \mathsf{P/poly}$", when encoded as a family of CNF formulas, does not admit efficient refutations in those systems.

More generally, one can define the *truth-table generator*, which maps a description of a small Boolean circuit to the truth table of the function it computes. Establishing that a string b lies outside the image of this generator is equivalent to proving that no small circuit computes the function with truth table b. Hence, the truth-table generator constitutes a proof-complexity generator against a system $\mathcal{P}$ exactly when $\mathcal{P}$ cannot efficiently prove any circuit lower bounds.

Linear algebraic instances. Beyond simple counting arguments like the pigeonhole principle, linear algebra is a key tool in discrete mathematics. Accordingly, Cook and Rackoff suggested linear algebraic statements as potential hard instances for strong propositional proof systems. Bonet, Buss, and Pitassi [15, Sec. 3.1.1] further explored this idea and identified candidates hard tautologies such as the *oddtown principle*, which asserts $XX^T \neq I_m$ for an $m \times n$ variable matrix X with $m > n$, where I_m is the $m \times m$ identity matrix. Soltys and Cook [77] systematically studied the *hard matrix identities* in the context of bounded arithmetic, focusing on statements such as the *inversion principle*, which asserts that $XY = I_n$ implies $YX = I_n$ for square $n \times n$ variable matrices X, Y, as well as other equivalent formulations of basic linear algebraic facts. Their goal was to identify minimal formal theories capable of proving such statements. Soltys and Urquhart [78] showed that the pigeonhole principle is reducible to (hence, not stronger than) these matrix identities. Later, it was demonstrated by Hrubeš and Tzameret over $\mathbb{F}_2$ [37] and by Tzameret and Cook over the integers [81] that these linear algebraic principles admit quasipolynomial-size propositional (i.e., Frege) proofs and are provable in relatively weak theories of arithmetic. The latter two works roughly show that linear algebra sits within "NC^2-reasoning" (formally, the theory VNC^2). The hard matrix identities were also considered in the context of the Ideal Proof System (IPS) by Grochow and Pitassi [34], and Andrews and Forbes [7] who investigated a close unsatisfiable instance $\{\det(X) = 0, XY = I\}$ for two square variable matrices X, Y.

A related algebraic principle is the (*strong*) rank principle: Let $m = n + 1$. Given two variable matrices X, Y of dimension $m \times n$ and $n \times m$, respectively, the product $XY = A$ is unsatisfiable whenever A is an $m \times m$ scalar matrix of rank m. This formula was considered implicitly in Krajíček [52], as a way to algebraically express proof complexity generators based on PHP.

For the specific case where A is the identity matrix I, Soltys and Cook [77, Equation (V), page 287] showed that the strong rank principle is equivalent over their theories (the base one denoted LA; hence over Frege) to the hard matrix identities, and specifically the inversion principle. Galesi, Grochow, Pitassi, and She [31] formulated the rank principle explicitly, for the special case when A is the identity matrix I, and when m is not necessarily $n+1$. Galesi *et al.* established PC degree lower bounds for the rank principle, using the same reduction from PHP degree lower bounds that was used in [78].

The weak rank principle. In this work we show the advantage in considering what we call the *weak rank principle*, WRank for short, as a natural algebraic analogue and augmentation of the weak pigeonhole principle. Given two variable matrices X and Y of dimensions $m \times n$ and $n \times m$, respectively, WRank states that

WRank. For an arbitrary scalar matrix A of rank at least $n+1$, the equation $XY = A$ is unsatisfiable, where $m > n$; here we mean that m is *arbitrarily larger* than n.

Notice that WPHP is (usually) considered in the same regime, namely when m is arbitrarily larger than n [71]. Accordingly, all our lower bounds are expressed in terms of n and are *independent* of m.

Our results show that the weak rank principle can be applied in settings where the weak pigeonhole principle fails, and that it provides a framework for both lower and upper bounds in proof complexity. In particular, we obtain lower bounds and corresponding proof-complexity generators with a good stretch for $\mathsf{PCR}_{\mathbb{F}_2}$ which can also be iterated to a function generator (where none were previously known) and introduce a new generator for the Sherali–Adams system, establish the hardness of circuit lower-bound statements for $\mathsf{PCR}_{\mathbb{F}_2}$ (which was open), and identify upper bounds—namely, feasibly constructive proofs—that are facilitated by the weak rank principle itself.

The proof systems we shall consider in this work are polynomial calculus resolution PCR and Sherali–Adams SA. See Section 4 for the precise definitions and references.

What is known about WRank. For the *strong* rank principle (where $m = n + 1$, and in fact up to $m \leq n^2$), size lower bounds against PCR could be shown over any field, by a reduction to the (strong) pigeonhole principle (with m pigeons; see [31, 78] for this reduction), and then using a size-degree tradeoff argument. However, for the *weak* rank principle (when m is arbitrary) only *degree* lower bounds are known in polynomial calculus resolution (PCR); again, this follows easily from known degree lower bounds for WPHP. However, the more challenging and meaningful regime is that of *size* lower bounds for PCR and stronger systems. Notably, no PCR size lower bounds are currently known for WPHP for arbitrary many pigeons, and in fact when the number of pigeons exceeds n^2 (see Mikša and Nordström [55] and de Rezende, Nordström, Risse and Sokolov [28])[1]. This motivates algebraically extending WPHP to WRank, which enables new size lower bounds in settings where WPHP has so far proven insufficient (as the current work shows).

With respect to *upper bounds*, while WPHP admits polynomial-size proofs in TC^0-Frege, the best known upper bound for WRank is a polynomial-size proof in NC^2-Frege. This could be shown as follows: for strong enough proof systems closed under low degree reductions WRank is implied by the special case of WRank when $A = I$ (see Lemma 7.4), which in turn is implied by the inversion principle by [77]; finally, the inversion principle admits polynomial-size proofs in NC^2-Frege by the work of Hrubeš and Tzameret [37]. On the other hand, it is reasonable to conjecture that Frege does not admit polynomial-size proofs of WRank by the fact that linear algebraic statements are expected not to have polynomial-size Frege proofs as noted by Buss *el al.* [15].

Note that the relation between the weak rank principle and the strong one (and hence, by [77], its relation to the hard matrix identities) is not entirely understood, since the latter concerns square matrices, while our focus is on highly non-square matrices (hence, the "weak" regime).

2 Our Results

We present four types of results based on the weak rank principle: Lower bounds and generators for PCR over $\mathbb{F}_2$, hereafter denoted $\mathsf{PCR}_{\mathbb{F}_2}$ (Section 2.1), lower bounds and generators for SA (Section 2.2), hardness of circuit lower bound statements for $\mathsf{PCR}_{\mathbb{F}_2}$ (Section 2.3), and upper bounds (namely, feasible constructive proofs) facilitated by the weak rank principle (Section 2.4).

2.1 Lower Bounds and Generators for $\mathsf{PCR}_{\mathbb{F}_2}$

We establish lower bounds and construct generators for PCR over $\mathbb{F}_2$, under the following encodings of increasing strength:

[1] Beyond n^2 pigeons, size lower bound techniques against PCR based on degree break down. Note that for *resolution*, using different techniques by Raz [65] and subsequently Razborov [70, 72] as well as de Rezende *et al.* [28], the case of WPHP lower bounds with arbitrary many pigeons m is resolved.

- **Algebraic encoding.** This setting provides the most direct algebraic formulation and serves as a foundation for the subsequent encodings.
- **Perfect matching (PM) encoding.** In the PM encoding, we obtain lower bounds for the weak rank principle, when $A = I$, against $\mathsf{PCR}_{\mathbb{F}_2}$. This encoding is in a CNF. To get a generator in this encoding, we should prove the lower bound for every A. Although it is achievable by similar techniques used in the next item, we do not formally prove this case, since this encoding does not appear to be directly useful to establish hardness of circuit lower bound statements. The case $A = I$ is conceptually simpler than the general case of arbitrary A, yet serves as an instructive case for the forthcoming generators because those results expand on similar ideas. It requires a different notion of degree from the algebraic encoding, that is useful in the sequel (e.g., for SA lower bounds).
- **Bamboo-tree encoding.** The Bamboo-tree encoding yields the strongest construction, achieving the same stretch as the generators above ($2mn$ to m^2). In addition, we are able to prove that this generator is *iterable* (in the sense of [50, 73]) under this encoding, hence we establish a *function* generator (i.e., a generator with a stretch of $2^{n^{\Omega(1)}}$). A notable consequence of this function generator is that $\mathsf{PCR}_{\mathbb{F}_2}$ does not admit short proofs of circuit lower bound statements such as $\mathsf{NP} \not\subseteq \mathsf{P/poly}$.

We start by providing more technical background to our new generators.

Context and motivation for our generators. Recall that a proof complexity generator encodes the statement that a point $b \in \{0,1\}^\ell$ is not in the image of a polynomial-time map $G : \{0,1\}^m \to \{0,1\}^\ell$, with $m < \ell$. When the weak rank principle is viewed in this framework, the matrix product XY plays the role of the map G, and the point outside its image is the matrix A.

The known generators for $\mathsf{PCR}_{\mathbb{F}_2}$ in the literature are based on reductions to the pigeonhole principle. For the *strong* pigeonhole principle, Krajíček [52, Section 1] constructed a generator stretching n bits to $n + 1$ bits. The same construction can be combined with the best known lower bounds for the *weak* pigeonhole principle over $\mathsf{PCR}_{\mathbb{F}_2}$ [5, 55] to yield a slightly superlinear stretch—from n^3 to n^4 bits[2]. (For comparison, our results achieve a nearly quadratic stretch of $2mn$ to m^2 since our lower bounds hold in the regime where m is arbitrarily larger than n.)

In the present work, we aim to base the hardness of such generators on the hardness of WRank instead, which is *stronger* than WPHP. For instance, WPHP is easy for the SoS proof system, but WRank is plausibly hard for it; likewise, $\mathsf{Res}(\log n)$ admits quasipolynomial-size refutations of WPHP [54], yet statements based on linear algebra (and in particular WRank) are expected to be hard for it [15].

As mentioned above, for arbitrary m, the hardness of WPHP against PCR over any field remains open. If such bounds were known, they could yield strong generators through Krajíček's construction and further applications. In particular, a sufficiently strong lower bound for the Onto-WPHP would, via Raz's method [65], yield that certain circuit lower bound statements for unbounded fan-in circuits cannot be efficiently proven in PCR.

This led Alekhnovich *et al.* [4] to study hard instances distinct from WPHP on which to base proof-complexity generators and their applications to circuit lower-bound statements. They proposed the so-called *Nisan generator*, a special case of the Nisan–Wigderson generator [59], which is based on systems of linear equations over $\mathbb{F}_2$ defined over expander graphs. The stretch of this construction alone is not sufficient to yield application to circuit lower bound statements.

An important research direction is to obtain proof complexity generators with *as large stretch as possible*. When the stretch is exponential (i.e., $2^{n^{\Omega(1)}}$ in the seed length n) the generator is called a *function generator*. To achieve such amplification, Krajíček [50] introduced the notion of *s-iterability*, designed to boost the stretch of a variant of the Nisan generator [59]. Improving [4], Razborov [73] relaxed the expander requirements and showed that linear systems as in [4]

[2]Given a formula PHP^m_n, Krajíček [52] builds a function stretching $nm+tn$ bits into tm, for any parameter t; the ratio $tm/(nm+tn)$ is maximised at $t = \Theta(n^2)$. The best known lower bounds for PHP^m_n against PCR hold for $m = o(n^2)$. If we plug these values of t and m into $nm+tn$ and tm, respectively, we obtain a stretch of n^3 to n^4.

can be *iterated* to achieve a much larger stretch—about 2^{n^ε}. In particular, the hardness of the base generator transfers to the iterated version, since an iterated expander remains an expander. However, systems of linear equations over $\mathbb{F}_2$ are *easy* to refute in $\mathsf{PCR}_{\mathbb{F}_2}$; therefore, this construction cannot yield generators hard for $\mathsf{PCR}_{\mathbb{F}_2}$.

The limitations of existing principles motivate the use of the WRank which subsumes both the weak pigeonhole principle and systems of linear equations. This allows us to obtain lower bounds for WRank (over $\mathbb{F}_2$) for arbitrary m, thereby producing a hard *base generator*. The hardness of WRank persists under iteration, which enables us to construct function generators that remain hard and leads to the hardness of corresponding circuit lower-bound statements.

Among other results known about generators are Khaniki's Nisan–Wigderson generator against $\mathsf{AC}^0[p]$-Frege [46] encoded as a (non-CNF) propositional formula. In addition, Sokolov [76] improved the lower bounds for a particular generator encoding (functional encoding as in [4]).

Algebraic encoding. The algebraic encoding of the negation of WRank, denoted $\mathsf{Rank}_n^m(A)$, consists of m^2 polynomial equations of degree 2,

$$\mathsf{Rank}_n^m(A): \qquad \sum_{k=1}^{n} x_{i,k}y_{k,j} = A_{i,j}, \quad \text{for all } i,j \in [m]. \tag{1}$$

Theorem 2.1 (Algebraic encoding lower bound; see Theorems 5.7 and 5.43)**.** *For every $m > n$ and $A \in \mathbb{F}_2^{m\times m}$, every $\mathsf{PCR}_{\mathbb{F}_2}$ refutation of $\mathsf{Rank}_n^m(A)$ requires size $2^{\Omega(n)}$. Consequently, $\mathsf{Rank}_n^m(A)$ is a proof complexity generator stretching $2nm$ bits into m^2. Moreover, the iterated variant of $\mathsf{Rank}_n^m(A)$ is a function generator with stretch $2^{n^{\Omega(1)}}$.*

Here, size is measured by the number of distinct monomials appearing in the refutation (see precise definitions in Section 4).

Algebraic encoding lower bounds are obtained using random restrictions, which yield a size-to-degree reduction and already suffice to derive the hardness of certain circuit lower-bound statements (for example, for non-commutative algebraic branching programs; see Section 8.3.1). The argument in this setting is technically simpler than the proofs for the CNF encodings introduced below, as the latter requires translating the algebraic reasoning into a combinatorial framework. The lower bound for the algebraic instance in Theorem 2.1 thus forms the basis for the CNF lower bounds presented later and underlies the high-level random-restriction approach used throughout.

The algebraic encoding, however, is specific to algebraic proof systems and therefore not directly comparable with encodings suited for other systems. To address this, we encode WRank as a CNF formula based on the perfect matching principle, and later consider the more demanding *bamboo-tree* encoding (see Section 5.3). The choice to work with CNF encodings is natural, as CNF is the standard formulation in proof complexity. Moreover, to extend lower bounds from algebraic proof systems such as PCR and SoS to systems like AC^0-Frege or $\mathsf{Res}(\mathrm{lin})$ (that is, resolution over linear equations [66]), CNF encodings are the appropriate framework, whereas the algebraic formulation—involving degree-2 polynomial equations—lies outside the expressive power of these systems.

Perfect matching encoding. The perfect matching CNF encoding of WRank, denoted $\mathsf{PMRank}_n^m(A)$, encodes each equation $\sum_{k=1}^{n} x_{i,k}y_{k,j} = A_{i,j}$ of $\mathsf{Rank}_n^m(A)$ by stating there exists a perfect matching on the satisfied monomials (i.e., those equal 1) of this equation. To encode such a matching we use extension variables for each pair of monomials in the equation (together with an extra point if $A_{i,j} = 1$). See Section 5.2 for the definition. Similar encodings of parity computations were considered in Impagliazzo–Segerlind and Ken [40, 45].

As mentioned above, we shall consider only the case $A = I$ and prove lower bounds for this encoding against $\mathsf{PCR}_{\mathbb{F}_2}$. The case for every A, yielding a generator could be achieved with techniques similar to the ones in the bamboo-tree encoding.

Theorem 2.2 (Perfect matching encoding lower bound against $\mathsf{PCR}_{\mathbb{F}_2}$; see Theorem 5.9)**.** *For every $m > n$, every $\mathsf{PCR}_{\mathbb{F}_2}$ refutation of the perfect matching CNF encoding $\mathsf{PMRank}_n^m(I_m)$ requires size $2^{\Omega(n)}$.*

The case of $\mathsf{PCR}_{\mathbb{F}_2}$ is the most interesting because the perfect matching principle (stating that there is no perfect matching on an odd size set) is in fact easy for $\mathsf{PCR}_{\mathbb{F}_2}$, hence the hardness of $\mathsf{PMRank}_n^m(I_m)$ does not stem from the encoding per se. This contrasts many other cases where the hardness follows from the hardness of the perfect matching principle itself [9, 17, 19, 33, 39, 48], as we show for the case of $\mathsf{PCR}_{\mathbb{F}}$ when $\mathrm{char}(\mathbb{F}) \neq 2$ in the next theorem.

The next result demonstrates the sensitivity of the encoding of the generators. Although we can construct generators for several proof systems using the PM encoding, it is not known how to get hardness of circuit lower bound statements from these generators.

Theorem 2.3 (Perfect matching encoding lower bound over any field; see Theorem 5.17)**.** *For every $m > n$ and $A \in \{0,1\}^{m \times m}$, every $\mathsf{PCR}_{\mathbb{F}}$ for any field $\mathbb{F}$ with $\mathrm{char}(\mathbb{F}) \neq 2$, SoS, or AC^0-Frege refutation of the perfect matching CNF encoding $\mathsf{PMRank}_n^m(A)$ requires size $2^{\Omega(n)}$.*

Bamboo-tree encoding. The main challenge and open problems regarding proof complexity generators and their applications is predominantly about proving lower bounds for good encodings; where an encoding is good, if it has extension variables that correspond to gates of a circuit, hence could be applied to circuit statement lower bounds [4, 73].

The bamboo-tree CNF encoding of the WRank, denoted $\mathsf{BTRank}_n^m(A)$, encodes each equation $\sum_{k=1}^n x_{i,k}y_{k,j} = A_{ij}$ of $\mathsf{Rank}_n^m(A)$ by using extension variables introduced to sequentially compute all inner products involved. The extension variables for each inner product are arranged in a totally unbalanced binary tree known as a "bamboo". Each extension variable $u_{i,j,\ell}$ encodes the partial sum $\sum_{k=1}^{\ell} x_{i,k}y_{k,j}$ (for $\ell \in [n]$). Moreover, each monomial $x_{i,k}y_{k,j}$ has its own extension variable $z_{i,j,k}$.

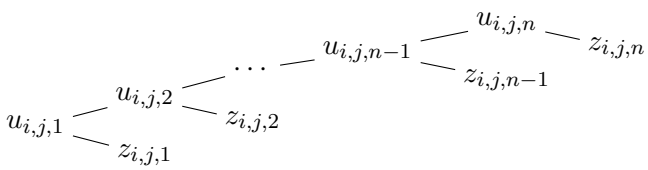


Figure 1: Example of one axiom of $\mathsf{BTRank}_n^m(A)$. Here, $u_{i,j,\ell}$ are the extension variables for the partial sum $\sum_{k=1}^{\ell} x_{i,k}y_{k,j} = \sum_{k=1}^{\ell} z_{i,j,k}$ (for $\ell \in [n]$). See Definition 5.18.

This natural encoding corresponds to a circuit in the sense of [4, 73], and similar encodings have been used repeatedly for parity computations [4, 73, 78].

Theorem 2.4 (Bamboo-tree encoding lower bound; see Theorems 5.19 and 5.67)**.** *For every $m > n$ and $A \in \mathbb{F}_2^{m \times m}$, every $\mathsf{PCR}_{\mathbb{F}_2}$ refutation of $\mathsf{BTRank}_n^m(A)$ requires size $2^{\Omega(n)}$. Consequently, $\mathsf{BTRank}_n^m(A)$ is a proof complexity generator stretching $2nm$ bits into m^2 bits. Moreover, there is an iterated variant of $\mathsf{BTRank}_n^m(A)$ that yields a function generator with stretch $2^{n^{\Omega(1)}}$.*

This result resolves an open problem raised in [4, 73] concerning the construction of proof-complexity generators for $\mathsf{PCR}_{\mathbb{F}_2}$. Razborov's [73] established generators against PCR based on the Nisan construction only over fields of characteristic different from 2. Our result closes this gap by exhibiting hard generators for $\mathsf{PCR}_{\mathbb{F}_2}$. Lower bounds over $\mathbb{F}_2$ are particularly significant and technically more challenging than those over other fields, as we now explain.

There are two distinct field parameters to consider: the *ground field*, over which the proof system operates, and the *expressed field*, over which the matrix product expressed in the weak rank principle is computed. Although these two fields may differ, the case where both are $\mathbb{F}_2$—that is, WRank over $\mathbb{F}_2$ and PCR over $\mathbb{F}_2$—is the most natural and the most difficult.

For example, unsatisfiable linear systems over $\mathbb{F}_2$ are easy for $\mathsf{PCR}_{\mathbb{F}_2}$, and more generally, linear systems over $\mathbb{F}_p$ are easy for $\mathsf{PCR}_{\mathbb{F}_p}$. When $p \neq 2$, however, such systems are non-Boolean and require explicit encoding of non-Boolean field elements, which makes the lower-bound task formally easier but conceptually less meaningful, as the hardness would then stem from the encoding rather than from the inherent structure of the weak rank principle. In contrast, working with both ground and expressed fields equal to $\mathbb{F}_2$ keeps all variables Boolean and ensures that the difficulty arises from the combinatorial and algebraic content of the principle itself.

Furthermore, $\mathbb{F}_2$ is usually the most challenging case for algebraic and semi-algebraic proof systems. For instance, lower bounds in the Nullstellensatz system or its variants often require substantially more complex designs over $\mathbb{F}_2$ than over larger or characteristic-0 fields (cf. [12, Theorem 12], [47]). Likewise, proof systems such as $\mathsf{Res}(\mathrm{lin})$ admit lower bounds over characteristic 0 [62], whereas corresponding results over finite fields—and in particular over $\mathbb{F}_2$ (cf. [41])—remain open. Thus, establishing hard generators over $\mathbb{F}_2$ advances our understanding precisely in the setting that is both the most natural and the least understood.

Lower bounds techniques. All our lower bounds share the following general *random self-reduction* structure: Use a reduction from size to appropriate, carefully defined notions of degree that vary from formula to formula and across our results. This means that we shall start, by way of contradiction, from a small refutation (having a small number of distinct monomials) and apply a random restriction or a generalised random restriction (changing variables to different ones) that simplifies terms in the refutation with respect to the appropriate notion of degree, reducing the formula to a smaller instance of the same principle. The second step is proving a lower bound on the relevant notion of degree, which will result in a contradiction (namely, no small size refutation exists).

The novelty and challenge is in finding the appropriate notions of degree and in devising the right random substitutions which will decrease the corresponding notion of degree. These notions of degree increase in level of complication along with the complexity of the encoding. Accordingly, the random substitutions increase in level of complication.

One idea that is different from the usual proof complexity lower bounds is that our generalised random restrictions are *random substitutions* of both 0-1 and variables in formulas. In PHP lower bounds, the usual argument hinges on applying 0-1 restrictions (representing partial matchings). But in our case partial 0-1 random restrictions are not always sufficient, hence we need to substitute the original variables by both 0-1 and other *variables or their negations*. The goal is to get self-reducibility: a smaller version of the principle. In the literature such random substitutions were used in works by, e.g., Pitassi, Rossman, Servedio and Tan [64] and subsequently Haståd [36] for AC^0-Frege lower bounds.

Bamboo-tree encoding of rank principle. The following explains the lower bounds for both the algebraic $\mathsf{Rank}_n^m(A)$ and the bamboo tree $\mathsf{BTRank}_n^m(A)$ encoding. We outline some ideas behind the proof of Theorem 2.4, which establishes a $2^{\Omega(n)}$ size lower bound for $\mathsf{BTRank}_n^m(A)$ in $\mathsf{PCR}_{\mathbb{F}_2}$. The key challenge is that this lower bound must hold independently of the parameter m, which precludes the use of standard expander-based techniques. These techniques would typically involve restricting one of the matrices, say X, to an expander, zeroing out most of the entries $x_{i,k}$, for $k \in [n]$, in each row $i \in [m]$. However, when the gap between m and n is too large, there are no bipartite expanders with suitable parameters for achieving degree lower bounds.

To overcome this, we relax the degree notion, aiming to balance two competing requirements for establishing size lower bounds: (1) the existence of random self-reductions of $\mathsf{BTRank}_n^m(A)$ that effectively reduce the relaxed degree, and (2) the existence of a lower bound on the relaxed degree for refutations of $\mathsf{BTRank}_n^m(A)$. The random self-reduction we design to achieve (1) is highly sensitive to the structure of the extension variables (the z-variables and u-variables defined above) and its necessarily technical nature leads us to present it in two stages for clarity. In this outline, we focus solely on motivating the notion of the relaxed degree that the self-reduction aims to decrease, and we primarily discuss requirement (2).

Consider a term t in x-, y- and z-variables of $\mathsf{BTRank}_n^m(A)$, that is, a product of some x-, y-

and z-variables and their negations. For a variable v, we write v^1 to denote v and v^0 to denote its negation, $\overline{v}$. Let C be the set of indices k such that $x^b_{i,k}$, $y^b_{k,j}$ or $z^b_{i,j,k}$ appears in t for some $b \in \{0,1\}$ and $i,j \in [m]$. We refer to C as the set of *columns* X-, Y^T- and Z-*mentioned* in t. Now, let τ be the substitution of X^TA for Y, i.e., $\tau(x_{i,k}) = x_{i,k}$, $\tau(y_{k,j}) = \sum_{i' \in [m]} x_{i',k}A_{i',j}$, and $\tau(z_{i,j,k}) = \tau(x_{i,k})\tau(y_{k,j})$ for all $i,j \in [m]$ and $k \in [n]$, with $\tau(\overline{v}) = 1 + \tau(v)$ for any variable v. We see that if we apply τ to t, the columns X-mentioned in each term of the polynomial $\tau(t)$ remain in C. It follows that each term t' of $\tau(t)$ either has degree at most $|C|$ (since we are working over the ring of multilinear polynomials), or there is $k \in C$ and $i < i' \in [m]$ such that t' is a multiple of $x_{i,k}x_{i',k}$ (by the pigeonhole principle).

Why is the last observation useful? The substitution τ maps the set of polynomial equations $XY = A$ to the set of polynomial equations $XX^TA = A$, and the latter has a straightforward degree-2 derivation from the oddtown equations $XX^T = I_m$, which in turn have an immediate degree-2 derivation from the algebraic formulation of the functional pigeonhole principle FPHP^m_n. For FPHP^m_n, Razborov [69] established a degree lower bound of $n/2$, which holds even for PCR proofs operating with multilinear polynomials modulo the ideal generated by the hole axioms ($x_{i,k}x_{i',k}$ for $i < i' \in [m]$ and $k \in [n]$) and the functionality axioms ($x_{i,k}x_{i,k'}$ for $i \in [m]$ and $k < k' \in [n]$). We conclude that there is no refutation of the algebraic formulation $\mathsf{Rank}^m_n(A)$ each term of which has less than $n/2$ X- or Y^T-mentioned columns. If such a refutation existed, then τ, along with the aforementioned degree-2 derivations, would convert it into a refutation of FPHP^m_n, where every term has either degree less than $n/2$ or is a multiple of a hole axiom, contradicting the cited lower bound. This forms the column degree lower bound part in the proof of Theorem 2.1. Similarly, this argument rules out the existence of a refutation of a variant of $\mathsf{Rank}^m_n(A)$ that involves the x-, y-, and z-variables (but not the u-variables), where each term in the refutation has less than $n/2$ X-, Y^T- or Z-mentioned columns.

It is clear that the argument from the above paragraph alone is not sufficient for $\mathsf{BTRank}^m_n(A)$. This is because τ must be consistently extended to the u-variables by $\tau(u_{i,j,k}) = \sum_{\ell \in [k]} \tau(z_{i,j,\ell})$, and the column index k of $u_{i,j,k}$ is not particularly relevant here: when τ is applied to a product of multiple u-variables mentioning a small number of columns, it leads to a blow up in the X-mentioned columns in the resulting terms. Our notion of degree for the u-variables concerns the first of the three indices of $u_{i,j,k}$. We say that i is *U-left-row-mentioned* in a term t if $u^b_{i,j,k}$ appears in t for some $j \in [m]$, $k \in [n]$, and $b \in \{0,1\}$.

To appreciate this definition, let us first calculate $\tau(u^{1-b}_{i,j,k})$ modulo the hole axioms. We have

$$\tau(u^{1-b}_{i,j,k}) = b + \tau(u_{i,j,k}) = b + \sum_{\ell \in [k]} \tau(z_{i,j,\ell}) = b + \sum_{\ell \in [k]} \tau(x_{i,\ell})\tau(y_{\ell,j}) = b + \sum_{\ell \in [k]} x_{i,\ell} \sum_{i' \in [m]} x_{i',\ell}A_{i',j}$$
$$= b + \sum_{\ell \in [k]} \sum_{i' \in [m]} x_{i,\ell}x_{i',\ell}A_{i',j} = b + \sum_{\ell \in [k]} x_{i,\ell}x_{i,\ell}A_{i,j} = b + A_{i,j} \sum_{\ell \in [k]} x_{i,\ell}.$$

We see that, modulo the hole axioms, the only remaining row index is i. Let t be a term consisting of u-variables and their negations and let R be the set of indices U-left-row-mentioned in t. Based on the above calculation, we observe that each term t' of the polynomial $\tau(t)$ either has degree at most $|R|$, or is a multiple of a hole axiom, or (by the pigeonhole principle) is a multiple of a functionality axiom of FPHP^m_n.

The preceding discussion motivates the definition of the relaxed degree of a general term t in the variables of $\mathsf{BTRank}^m_n(A)$ as the sum of the cardinality of the set of indices U-left-row-mentioned in t and the cardinality of the set of X-, Y^T- or Z-mentioned columns in t. For a precise definition of random self-reductions and a proof of their effectiveness in reducing the relaxed degree, we refer the reader to the proof of Theorem 5.19.

Iterated rank principles. In order to address the iterated variants of the rank principle, we need additional techniques besides the ones that were sufficient for Theorem 2.1. We start by describing the ideas behind the iterated algebraic principle. We consider the classical Goldwasser, Goldreich and Micali [32] iteration protocol, which was also used in [73]. This protocol achieves a generator with exponential stretch (i.e., a function generator) by iterating the base generators (the way to

achieve such a function generator from the weak rank principle is described after Theorem 2.8 in this section).

Let π be a binary string of length at most κ and consider the polynomial system $\mathsf{IRank}_n^m(\{A^{(\pi)}\}, \kappa) = \bigcup_{\pi \in \{0,1\}^{\leq \kappa}} X^{(\pi)}Y = A^{(\pi)}$. Here, each $X^{(\pi)}Y = A^{(\pi)}$ is an instance of the weak rank principle, except that the matrices $A^{(\pi)}$ are not necessarily constant: we also allow them to contain the variables from $X^{(\pi')}$ for some $|\pi'| > |\pi|$. Letting "()" be the empty string, these copies of Rank are naturally arranged in a binary tree as shown in Figure 2.

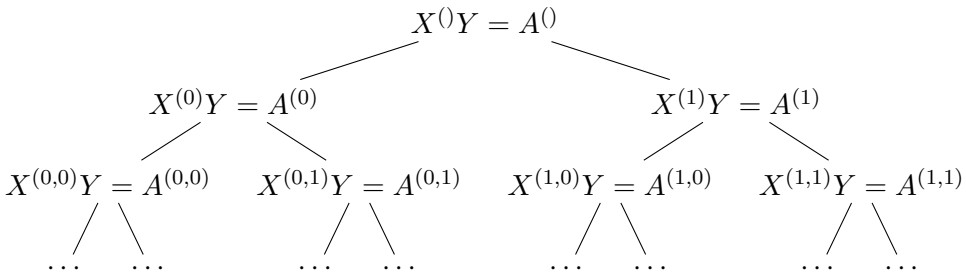


Figure 2: Iteration structure of IRank.

In this tree, the entries of each matrix $A^{(\pi)}$ can depend only on the entries of $X^{(\pi')}$ from the layers below. This differs from the standard notion of s-iterability, which only assumes a flat structure; that is, the iterated copies are arranged as a path and not as a tree. We need to use a tree structure to maximise the stretch versus the iteration depth ratio, since our lower bound depends on the depth of the tree (that is, on κ in the above notation). The tree structure was also used by Razborov [73]. Nevertheless, this construction turns out to be sufficient for applications to circuit lower bounds statements. Our goal would be to show that any refutation of IRank with parameters m and n requires size $2^{(n/\kappa)^{\Omega(1)}}$.

We consider two notions of degree for IRank:

- the *column degree*, which measures the number of different columns of $X^{(\pi)}$ or Y^T the term mentions, where the same columns from different matrices are counted at most *once*; and
- the *row degree*, which measures the number of different rows of $X^{(\pi)}$ or Y^T the term mentions, where the same rows from different matrices *are counted individually*.

For example, the term $x^{(0)}_{1,1}x^{(1)}_{1,1}y_{1,1}$ has column degree 1 and row-degree 3. We perform two random self-reductions ρ and σ. The former reduces the row degree of every term in a refutation to $\leq d$ while the latter reduces the column degree to $\leq d$. This implies the total degree does not exceed $2d^2$. We show that $\mathsf{IRank}_n^m(A^{(\pi)}, \kappa)$ requires degree $n/2$ by reducing it to one copy of the formula $\mathsf{Rank}_n^m(I_m)$ using a reduction that substitutes each $X^{(\pi)}$ with $A^{(\pi)}X$ for a new variable X. Since the entries of $A^{(\pi)}$ are not necessarily constant, this reduction can increase the degree of a refutation. However, it can grow by at most a factor of $\kappa + 1$, because for each copy the degree grows by at most 1. This explains the dependency on κ we mentioned earlier.

We now turn to the CNF encoding of $\bigcup_{\pi \in \{0,1\}^{\leq \kappa}} X^{(\pi)}Y^{(\pi)} = A^{(\pi)}$ (note that here the matrix Y is different in each iteration, unlike before) and again use the iterated protocol from [32]. We encode $\bigcup_{\pi \in \{0,1\}^{\leq \kappa}} X^{(\pi)}Y^{(\pi)} = A^{(\pi)}$ using the extension variables that are similar to the ones from BTRank and additionally impose some structure on the matrices $Y^{(\pi)}$. Our goal is again to prove that any $\mathsf{PCR}_{\mathbb{F}_2}$ refutation requires size $2^{(n/\kappa)^{\Omega(1)}}$.

The notion of column degree is not well suited for the extension variables. For instance, given an extension variable $u^{(\pi)}_{i,j,k}$ which semantically encodes the sum $\sum_{\ell \in [k]} x^{(\pi)}_{i,k} y^{(\pi)}_{k,j}$, it is clear that it depends not only on the kth column but also on the preceding columns $\{1, \ldots, k-1\}$. To address this, we restrict our matrices $Y^{(\pi)}$ (and hence the extension variables) to a bipartite expander G with a small left-degree Δ. This automatically restricts the column degree of all but x-variables to be at most Δ, thus for all extension variables we only need to reduce the row degree.

Overall, the proof strategy is executed as follows: we start by reducing the row-degree (and thus the total degree) in u-variables that compute partial inner products. We then reduce the column degree in the x- and z-variables (recall that the latter compute the binary ANDs: $z^{(\pi)}_{i,j,k} = x^{(\pi)}_{i,k} y^{(\pi)}_{k,j}$). This is performed in the same way as in the algebraic construction. Finally, we reduce the row degree in the x-, y-, and z-variables by using a random substitution similar to the one that reduces the row degree for IRank. To deal with the z-variables we need to further modify the refutation. This is because of the terms of the form $s = \prod_{j \in J} \overline{z}_{i_0,j,k}$ (or of the symmetric form $\prod_{I \in J} \overline{z}_{i,j_0,k}$), which have the shape of a *star* (when the x- and y-variables are considered as two sides of a bipartite graph with an edge between $x^{(\pi)}_{i,k}$ and $y^{(\pi)}_{k,j}$ present whenever $\overline{z}^{(\pi)}_{i,j,k}$ appears in s). Such stars have common centre i_0, and our substitutions do not, in fact, set them to 0 w.h.p. However, we can show that each such a star with sufficiently many rays—that is, with large enough set J—collapses to its centre $\overline{x}_{i_0,k}$ w.h.p. This property limits the degree of all such star terms. For the rest of the variables, we can greedily identify a large set of variables in a term that are independently set to 0 w.h.p., implying that such a term vanishes from the proof w.h.p.

2.2 Generators for Sherali–Adams

We address the problem of establishing proof complexity generators for the Sherali-Adams (SA) semi-algebraic refutation system [25].

First, note that the Nisan generator construction, denoted $\tau(A, b)$ in [73], can be shown to work also for SA and even SoS. Specifically, its hardness follows from the lower bound on the *Gaussian width* of $\tau(A, b)$ as introduced in [14], and whose lower bound against SoS was established in [33,74]. Combined with the random restriction from Razborov [73], this gives an SA size lower bound for $\tau(A, b)$.

We provide a different generator for SA than Razborov's by proving that our bamboo-tree encoding of WRank is such a generator. Note that WPHP is easy for SA in terms of size. Therefore, WPHP cannot be directly used as a generator. We thus come up with a new technique that does not use the reduction to PHP and instead defines a relaxed notion of degree (row degree, in our case). The lower bounds are thus based on a reduction from size to row degree, followed by a lower bound on row degree. To establish the row degree lower bound we come up with a pseudoexpectation based on a new family of distributions tailored to WRank (and not to WPHP).

Lemma 2.5 (Row degree lower bound for SA (informal); Lemma 6.4)**.** *For every $m > n$ and every $A \in \{0,1\}^{m \times m}$, every SA refutation of (a variant of) $\mathsf{BTRank}^m_n(A)$ requires row degree $n - 1$.*

Theorem 2.6 (Size lower bound for SA (informal); see Theorem 6.8)**.** *Assume $m > n$ and $A \in \{0,1\}^{m \times m}$ is a Boolean matrix. Then any SA refutation of (a variant of) $\mathsf{BTRank}^m_n(A)$ requires size $2^{\Omega(n)}$.*

This result fits in the generator approach to proof complexity as stated by Razborov [73, p. 417] and proposed earlier by Krajíček [49, 50] and Alekhnovich *et al.* [4]. Specifically, the *generator approach* seeks to establish proof complexity generators for as many proof systems as possible, roughly based on the computational hardness of the generator.

To rule out low row-degree SA refutations of $\mathsf{BTRank}^m_n(A)$, we define a family of distributions over partial assignments. Each distribution in this family is indexed by a pair (I, J), where $I \subseteq [m]$ and $J \subseteq [m]$ are sets of row indices of X and Y^T, respectively, with $|I|+|J| \leq n-2$. The distribution corresponding to (I, J) is the uniform distribution supported on certain assignments to all variables $x_{i,k}$ with $i \in I, k \in [n]$ and $y_{\ell,j}$ with $\ell \in [n], j \in J$.

Before specifying these assignments, it is helpful to recall the family of distributions used against the functional pigeonhole principle FPHP^m_n by [26]. Each distribution in that family is indexed by a set $I \subseteq [m]$ of at most $n - 2$ pigeons and consists of the uniform distribution over all matchings of the pigeons in I to holes. Thus, the distribution indexed by I is supported on all assignments to the variables $x_{i,k} : i \in I, k \in [n]$ that do not violate any axiom of FPHP^m_n. In other words, no condition whatsoever limits these assignments except the axioms involving the pigeons in I.

In contrast, for $\mathsf{BTRank}_n^m(A)$, we cannot allow similar freedom in the supports of the distributions in our family. It is straightforward to verify that if the support consisted of all assignments to $x_{i,k} : i \in I, k \in [n]$ and $y_{\ell,j} : \ell \in [n], j \in J$ that do not violate any axiom of $\mathsf{BTRank}_n^m(A)$, the marginal distribution condition—a key ingredient of SA lower bounds[3]—would fail. In other words, limiting the support only by the requirement that the axioms concerning $A_{I,J}$ (the submatrix of A determined by rows I and columns J) hold is insufficient. Our approach therefore imposes stronger restrictions on the support than those dictated by the axioms of $\mathsf{BTRank}_n^m(A)$ alone.

Specifically, we require that the row vectors assigned to the rows of X indexed by I be linearly independent, that the column vectors assigned to the columns of Y indexed by J form a linearly independent set of vectors, and that the product of these rows and columns evaluates to $A_{I,J}$. Of these three requirements, only the last is directly dictated by the axioms of $\mathsf{BTRank}_n^m(A)$. We show that the uniform distribution over such assignments satisfies the marginal distribution conditions for members of our family. Notably, these assignments violate the FPHP_n^m axioms even in the special case $A = I_m$ and $Y = X^T$ (the oddtown case $XX^T = I_m$), highlighting the bespoke nature of our distribution family.

It is plausible that our method could be extended to the case of SoS, though we have not pursued this direction.

2.3 Hardness of Circuit Lower Bounds from the Weak Rank Principle

Next, we connect the weak rank principle to the provability of circuit lower bounds. We show that the weak rank principle is *necessary* for proving certain circuit lower bound statements, while in the sequel (Section 2.4) we show that it is also *sufficient* for proving some known circuit lower bounds of interest. These results suggest a fundamental relationship between the weak rank principle and the provability of circuit lower bounds.

Our results are inspired by—and, to some extent, mirror—the connection between the weak pigeonhole principles and the provability of complexity lower bounds. Razborov [69,72] and Raz [65] showed the unprovability of circuit lower bounds such as $\mathsf{NP} \not\subseteq \mathsf{P/poly}$ in weak proof systems via reductions from WPHP. Müller and Pich [57] formalised a wide range of circuit lower bounds in Jeřábek's theory for approximate counting in bounded arithmetic [42–44], which includes the dual weak pigeonhole principle as an axiom. More recently, Chen, Li, and Oliveira [18] showed that certain lower bound statements are *equivalent* to variants of weak pigeonhole principles.

We extend the above line of research in two aspects. First, we present low-degree reductions from the weak rank principle to circuit lower bound sentences, generalising the aforementioned connections by Razborov and Raz [65, 69, 72]. Then, as a concrete example, we show that $\mathsf{PCR}_{\mathbb{F}_2}$ does not have efficient proofs of circuit lower bound statements such as $\mathsf{NP} \not\subseteq \mathsf{P/poly}$, by *iterating* the WRank-based proof complexity generators against $\mathsf{PCR}_{\mathbb{F}_2}$ (as in [73]). A variant of circuit lower bound statements was recently proved to be hard for SoS [10].

Necessity of the weak rank principle. First, we present low-degree reductions showing that WRank is necessary for proving circuit lower bounds:

Theorem 2.7 (WRank is necessary for Boolean circuit lower bounds (informal); see Corollary 8.4 and Remark 8.5)**.** *Let $\mathcal{P}$ be an algebraic proof system closed under low-degree reductions. If $\mathcal{P}$ cannot prove the weak rank principle efficiently, then for every Boolean function f (represented as a truth table), $\mathcal{P}$ cannot prove circuit lower bounds for f efficiently.*

Interestingly, our argument goes through algebraic circuit complexity. Specifically, we show that WRank is necessary for proving lower bounds against non-commutative algebraic branching programs (non-commutative ABPs, or ncABPs for short), which is a fairly weak algebraic circuit model (making our *unprovability* results stronger). Our reduction relies on Nisan's characterisation

[3] In our case, the marginal distribution condition says that marginalising the distribution indexed by $(I \cup \{i_0\}, J)$ to the variables $x_{i,k} : i \in I, k \in [n]$ and $y_{\ell,j} : \ell \in [n], j \in J$ coincides with the distribution indexed by (I, J), and similarly for the distribution indexed by $(I, J \cup \{j_0\})$.

of ncABP complexity via matrix rank [58]. We then establish that lower bounds on ncABP complexity are themselves necessary for proving lower bounds on (Boolean) circuit complexity.

Concrete lower bounds. Inspired by the above connection, we use the generators for $\mathsf{PCR}_{\mathbb{F}_2}$ demonstrated in Section 2.1 to show that this system cannot efficiently prove circuit lower bounds[4].

Theorem 2.8 (Informal; see Theorem 8.9)**.** *Let $f\colon \{0,1\}^n \to \{0,1\}$. There exists a constant $c \geq 1$ such that for every $s > n^c$, any $\mathsf{PCR}_{\mathbb{F}_2}$ refutation of the statement "f cannot be computed by Boolean circuits of size s" (encoded as a system of polynomial equations) requires size $2^{n^{\Omega(1)}}$.*

As in the case of Razborov [73] our Boolean circuits are in the basis $\neg, \wedge, \vee, \oplus$ where the last three connectives are binary. The proof idea is similar to [73]. We work with the iterated rank principle $\bigcup_{\pi\in\{0,1\}^{\leq n}} X^{(\pi)}Y^{(\pi)} = A^{(\pi)}$ encoded as a CNF using the bamboo-tree encoding. Given $\pi \in \{0,1\}^n$, we choose the matrices $A^{(\pi)}$ such that $A^{(\pi)}_{1,1} = f(\pi)$ the rest of the matrices (for $|\pi| < n$) are arranged as $A^{(\pi)} = \begin{bmatrix} X^{(\pi*0)} & X^{(\pi*1)} & Y^{(\pi*0)^T} & Y^{(\pi*1)^T} \end{bmatrix}$. That is, given a copy $X^{(\pi)}Y^{(\pi)} = A^{(\pi)}$, we can compute both copies $X^{(\pi*0)}Y^{(\pi*0)} = A^{(\pi*0)}$ and $X^{(\pi*1)}Y^{(\pi*1)} = A^{(\pi*1)}$ recursively. This way, starting with the empty string "()", we can gradually compute $A^{(\pi)}$ for $\pi \in \{0,1\}^n$, thus obtaining $f(\pi)$. This computation can be naturally expressed as a Boolean circuit, using the gates that correspond to the extension variables.

2.4 On the Strength of WRank

Finally, we initiate the study of the weak rank principle as an axiom in bounded arithmetic. Linear algebra is used extensively throughout combinatorics and complexity theory, resulting in a variety of breakthroughs such as the resolution of the finite field Kakeya conjecture [29], Cap Set problem [24, 30] and the Sensitivity Conjecture [38]. Indeed, there is a whole book dedicated to linear algebraic methods in combinatorics [11].

Soltys and Cook [77] initiated the study of formal theories that "capture linear algebra" from the complexity perspective. Specifically, they considered a few formal theories for linear algebraic reasoning and showed that $\forall\mathsf{LAP}$, the strongest theory considered in [77] which incorporates matrix powering and certain induction schema, proves many linear algebraic identities including the (strong) rank principle. Subsequently, Tzameret and Cook [81] showed that the seemingly weaker theory VNC^2 suffices for linear algebraic reasoning and specifically proving properties of the determinant. We take a somewhat similar route, but instead of powerful concepts such as matrix powering (which is DET-complete [21] and hence intuitively captures "full" linear algebra), we only consider the *weak* rank principle, hence our theories appear to be somewhat weaker.

An important motivation for considering the *weak* rank principle is that they capture arguments in combinatorics and complexity theory that are "*loose*" (i.e., not tight). Intuitively, the *weak* rank principle should already suffice when one is satisfied with a bound that is only tight within multiplicative factors. This is the case when we are satisfied with, say, a bound of $c \cdot 2.756^n$ for the Cap Set problem or a bound of $c \cdot 2^{n^{1/2d}}$ for $\mathsf{AC}^0[p]$ circuit complexity, where $c > 0$ is an unspecified constant. This is similar to the case of approximate counting where we only care about the sizes of sets *approximately*, hence the *weak* pigeonhole principle is already applicable [44].

In this work, we put forward a theory $\overline{\mathbf{V}^0(p)} + \mathrm{WRank}_p$, which incorporates the two-sorted theory $\overline{\mathbf{V}^0(p)}$ in the style of Cook–Nguyen [20] with an extra axiom WRank_p expressing the weak rank principle over $\mathbb{F}_p$. We demonstrate the power of the weak rank principle and confirm the above intuition by showing that this theory can prove Smolensky's circuit lower bound against $\mathsf{AC}^0[p]$ [75]:

Theorem 2.9 (Informal)**.** *For every prime number $p > 2$, $\overline{\mathbf{V}^0(p)} + \mathrm{WRank}_p$ proves that MOD_2 cannot be computed by $\mathsf{AC}^0[p]$ circuits of depth d and size $2^{o(n^{1/(2d)})}$.*

[4] Unfortunately, when measured by *size*, $\mathsf{PCR}_{\mathbb{F}_2}$ is not closed under low-degree reductions. Hence our concrete lower bounds are not direct corollaries of Theorem 2.7 and requires more work.

Previously, Müller and Pich [57] formalised Smolensky's $\mathsf{AC}^0[p]$ lower bounds in Jeřábek's theory $\mathbf{APC}_1$ [42, 44]. The difference between our formalisation and theirs will be discussed in Remark 9.13, at the end of Section 9.2.2. We also note that Razborov mentioned in [68, Section E.3] that the metamathematics of Razborov–Smolensky lower bounds are left open. Our work addresses this gap by showing that Smolensky's lower bounds can be proved in $\overline{\mathbf{V}^0(p)} + \mathrm{WRank}_p$. In addition, Galesi *et al.* [31] considered the rank principle with $A = I$ as an axiom added to the polynomial calculus.

3 Conclusions and Open Problems

Our work introduces the weak rank principle as a new object of study in proof complexity and applies it to advance the *generator approach* to proof complexity, introduced by Krajíček [49,50] and Alekhnovich *et al.* [4], and later emphasized by Razborov [73, p. 417]. The goal of this approach is to construct *proof-complexity generators* for as many proof systems as possible, where the hardness of the generator reflects the computational limitations of the corresponding system. In our case, the hardness originates from linear-algebraic reasoning: the weak rank principle expresses the unsatisfiability of certain linear systems and matrix identities, and its difficulty is directly tied to the inability of a proof system to efficiently formalize arguments involving matrix rank. Consequently, the weak rank principle is expected to be hard for proof systems that cannot efficiently reason about linear algebra.

Future directions. Several directions appear promising for further study:

- The weak rank principle provides a useful family of tautologies to study in proof systems for which the pigeonhole principle is easy or for which no proof-complexity generators are known. The basic instance, $XY = I$, already gives a concrete candidate for proving lower bounds. Obtaining a lower bound for this instance is the first step toward establishing lower bounds for the more general case $XY = A$, where A ranges over matrices of rank greater than n. Such results would yield a proof-complexity generator based on WRank. Once such a base generator is obtained, it can be iterated to obtain a *function generator*, showing that the proof system in question cannot efficiently prove certain complexity-class separations such as $\mathsf{NP} \not\subseteq \mathsf{P/poly}$.
- Develop bounded arithmetic theories that use WRank as axioms, such as the theory $\overline{\mathbf{V}^0(p)} + \mathrm{WRank}_p$ developed in this paper. We speculate that many interesting results in combinatorics and complexity theory can be formalised in such theories and that the *weak* rank principles suffice. Our formalisation of Smolensky's lower bounds [75] can be seen as the first step towards this goal.
- The weak rank principle provides a natural candidate for lower bounds against $\mathsf{AC}^0[p]$-Frege (for which no lower bounds are currently known) and SoS. This connection follows from the conjecture that NC^2 captures the computational complexity of linear algebra. According to the informal correspondence between circuit classes and propositional proof systems whose proof-lines come from those classes, one expects that proofs operating with NC^2-circuits (that is, NC^2-Frege) are exactly those capable of efficiently reasoning about rank-based arguments. In contrast, the weak pigeonhole principle admits quasipolynomial-size proofs already in $\mathsf{Res}(\log n)$ and thus in AC^0-Frege [54, 61], indicating that stronger algebraic principles are required to obtain meaningful lower bounds.

4 Preliminaries

We will use the following common notations throughout the paper.

- For all $k > 0$, I_k denotes the $k \times k$ identity matrix $(I_k)_{i,j} = \delta_{i,j}$ for all $i, j \in [k]$.
- For all $k, \ell > 0$, $J_{k,\ell}$ denotes the $k \times \ell$ all-one matrix, i.e., $(J_{k,\ell})_{i,j} = 1$ for all $i \in [k], j \in [\ell]$.

4.1 Proof Systems

Let TAUT denote the coNP-complete set of propositional tautologies. Cook and Reckhow [23] defined *propositional proof systems* as nondeterministic algorithms for TAUT. Equivalently, a propositional proof system $\mathcal{P}(\varphi, \pi)$ is a deterministic algorithm that takes as inputs a propositional formula φ and a purported proof π, and satisfies the following properties:

- **Completeness:** If $\varphi \in \mathsf{TAUT}$, then there exists a proof π such that $\mathcal{P}(\varphi, \pi)$ accepts.
- **Soundness:** If $\varphi \notin \mathsf{TAUT}$, then for every π, $\mathcal{P}(\varphi, \pi)$ rejects.
- **Efficiency:** $\mathcal{P}$ runs in time polynomial in $|\varphi| + |\pi|$.

A propositional proof system $\mathcal{P}$ is *polynomially bounded* (or *p-bounded*) if there is a polynomial $p(\cdot)$ such that every tautology $\varphi \in \mathsf{TAUT}$ admits a proof π of length at most $p(|\varphi|)$ for which $\mathcal{P}(\varphi, \pi)$ accepts. Cook and Reckhow [23] showed that p-bounded propositional proof systems exist if and only if $\mathsf{NP} = \mathsf{coNP}$.

Sometimes we will equivalently consider *refutation* systems, which are nondeterministic algorithms for the language $\overline{\mathsf{SAT}}$. A DNF F is a tautology if and only if $\neg F$ (which can be expressed as a CNF) is unsatisfiable. Thus a *proof* of F can be equivalently viewed as a *refutation* of $\neg F$.

While traditional proof systems reason about Boolean formulas, *algebraic proof systems* reason about the unsatisfiability of collections of *polynomial equations*. Fix an underlying field $\mathbb{F}$, and let $f_1, f_2, \ldots, f_m \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ be a collection of polynomials, where each f_i is called an *axiom* and means $f_i(\vec{x}) = 0$. The goal is to prove that these polynomials do not have a common zero over $\mathbb{F}^n$. It is standard in the literature to add the *Boolean axioms* $x_i^2 - x_i$ into the collection to enforce that all variables take values in $\{0, 1\}$; however we do *not* include these Boolean axioms in our definition of rank principles.

For a polynomial f, let $\|f\|$ denote the number of monomials appearing with a nonzero coefficient in f.

Definition 4.1. Let $F = (f_1, f_2, \ldots, f_m)$ be an unsatisfiable collection of polynomial equations over a field $\mathbb{F}$.

- A *Nullstellensatz* ($\mathsf{NS}_{\mathbb{F}}$) [13] refutation of F is a sequence of polynomials $(g_1, g_2, \ldots, g_m)$ such that the following polynomial identity holds.

$$\sum_{i=1}^{m} f_i \cdot g_i = 1.$$

  The *degree* of the refutation is $\max_{i \in [m]}\{\deg(f_i \cdot g_i)\}$. The *size* of the refutation is $\sum_{i=1}^{m} \|f_i\| \cdot \|g_i\|$.

- *Polynomial Calculus* ($\mathsf{PC}_{\mathbb{F}}$) [19] is a dynamic proof system where proof lines are polynomials over $\mathbb{F}$. Starting from $(f_1, f_2, \ldots, f_m)$ as axioms, this system has two inference rules:

$$\frac{f \qquad g}{\alpha f + \beta g} \text{ (for } \alpha, \beta \in \mathbb{F}) \quad \text{and} \quad \frac{f}{x_i \cdot f}.$$

  A $\mathsf{PC}_{\mathbb{F}}$ *refutation* of F is a derivation of 1 from F. The *degree* of the refutation is the maximum degree of any polynomial appearing in it. The *size* of the refutation is the total number of monomials appearing in it.

- Suppose $\mathbb{F} = \mathbb{R}$. A *Sum-Of-Squares* (SoS) refutation of F is a sequence of polynomials $(g_1, g_2, \ldots, g_m)$ and $(h_1, h_2, \ldots, h_\ell)$ such that the following polynomial identity holds.

$$\sum_{i=1}^{m} f_i \cdot g_i + \sum_{j=1}^{\ell} h_j^2 = 1.$$

The *degree* of the refutation is the maximum over $\max_{i\in[m]}\{\deg(f_i \cdot g_i)\}$ and $2\max_{j\in[\ell]}\{\deg(h_j)\}$. The *size* of the refutation is $\sum_{i\in[m]} \|f_i\| \cdot \|g_i\| + \sum_{j\in[\ell]} \|h_j\|$.

Definition 4.2. Let $F = (f_1, f_2, \ldots, f_m)$ be an unsatisfiable collection of polynomial equations over $\mathbb{R}$. We enforce the variables $x_1, x_2, \ldots, x_n$ to be Boolean by adding every Boolean axiom $x_i^2 - x_i$ in F. A *Sherali–Adams* (SA) [25] refutation of F is a sequence of polynomials $(g_1, g_2, \ldots, g_m)$ and a conical junta $\mathcal{J}$ such that the following polynomial identity holds.

$$\sum_{i\in[m]} f_i \cdot g_i + \mathcal{J} = 1.$$

Here, $\mathcal{J}$ is a *conical junta* if it is a nonnegative linear combination of terms ($\mathcal{J} = \sum_j^\ell \alpha_j t_j(x)$ for $\alpha_j > 0$), and each term is a product of some x_i's and some $(1 - x_j)$'s. The *degree* of the refutation is the maximum of $\deg(\mathcal{J})$ and $\max_i\{\deg(f_i) + \deg(g_i)\}$. The *size* of the refutation is $\sum_{i\in[m]} \|f_i\| \cdot \|g_i\| + \ell$.

Definition 4.3. Let $F = (f_1, f_2, \ldots, f_m)$ be an unsatisfiable collection of polynomial equations over a field $\mathbb{F}$ with underlying variables $x_1, x_2, \ldots, x_n$. We enforce the variables to be Boolean by adding every Boolean axiom $x_i^2 - x_i$ in F. A *Polynomial Calculus Resolution* ($\mathsf{PCR}_\mathbb{F}$) [3] refutation of F is a $\mathsf{PC}_\mathbb{F}$ refutation of F', where F' is F with the *twin variables* $\overline{x}_1, \overline{x}_2, \ldots, \overline{x}_n$ and the axioms $1 - x_i - \overline{x}_i$ and $\overline{x}_i^2 - \overline{x}_i$ added.

Note that $\mathsf{PC}_\mathbb{F}$ and $\mathsf{PCR}_\mathbb{F}$ are equivalent w.r.t. the degree measure, but a collection of polynomial equations might have much more efficient $\mathsf{PCR}_\mathbb{F}$ proofs than $\mathsf{PC}_\mathbb{F}$ proofs in terms of size.

4.2 Substitutions

In the proof complexity setting, substitutions are usually defined as follows.

Definition 4.4. Given variables $(x_1, \ldots, x_n)$ and their twins $(\overline{x}_1, \ldots, \overline{x}_n)$, the *restriction* ρ is a partial mapping from $\{x_1 \ldots, x_n\} \cup \{\overline{x}_1, \ldots, \overline{x}_n\}$ to $\{0, 1\}$.

Here we consider a generalised notion of substitutions, when we can substitute variables with new fresh variables.

Definition 4.5. Given variables $(x_1, \ldots, x_n)$ and $(y_1, \ldots, y_m)$ and their twins $(\overline{x}_1, \ldots, \overline{x}_n)$ and $(\overline{y}_1, \ldots, \overline{y}_m)$, the *restriction* ρ is a mapping from $\{x_1 \ldots, x_n\} \cup \{\overline{x}_1, \ldots, \overline{x}_n\}$ to $\{0, 1\} \cup \{y_1 \ldots, y_m\} \cup \{\overline{y}_1, \ldots, \overline{y}_m\}$, which is consistent w.r.t. the twin variables: if $\rho(v) = b$ for some $b \in \{0, 1\}$, then $\rho(\overline{v} = 1 - b)$; if $\rho(v) = u$ for some variable u, then $\rho(\overline{v}) = \overline{u}$.

It coincides with the standard definition when $(y_1, \ldots, y_m) = (x_1, \ldots, x_n)$ and for every v with $\rho(v) \notin \{0, 1\}$, $f(v) = v$.

Given a polynomial $f \in \mathbb{F}[x_1, \ldots, x_n, \overline{x}_1, \ldots, \overline{x}_n]$ and a restriction ρ, the application of ρ to f, denoted $f \restriction \rho$ is the polynomial $g(y_1, \ldots y_m, \overline{y}_1, \ldots, \overline{y}_m) = f(\rho(x_1), \ldots, \rho(x_n), \rho(\overline{x}_1), \ldots, \rho(\overline{x}_n))$.

Given a proof Π (a sequence of polynomial), the application of a restriction ρ to Π, denoted $\Pi \restriction \rho$, is obtained by applying the $p \restriction \rho$ to each line p of Π and removing any line that becomes the zero polynomial

4.3 Reductions in Proof Complexity

Let F and G be two collections of polynomial equations. In this paper, we use *low-degree algebraic reductions* [17, 27] to formalise the idea that F is "easier" to prove than G. Intuitively, this happens when F is a substitution instance of G, namely there is a substitution to G under which G equals F; or more precisely, there is a substitution R to G, such that there is an efficient (e.g. low degree) derivation from F of the substitution instance $G \circ R$. Hence, a short proof of $G \circ R$ is also a short proof of F. For example, to show that *circuit lower bounds* are as hard to prove as *the weak rank principle*, we exhibit a low-degree reduction from the polynomial equations encoding the weak rank principle to those encoding circuit lower bounds.

Definition 4.6 (Algebraic reductions; [27, Def. 8.2])**.** Let $F = (f_1, \ldots, f_m)$ be a collection of polynomials over variables $(x_1, \ldots, x_m)$, and $G = (g_1, \ldots, g_n)$ be a collection of polynomials over variables $(y_1, \ldots, y_{n'})$. A *degree-d algebraic reduction* (denoted as $F \leq_d^{\text{alg}} G$) consists of the following:

(Reduction) a mapping $R : \mathbb{F}^{m'} \to \mathbb{F}^{n'}$ such that each output element $R_i \in \mathbb{F}[x_1, \ldots, x_{m'}]$, $i \in [n]$, is a degree-d polynomial in $(x_1, \ldots, x_{m'})$;

(Axioms) for every $i \in [n]$, the polynomial $g_i \circ R$ has an $\mathsf{NS}_{\mathbb{F}}$-proof from F of degree $d \cdot \deg(g_i)$. That is, there exist polynomials $(q_{i,1}, \ldots, q_{i,m})$ such that

$$g_i \circ R = \sum_{k=1}^{m} f_k q_{i,k},$$

and for every $k \in [m]$, $\deg(f_k) + \deg(q_{i,k}) \leq d \cdot \deg(g_i)$.

It is a standard and useful fact that algebraic reductions are closed under composition.

Fact 4.7. *Let $F = (f_1, \ldots, f_m)$, $G = (g_1, \ldots, g_n)$, and $H = (h_1, \ldots, h_\ell)$ be systems of polynomial equations. If $F \leq_{d_1}^{\text{alg}} G$, $G \leq_{d_2}^{\text{alg}} H$, then $F \leq_{d_1 d_2}^{\text{alg}} H$.*

Proof. Suppose that F is over variables $(x_1, \ldots, x_{m'})$, G is over variables $(y_1, \ldots, y_{n'})$, and H is over variables $(z_1, \ldots, z_{\ell'})$. Let $R^1 : \mathbb{F}^{m'} \to \mathbb{F}^{n'}$ be a degree-d_1 reduction from F to G and $R^2 : \mathbb{F}^{n'} \to \mathbb{F}^{\ell'}$ be a degree-d_2 reduction from G to H. We claim that $R^2 \circ R^1 : \mathbb{F}^{m'} \to \mathbb{F}^{\ell'}$ is a degree-$d_1 d_2$ reduction from F to H. Clearly, every output element of $R^2 \circ R^1$ is a degree-$d_1 d_2$ polynomial over its variables (i.e., $(x_1, \ldots, x_{m'})$).

Now consider some axiom h_i in H, we want to show that $h_i \circ R^2 \circ R^1$ has an NS-proof from F of degree $d_1 d_2 \cdot \deg(h_i)$. We have

$$h_i \circ R^2 = \sum_{k=1}^{n} g_k q_{i,k}$$

for some polynomials $(q_{i,1}, \ldots, q_{i,n})$ such that for every $k \in [n]$, $\deg(g_k) + \deg(q_{i,k}) \leq d_2 \cdot \deg(h_i)$. For each $k \in [n]$, we also have

$$g_k \circ R^1 = \sum_{j=1}^{m} f_j p_{k,j}$$

for some polynomials $(p_{k,1}, \ldots, p_{k,m})$ such that for every $j \in [m]$, $\deg(f_j) + \deg(p_{k,j}) \leq d_1 \cdot \deg(g_k)$. Hence

$$h_i \circ R^2 \circ R^1 = \sum_{k=1}^{n} (g_k \circ R^1)(q_{i,k} \circ R^1) = \sum_{j=1}^{m} f_j \cdot \underbrace{\left(\sum_{k=1}^{n} p_{k,j} \cdot (q_{ik} \circ R^1) \right)}_{r_{i,j}}. \tag{2}$$

Note that $\deg(f_j) + \deg(r_{i,j}) = \max_k \{\deg(f_j) + \deg(p_{k,j}) + \deg(q_{i,k}) \cdot d_1\} \leq \max_k \{d_1 \cdot (\deg(g_k) + \deg(q_{i,k}))\} \leq d_1 d_2 \cdot \deg(h_i)$. Hence, (2) is an NS-proof of $h_i \circ R^2 \circ R^1$ from F that has degree $d_1 d_2 \cdot \deg(h_i)$.

In conclusion, $R^2 \circ R^1$ is a degree-$d_1 d_2$ reduction from F to H. □

Algebraic proof systems such as Nullstellensatz and Polynomial Calculus are closed under low-degree algebraic reductions when the efficiency measure is degree [27, Lemma 8.3]. This paper exhibits many low-degree algebraic reductions; for example, Corollary 8.4 showed a low-degree algebraic reduction from the weak rank principles to circuit lower bound statements. Such a result can be interpreted as: for any algebraic proof system $\mathcal{P}$ closed under low-degree algebraic reductions, if $\mathcal{P}$ cannot prove the weak rank principles, then $\mathcal{P}$ cannot prove any circuit lower bounds.

4.4 The Pigeonhole Principle

We define the *algebraic* encoding of the pigeonhole principle, first considered by Razborov in [69]—this version is sometimes called the *functional pigeonhole principle* because of the Functionality Axioms below. Fix positive integer parameters m and n with $m > n$. FPHP_n^m is defined over mn variables arranged as a Boolean matrix $X \in (x_{i,k})_{i\in[m],k\in[n]}$. It consists of the following polynomial equations:

Pigeon Axioms: For $i \in [m]$, the polynomial

$$1 - \sum_{k\in[n]} x_{i,k}. \tag{3}$$

Hole Axioms: For $i, j \in [m], i \neq j, k \in [n]$, the polynomial

$$x_{i,k}x_{j,k}. \tag{4}$$

Functionality Axioms: For $i \in [m], k, \ell \in [n], k \neq \ell$, the polynomial

$$x_{i,k}x_{i,\ell}. \tag{5}$$

Boolean Axioms: For $i \in [m], k \in [n]$, the polynomial

$$x_{i,k}^2 - x_{i,k}. \tag{6}$$

We comment that the standard (non-functional) PHP from m pigeons to n holes is defined the same as FPHP_n^m, only excluding the Functionality Axioms (5).

Razborov [69] proved a $\mathsf{PCR}_{\mathbb{F}}$ degree lower bound on FPHP_n^m for arbitrary $m > n$.

Theorem 4.8 ([69])**.** *For every field $\mathbb{F}$, every $\mathsf{PC}_{\mathbb{F}}$ refutation of FPHP_n^m has a term that mentions at least $n/2 + 1$ pigeons and at least $n/2 + 1$ holes.*

Although not stated explicitly, the lower bounds in [69] holds when the refutation is considered modulo the ideal generated by the functional and hole axioms. This implies that every refutation of FPHP_n^m contains a term $\prod_{\nu\in[\ell]} x_{i_\nu,k_\nu}$, where $\ell \geq n/2+1$, all i_ν are distinct and all k_ν are distinct.

There is a similar degree lower bound for SA. It was originally stated for FPHP_n^{n+1}, but exactly the same proof applies to FPHP_n^m.

Theorem 4.9 ([26])**.** *Every SA refutation of FPHP_n^m contains a term that mentions at least $n-1$ pigeons.*

4.5 The Perfect Matching Principle

The perfect matching principle, which we denote by Count_n^2, states that it is possible to find a perfect matching on n elements ([1, 60]). Formally, Count_n^2 is a CNF over the variables $y_{\{k,\ell\}} : \{k, \ell\} \in \binom{[n]}{2}$ that consists of the following axioms, expressing that n elements can be partitioned into a set of pairs $\{k, \ell\} \in \binom{[n]}{2}$ (with each element in $[n]$ appearing in some pair—first axioms below; and each element appearing in at most one pair—second axioms below):

$$\bigvee_{\ell\in[n]\setminus\{k\}} y_{\{k,\ell\}}, \qquad k \in [n],$$

$$\neg y_{\{k,\ell\}} \vee \neg y_{\{k,\ell'\}}, \qquad k \in [n], \ell, \ell' \in [n] \setminus \{k\}, \ell \neq \ell'.$$

When n is odd, it is clear that this formula is unsatisfiable.

4.6 Lossless Expanders

Let G be an $m \times n$ bipartite graph with parts L and R.

Definition 4.10. Given $i \in L$, the *neighbourhood* of i in G, denoted $\mathcal{N}_G(i)$, is the set of all $k \in R$ that are connected to i in G.

Definition 4.11. Given a set $I \subseteq L$, the *boundary* of I, denoted $\partial_G(i)$, is the set of all unique neighbours of I:

$$\partial_G(I) = \{k \in R : \text{there is exactly one } i \in I \text{ satisfying } k \in \mathcal{N}_G(i)\}.$$

Definition 4.12. G is an (r, c)-*boundary expander* if for every set $I \subseteq L$ with $|I| \leq r$, it holds that

$$|\partial_G(I)| \geq c|I|.$$

Definition 4.13. G is an (r, d)-*lossless expander* if for every set $I \subseteq L$ with $|I| \leq r$, it holds that

$$\sum_{i \in I} |\mathcal{N}_G(i)| - |\partial_G(I)| \leq d|I|. \tag{7}$$

This is called a *lossless* expander because the expansion from the left side to the right side preserves (almost) all edges without significant loss of distinctness. The following fact immediately follows from this definition.

Fact 4.14. *Let Δ_{min} be the minimum left-degree of the vertices in G. Then if G is an (r, d)-lossless expander, then it is also an (r, c)-boundary expander with $c = \Delta_{min} - d$.*

Lemma 4.15. *Let $C > 1$. There exist constants $\delta, d > 0$ such that for every large enough positive integers m, n with $n < m < Cn$, there is an $m \times n$ bipartite graph G satisfying the following:*

1. *the minimum left-degree of G is at least $\Delta_{min} = 50 \log n$,*
2. *the maximum left-degree of G is at most $\Delta_{max} = 150 \log n$,*
3. *G is an (n^δ, d)-lossless expander.*

In particular, G is an $(n^\delta, \Delta_{min} - d)$-boundary expander.

Let G be a bipartite graph with parts L and R and edges E. Given $K \subseteq R$, we define $G \setminus K$ as the bipartite graph with parts L and $R \setminus K$ and edges $\{(i, k) \in E : i \in L, k \in R \setminus K\}$. Observe that for every $i \in L$, $\mathcal{N}_{G \setminus K}(i) = \mathcal{N}_G(i) \setminus K$.

Lemma 4.16. *Let G be an $m \times n$ (n^δ, d)-lossless expander with parts L and R, a minimum left-degree at least $\Delta_{min} = 50 \log n$ and a maximum left-degree at most $\Delta_{max} = 150 \log n$. Let K be a random subset of R such that every $j \in R$ is added to K independently with probability $2/3$. Then the graph $G \setminus K$ is an (n^δ, d)-lossless expander with a minimum left-degree $\Delta_{min}/6$ with probability $1 - o(1)$. In particular, $G \setminus K$ is an (n^δ, c)-boundary expander, where $c = \Delta_{min}/6 - d$.*

The proofs of these lemmas can be found in Appendix A.

4.7 The Rank Principle and Oddtown Principle

In this section, we introduce our main instance. Here we focus on their purely algebraic formulations, as it is the simplest and most transparent. Later, we will also consider its CNF encodings.

Fix a field $\mathbb{F}$ and positive integer parameters m and n with $m > n$. We denote $\mathsf{Rank}_n^m(A)$ the system of degree-2 polynomial equations stating that the rank of an $m \times m$ matrix A is at most n over $\mathbb{F}$. More precisely, the *rank principle* $\mathsf{Rank}_n^m(A)$ is defined over $2mn$ variables arranged into two matrices $X \in \mathbb{F}^{m \times n}$ and $Y \in \mathbb{F}^{n \times m}$. For every $i, j \in [m]$, there is an equation in $\mathsf{Rank}_n^m(A)$ stating that the (i, j)th entry of the product XY is equal to $A_{i,j}$. That is:

$$A_{i,j} - \sum_{k \in [n]} x_{i,k} y_{k,j}, \qquad i, j \in [m]. \tag{8}$$

Every equation in Rank_n^m has degree 2 over the variables from X and Y. It follows from basic linear algebra that when the rank of A exceeds n, $\mathsf{Rank}_n^m(A)$ is unsatisfiable.

When $A = I_m$, the $m \times m$ identity matrix, we might omit explicitly specifying the matrix in the notation and simply write Rank_n^m.

We also need the *oddtown principle* $\mathsf{OT}_n^m(A)$, which is the special case of Rank_n^m with $Y = X^T$. That is, given a symmetric matrix $A \in \mathbb{F}^{m\times m}$, $\mathsf{OT}_n^m(A)$ is defined over mn variables arranged as a matrix $X \in \mathbb{F}^{m\times n}$, and for every $i, j \in [m]$, there is an equation in OT_n^m stating that the (i, j)th entry of XX^T is equal to $A_{i,j}$:

$$A_{i,j} - \sum_{k\in[n]} x_{i,k}x_{j,k}, \qquad i, j \in [m], i \le j. \tag{9}$$

5 Proof Complexity Generators for $\mathsf{PCR}_{\mathbb{F}_2}$

In this section, we consider the following generator and show that it is a proof complexity generator hard against $\mathsf{PCR}_{\mathbb{F}_2}$ under various encodings.

The Low-Rank Generator g

Assume $m > n$.
Input: Two matrices $X \in \mathbb{F}^{m\times n}$ and $Y \in \mathbb{F}^{n\times m}$.
Output: Their product $XY \in \mathbb{F}^{m\times m}$.

Note that $g\colon \mathbb{F}^{2mn} \to \mathbb{F}^{m^2}$, hence this function is stretching when $n < \frac{m}{2}$. This function was considered by Krajíček in [52] as a proof complexity generator based on the pigeonhole principle, for algebraic proof systems. It was also considered as a candidate hitting set generator in algebraic complexity and polynomial identity testing by Andrews and Forbes [6, 7].

Given an $m \times m$ matrix A over $\mathbb{F}_2$, in this section, we consider different encodings of the statement "$A \notin \mathrm{Range}(g)$".

In Section 5.1 we show the hardness of the algebraic encoding $\mathsf{Rank}_n^m(A)$ for $\mathsf{PCR}_{\mathbb{F}_2}$.

In Section 5.2 and Section 5.3, we consider two Boolean encodings of the statement "$A \notin \mathrm{Range}(g)$". The first encoding, $\mathsf{PMRank}_n^m(A)$, employs the perfect matching principle to encode parities. The second encoding, $\mathsf{BTRank}_n^m(A)$, uses extension variables arranged in unbalanced binary trees (bamboos). For the perfect matching encoding, when working with over $\mathbb{F}_2$ and specifically $\mathsf{PCR}_{\mathbb{F}_2}$, we only consider the case $A = I$, establishing its hardness against $\mathsf{PCR}_{\mathbb{F}_2}$. For fields different from $\mathbb{F}_2$, we consider $\mathsf{PMRank}_n^m(A)$ with any matrix A, and specifically construct a reduction to the perfect matching principle Count_n^2. Consequently, this implies hardness for $\mathsf{PCR}_{\mathbb{F}}$ with $\mathrm{char}(\mathbb{F}) \neq 2$, SoS, and AC^0-Frege.

For the bamboo-tree encoding $\mathsf{BTRank}_n^m(A)$, we demonstrate its hardness for $\mathsf{PCR}_{\mathbb{F}_2}$ in the general case when the matrix A is arbitrary.

In Section 5.4, we show that certain iterated variants of Rank and BTRank are hard for $\mathsf{PCR}_{\mathbb{F}_2}$. Iterability is a way to increase the stretch of a generator by repeatedly applying it multiple times. Krajíček [50] introduced the notion of *s-iterability*, designed to boost the stretch of a variant of the Nisan generator [59]. Improving [4], Razborov [73] relaxed the expander requirements and showed that linear systems as in [4] can be *iterated* to achieve a much larger stretch—about 2^{n^ε}.

Here we use a weaker notion compared to s-iterability that is still sufficient for our applications. Namely, this notion is sufficient for the circuit lower bounds in Section 8.3, which are obtained by reductions to the formulas in Section 5.4.

In this section, we consider PC in which every proof line is a multilinear polynomial (and the multiplication rule involves multiplying with a variable followed by multilinearisation). Namely, we assume that proof-lines are polynomials from a quotient ring $\mathbb{F}_2[\vec{x}]/(\vec{x}^2 - \vec{x})$ factorised over the

Boolean axioms for all variables. This does not increase neither the monomial-size nor the degree of PC refutations (see [19]).

5.1 Algebraic Rank Principle

In this section, we will use a special notion of degree, called *column degree*, that is equal to the number of distinct *columns* a term in a refutation of $\mathsf{Rank}_n^m(A)$ mentions. This is formally defined as follows.

Definition 5.1 (Column-mentioned variables)**.** Let t be a term in the variables of $\mathsf{Rank}_n^m(A)$. We say that $k \in [n]$ is *X-column-mentioned in t* if there is $i \in [m]$ such that $x_{i,k}$ or $\overline{x}_{i,k}$ appears in t. We say that $k \in [n]$ is *Y^T-column-mentioned in t* if there is $j \in [m]$ such that $y_{k,j}$ or $\overline{y}_{k,j}$ appears in t.

Definition 5.2 (Column degree)**.** Let t be a term in the variables of $\mathsf{Rank}_n^m(A)$. Let K be the set of all $k \in [n]$ that are either X-column-mentioned or Y^T-column-mentioned in t. We say that t *mentions* columns K. The *column degree* of t is defined as $|K|$.

We start with proving a lower bound on the column degree of $\mathsf{PCR}_{\mathbb{F}_2}$ refutations of $\mathsf{Rank}_n^m(A)$.

Lemma 5.3. *Suppose that $m > n > 0$ and $A \in \{0,1\}^{m \times m}$ is an $m \times m$ Boolean matrix. Then any $\mathsf{PCR}_{\mathbb{F}_2}$ refutation of $\mathsf{Rank}_n^m(A)$ requires column degree at least $n/2 + 1$.*

Proof. We reduce FPHP_n^m pigeonhole principle (in the sense of Definition 4.6) to this instance; namely, we show that there is a substitution τ under which $\mathsf{Rank}_n^m(A) \restriction \tau$ is efficiently derivable from the axioms of FPHP_n^m. The reduction τ is defined as follows.

Let $P = (p_{i,k})_{i \in [m], k \in [n]}$ be fresh variables. It is useful to think of P as an $m \times n$ variable matrix.

1. For each $i \in [m]$ and $k \in [n]$, set
$$\tau(x_{i,k}) = (AP)_{i,k} = \sum_{s \in [m]} A_{i,s} p_{s,k}.$$

2. For each $j \in [m]$ and $k \in [n]$ set
$$\tau(y_{k,j}) = p_{j,k}.$$

Observe that $\tau(x_{i,k})$ and $\tau(y_{k,j})$ only use the variables of the form $p_{s,k} : s \in [m]$.

Let $i, j \in [m]$. The (i,j)th axiom of $\mathsf{Rank}_n^m(A)$ under τ transforms as follows (recall that $A_{i,j} = -A_{i,j}$ over $\mathbb{F}_2$):

$$\begin{aligned}
\left(\sum_{k \in [n]} x_{i,k} y_{k,j} + A_{i,j}\right) \restriction \tau &= \sum_{k \in [n]} \left(\sum_{s \in [m]} A_{i,s} p_{s,k}\right) p_{j,k} + A_{i,j} \\
&= \sum_{s \in [m]} A_{i,s} \left(\sum_{k \in [n]} p_{s,k} p_{j,k}\right) + A_{i,j} \\
&= \sum_{s \in [m] \setminus \{j\}} A_{i,s} \left(\sum_{k \in [n]} p_{s,k} p_{j,k}\right) + A_{i,j} \left(\sum_{k \in [n]} p_{j,k} + 1\right),
\end{aligned}$$

which is a degree-2 $\mathsf{NS}_{\mathbb{F}_2}$ derivation from the Hole Axioms $p_{s,k} p_{j,k} : s \in [m] \setminus \{j\}$, and the Pigeon Axiom $\sum_{k \in [n]} p_{j,k} + 1$.

Let Π be a $\mathsf{PCR}_{\mathbb{F}_2}$ refutation of $\mathsf{Rank}_n^m(A)$ of column degree d and let $\Pi' = \Pi \restriction \tau$.

Under the substitution

$$\tau(x_{i,k}) = \sum_{s \in [m]} A_{i,s} p_{s,k} \quad \text{and} \quad \tau(y_{k,j}) = p_{j,k},$$

the image of every variable of $\mathsf{Rank}_n^m(A)$ that X-column mentions or Y^T-column mentions some $k \in [n]$ depends only on the pigeonhole principle variables $p_{s,k} : s \in [m]$ associated with the kth hole. Thus, each column k in the rank principle corresponds exactly to the hole k in the pigeonhole principle. Therefore, if a monomial in the rank principle axioms mentions a set $K \subseteq [n]$ of columns, its image under τ involves only the variables corresponding to holes in K. Consequently, every term in Π' mentions at most d holes.

The refutation Π' can be extended to a refutation Π'' of FPHP_n^m such that each term in Π'' still mentions at most d holes, in a straightforward manner (we omit the details). Combined with the bound from Theorem 4.8, we conclude that the column degree of Π must be at least $n/2 + 1$. □

We continue by demonstrating a trade-off between the size and the *column degree* of refutations of $\mathsf{Rank}_n^m(A)$. We construct a random substitution σ that w.h.p. turns any small refutation Π of $\mathsf{Rank}_n^m(A)$ into a refutation $\mathsf{Rank}_{\tilde{n}}^m(A)$ with $\tilde{n} = \Omega(n)$ while simultaneously reducing the column degree of Π. The proof of the next theorem is relatively straightforward, as there are no extension variables to take care of. This substitution will later be used in proving lower bounds on CNF encodings.

Definition 5.4 (Substitution σ)**.** Assume $m > n \geq 2$ and $A \in \{0,1\}^{m \times m}$ is an $m \times m$ Boolean matrix. A random substitution σ is chosen as follows.

1. For each $k \in [n-1]$, uniformly and independently sample $c_k \in \{*, 1, 0\}$. Then set $c_n = |\{k \in [n-1] : c_k = 1\}| \bmod 2$. This guarantees that $|\{k \in [n] : c_k = 1\}|$ is even. We will call c_k the *column type* of k.
2. Let $\tilde{n} = |\{k \in [n] : c_k = *\}|$ and let $\tilde{X} = (\tilde{x}_{i,k})_{i \in [m], k \in [\tilde{n}]}$ and $\tilde{Y} = (\tilde{y}_{k,j})_{k \in [\tilde{n}], j \in [m]}$ be fresh variables.
3. Let ι be a bijection between $\{k \in [n] : c_k = *\}$ and $[\tilde{n}]$.
4. For each $i \in [m]$ and $k \in [n]$ set
$$\sigma(x_{i,k}) = \begin{cases} \tilde{x}_{i,\iota(k)} & \text{if } c_k = *, \\ c_k & \text{if } c_k \in \{0,1\}. \end{cases}$$
5. For each $j \in [m]$ and $k \in [n]$ set
$$\sigma(y_{k,j}) = \begin{cases} \tilde{y}_{\iota(k),j} & \text{if } c_k = *, \\ c_k & \text{if } c_k \in \{0,1\}. \end{cases}$$
6. For any variable θ mapped to 0 or 1 by σ, set $\sigma(\overline{\theta}) = 1 - \sigma(\theta)$.
7. For any variable θ not mapped to a Boolean constant by σ, set $\sigma(\overline{\theta}) = \overline{\sigma(\theta)}$ (namely, the negated variable of $\sigma(\theta)$).

Lemma 5.5. *Assume $m > n \geq 2$ and $A \in \{0,1\}^{m \times m}$ is a Boolean matrix. Let t be a term that mentions columns $K \subseteq [n]$. Then $\Pr[t \restriction \sigma \neq 0] \leq (2/3)^{|K|}$. Furthermore, $\Pr[\tilde{n} < (n-1)/6] \leq e^{-\frac{n-1}{24}}$.*

Proof. For the former statement, assume w.l.o.g. that for each column k from the set K there is a single variable γ_k in t that mentions column k. Let Γ_k be the event that $(\gamma_k \restriction \sigma \neq 0)$. Then $\{\Gamma_k : k \in K\}$ is a set of $|K|$ mutually independent events and each of them happens with probability at most $2/3$.

For the second statement in the lemma, define for each $k \in [n-1]$ the random variable
$$z_k = \begin{cases} 1 & \text{if } c_k = *, \\ 0 & \text{otherwise.} \end{cases}$$

Then $\tilde{n} = \sum_{k\in[n-1]} z_k$. It follows from the multiplicative Chernoff bound that $\Pr\left[\tilde{n} < \frac{n-1}{6}\right] \leq e^{-\frac{n-1}{24}}$. □

The substitution σ transforms any refutation of $\mathsf{Rank}_n^m(A)$ into a refutation of $\mathsf{Rank}_{\tilde{n}}^m(A)$.

Lemma 5.6. *Assume $m > n \geq 2$ and $A \in \{0,1\}^{m\times m}$ is a Boolean matrix. Then for every $\mathsf{PCR}_{\mathbb{F}_2}$ refutation Π of $\mathsf{Rank}_n^m(A)$, $\Pi \restriction \sigma$ is a refutation of $\mathsf{Rank}_{\tilde{n}}^m(A)$.*

Proof. For every $i, j \in [m]$, the (i,j)th axiom of $\mathsf{Rank}_n^m(A)$ transforms under σ as follows:

$$\left(A_{i,j} + \sum_{k=1}^{n} x_{i,k}y_{k,j}\right) \restriction \sigma = A_{i,j} + \sum_{k\in[n],c_k=*} \tilde{x}_{i,\iota(k)}\tilde{y}_{\iota(k),j} + |\{k \in [n] : c_k = 1\}| = A_{i,j} + \sum_{\ell=1}^{\tilde{n}} \tilde{x}_{i,\ell}\tilde{y}_{\ell,j},$$

since $|\{k \in [n] : c_k = 1\}|$ is even and ι is a bijection between $\{k \in [n] : c_k = *\}$ and $[\tilde{n}]$. □

Theorem 5.7. *Suppose that $m > n \geq 2$ and $A \in \{0,1\}^{m\times m}$ is an $m \times m$ Boolean matrix. Then any $\mathsf{PCR}_{\mathbb{F}_2}$ refutation of $\mathsf{Rank}_n^m(A)$ requires size $2^{\Omega(n)}$.*

Proof. Assume that $\mathsf{Rank}_n^m(A)$ has a refutation Π of size less than $(3/2)^{\frac{n-1}{12}}(1 - e^{-\frac{n-1}{24}}) = 2^{\Theta(n)}$. Then, by the union bound and Lemmas 5.5 and 5.6 there exists a restriction σ such that $\Pi \restriction \sigma$ is a refutation of $\mathsf{Rank}_{\tilde{n}}^m(A)$ with $\tilde{n} \geq \frac{n-1}{6}$ and column degree less than $\frac{n-1}{12} \leq \frac{\tilde{n}}{2}$. This would contradict Lemma 5.3. □

5.2 Perfect Matching Encoding of the Rank Principle

To encode the rank formula $XY = A$ as a CNF, we consider the encoding that uses the *perfect matching principle* to encode the parities appearing $XY = A$. Similar encodings were used in [40, 45]. For every $i, j \in [m]$, we encode the parity $\sum_{k\in[n]} x_{i,k}y_{k,j}$ by exhibiting a perfect matching on the pairs $x_{i,k}y_{k,j}$ (together with an extra unmatched point when $A_{i,j} = 1$).

Definition 5.8 (The CNF encoding $\mathsf{PMRank}_n^m(A)$)**.** Assume $m > n$ and $A \in \{0,1\}^{m\times m}$.

Variables: $X = (x_{i,k})_{i\in[m],k\in[n]}$, $Y = (y_{k,j})_{k\in[n],j\in[m]}$, for each $i, j \in [m]$, $\{z_{i,j,\{k,\ell\}} : \{k,\ell\} \in \binom{[n]}{2}\}$ if $A_{i,j} = 0$ and $\{w_{i,j,\{k,\ell\}} : \{k,\ell\} \in \binom{[n+1]}{2}\}$ if $A_{i,j} = 1$.

Even Axioms: For every $i, j \in [m]$ with $A_{i,j} = 0$, we use the following clauses:

$$\neg x_{i,k} \vee \neg y_{k,j} \vee \bigvee_{\ell\in[n]\setminus\{k\}} z_{i,j,\{k,\ell\}}, \qquad k \in [n], \tag{10}$$

$$\neg x_{i,k} \vee \neg y_{k,j} \vee \neg z_{i,j,\{k,\ell\}} \vee x_{i,\ell}, \qquad k \in [n], \ell \in [n]\setminus\{k\}, \tag{11}$$

$$\neg x_{i,k} \vee \neg y_{k,j} \vee \neg z_{i,j,\{k,\ell\}} \vee y_{\ell,j}, \qquad k \in [n], \ell \in [n]\setminus\{k\}, \tag{12}$$

$$\neg x_{i,k} \vee \neg y_{k,j} \vee \neg z_{i,j,\{k,\ell\}} \vee \neg z_{i,j,\{k,\ell'\}}, \qquad k \in [n], \ell, \ell' \in [n]\setminus\{k\}, \ell \neq \ell'. \tag{13}$$

Odd Axioms: For every $i, j \in [m]$ with $A_{i,j} = 1$, we use the following clauses:

$$\neg x_{i,k} \vee \neg y_{k,j} \vee \bigvee_{\ell\in[n+1]\setminus\{k\}} w_{i,j,\{k,\ell\}}, \qquad k \in [n], \tag{14}$$

$$\bigvee_{\ell\in[n]} w_{i,j,\{n+1,\ell\}}, \tag{15}$$

$$\neg x_{i,k} \vee \neg y_{k,j} \vee \neg w_{i,j,\{k,\ell\}} \vee x_{i,\ell}, \qquad k \in [n], \ell \in [n]\setminus\{k\}, \tag{16}$$

$$\neg x_{i,k} \vee \neg y_{k,j} \vee \neg w_{i,j,\{k,\ell\}} \vee y_{\ell,j}, \qquad k \in [n], \ell \in [n]\setminus\{k\}, \tag{17}$$

$$\neg w_{i,j,\{n+1,\ell\}} \vee x_{i,\ell}, \qquad \ell \in [n], \tag{18}$$

$$\neg w_{i,j,\{n+1,\ell\}} \vee y_{\ell,j}, \qquad \ell \in [n], \tag{19}$$

$$\neg x_{i,k} \vee \neg y_{k,j} \vee \neg w_{i,j,\{k,\ell\}} \vee \neg w_{i,j,\{k,\ell'\}}, \qquad k \in [n], \ell, \ell' \in [n+1]\setminus\{k\}, \ell \neq \ell', \tag{20}$$

$$\neg w_{i,j,\{n+1,\ell\}} \vee \neg w_{i,j,\{n+1,\ell'\}}, \qquad \ell \in [n], \ell' \in [n]\setminus\{\ell\}. \tag{21}$$

In words, for each polynomial equation $\sum_{k\in[n]} x_{i,k}y_{k,j} = A_{i,j}$ in $\mathsf{Rank}_n^m(A)$, the statement that the equation is satisfied is encoded by stating that there is a perfect matching on the satisfied monomials appearing in the equation (namely, those monomials that evaluate to 1 under a given assignment). In particular, clauses (10)–(13) express that each polynomial equation $\sum_{k\in[n]} x_{i,k}y_{k,j} = 0$ is satisfied by stating that there is a perfect matching on the set consisting of the satisfied monomials among $x_{i,k}y_{k,j}$, with $k \in [n]$: each monomial $x_{i,k}y_{k,j}$ with $x_{i,k} = y_{k,j} = 1$ is matched with some other monomial $x_{i,\ell}y_{\ell,j}$ (that also satisfies $x_{i,\ell} = y_{\ell,j} = 1$) by the variable $z_{i,j,\{k,\ell\}}$. Similarly, clauses (14)–(21) express $\sum_{k\in[n]} x_{i,k}y_{k,j} = 0$ using an extra point: each monomial $x_{i,k}y_{k,j}$ with $x_{i,k} = y_{k,j} = 1$ can be either matched to another such monomial or to the extra point $n+1$ by setting $w_{i,j,\{k,n+1\}} = 1$. The axioms about the extra point ((15), (18), (19) and (21)) are stated separately since they have a simpler formulation than their counterparts (14), (16), (17) and (20).

To simplify the reasoning and highlight the main proof ideas, we focus on the case where A is the identity matrix I_m. The general case requires additional arguments, which we present in the next section (Section 5.3) for the *bamboo-tree* encoding, as it is more useful in the context of this paper. A similar approach can be taken for $\mathsf{PMRank}_n^m(A)$, but this would require repeating many parts of the proofs from Section 5.3. In the case $A = I_m$, we can consider a weaker variant of $\mathsf{PMRank}_n^m(I_m)$ when $Y = X^T$. Since the ones lie only on the diagonal we can replace each w-variable $w_{i,i,\{k,\ell\}}$ with $w_{i,\{k,\ell\}}$, where $i \in [m]$. For $i, j \in [m]$ with $i \neq j$, the axioms for $A_{i,j}$ and $A_{j,i}$ become symmetrical, thus we unify the variables $z_{i,j,\{k,\ell\}}$ and $z_{j,i,\{k,\ell\}}$ into a single variable $z_{\{i,j\},\{k,\ell\}}$. This leads to the following simplified set of axioms:

Even Axioms: For every $i, j \in [m]$ with $i \neq j$:

$$\neg x_{i,k} \vee \neg x_{j,k} \vee \bigvee_{\ell\in[n]\setminus\{k\}} z_{\{i,j\},\{k,\ell\}}, \qquad k \in [n], \tag{22}$$

$$\neg x_{i,k} \vee \neg x_{j,k} \vee \neg z_{\{i,j\},\{k,\ell\}} \vee x_{i,\ell}, \qquad k \in [n], \ell \in [n] \setminus \{k\}, \tag{23}$$

$$\neg x_{i,k} \vee \neg x_{j,k} \vee \neg z_{\{i,j\},\{k,\ell\}} \vee \neg z_{\{i,j\},\{k,\ell'\}}, \qquad k \in [n], \ell, \ell' \in [n] \setminus \{k\}, \ell \neq \ell'. \tag{24}$$

Odd Axioms: For every $i \in [m]$:

$$\neg x_{i,k} \vee \bigvee_{\ell\in[n+1]\setminus\{k\}} w_{i,\{k,\ell\}}, \qquad k \in [n], \tag{25}$$

$$\bigvee_{\ell\in[n]} w_{i,\{n+1,\ell\}}, \tag{26}$$

$$\neg x_{i,k} \vee \neg w_{i,\{k,\ell\}} \vee x_{i,\ell}, \qquad k \in [n], \ell \in [n] \setminus \{k\}, \tag{27}$$

$$\neg w_{i,\{n+1,\ell\}} \vee x_{i,\ell}, \qquad \ell \in [n], \tag{28}$$

$$\neg x_{i,k} \vee \neg w_{i,\{k,\ell\}} \vee \neg w_{i,\{k,\ell'\}}, \qquad k \in [n], \ell, \ell' \in [n+1] \setminus \{k\}, \ell \neq \ell', \tag{29}$$

$$\neg w_{i,\{n+1,\ell\}} \vee \neg w_{i,\{n+1,\ell'\}}, \qquad \ell \in [n], \ell' \in [n] \setminus \{\ell\}. \tag{30}$$

We call the formula consisting of the above axioms PMOT_n^m (since it encodes the negation of the *oddtown principle*).

Theorem 5.9. *Let $m > n \geq 15$ with n divisible by 5 and $n/5$ odd. Then every $\mathsf{PCR}_{\mathbb{F}_2}$ refutation of PMOT_n^m (and thus $\mathsf{PMRank}_n^m(I_m)$) requires size at least $(10/9)^{n/20}$.*

We prove this result by applying a random restriction that employs a different degree measure than the one used in Section 5.1. Previously, we counted how many times each *column* is mentioned in a term. While this approach is effective for x- and y-variables, it becomes less applicable for z- and w-variables. Instead, we are interested in the *row degree*, that is, the number of different columns a term mentions. Formally, it is defined as follows.

Definition 5.10 (Row-mentioned variables for perfect matching encoding)**.** Let t be a term in the variables of PMOT_n^m. We say that $i \in [m]$ is *X-row-mentioned in t* if there are $k \in [n]$ and $b \in \{0, 1\}$ such that $x_{i,k}^b$ appears in t. We say that $i \in [m]$ is *W-row-mentioned in t* if there are

$\{k,\ell\} \in \binom{[n]}{2}$ and $b \in \{0,1\}$ such that $w^b_{i,\{k,\ell\}}$ appears in t. We say that $i \in [m]$ is *Z-row-mentioned in t* if there are $j \in [m]$, $\{k,\ell\} \in \binom{[n+1]}{2}$ and $b \in \{0,1\}$ such that $z^b_{\{i,j\},\{k,\ell\}}$ appears in t.

Definition 5.11 (Row degree)**.** Let t be a term in the variables of PMOT^m_n. Let I be the set of all $i \in [m]$ that are either X-row-mentioned, W-row-mentioned or Z-row-mentioned in t. The *row degree* of t is defined as $|I|$. We also say that t *mentions* each $i \in I$.

As previously, we construct a random substitution ρ that eliminates every term of high row degree with exponentially small probability. The constructed is based on the matrix $\mathcal{B}_n$, which we define below.

Recall that $J_{\ell,\ell'}$ denotes the $\ell \times \ell'$ all-ones matrix. We use $\otimes$ for the Kronecker (tensor) product. For two matrices P and Q, the matrix $P \otimes Q$ is obtained by replacing each entry $P_{i,j}$ by the block $P_{i,j}Q$. In particular, if $Q = J_{1,t}$ is the $1 \times t$ all-ones matrix, then $P \otimes J_{1,t}$ is obtained by repeating each column of P into a block of t identical columns.

Let $\mathcal{B}$ be the 5×5 matrix

$$\mathcal{B} = \begin{pmatrix} 1 & * & 0 & 0 & 0 \\ 0 & 1 & * & 0 & 0 \\ 0 & 0 & 1 & * & 0 \\ 0 & 0 & 0 & 1 & * \\ * & 0 & 0 & 0 & 1 \end{pmatrix}. \tag{31}$$

We will use the $5 \times n$ matrix $\mathcal{B}_n = \mathcal{B} \otimes J_{1,n/5}$. For example,

$$\mathcal{B}_{15} = \mathcal{B} \otimes J_{1,3} = \begin{pmatrix} 1 & 1 & 1 & * & * & * & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & * & * & * & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & * & * & * & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & * & * & * \\ * & * & * & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

Given $r \in [5]$ and $s \in \{*,1,0\}$, let

$$C^s_n(r) = \{k \in [n] : (\mathcal{B}_n)_{r,k} = s\} \tag{32}$$

be the set of all the column indices of the occurrences of s in the rth row of $\mathcal{B} \otimes J_{1,n/5}$. For example, $C^1_n(r) = \{(r-1)n/5+1, (r-1)n/5+2, \ldots, rn/5\}$ for all $r \in [5]$.

The substitution ρ reduces PMOT^m_n to a smaller instance $\mathsf{PMOT}^m_{\tilde{n}}$ with $\tilde{n} = n/5$. For each row $i \in [m]$, we sample independently its *row type* $r_i \in [5]$, which corresponds to a row of $\mathcal{B}_n$ and assign the x-variables accordingly. We proceed by assigning the remaining z- and w-variables by assigning them to a random matching that is consistent with $\mathcal{B}_n$. Observe that we can freely set z- and w-variables with indices from $C^0_n(r_i)$ arbitrarily.

Definition 5.12 (Substitution ρ for PMOT^m_n)**.** Assume that n is divisible by 5 and $\tilde{n} = n/5$ is odd. For each $r \in [5]$ fix an arbitrary perfect matching $M(r)$ on the set $C^1_n(r) \cup \{n+1\}$. For each $r \in [5]$ fix $k(r)$ to be the first (for definiteness) integer in $C^1_n(r)$ and fix an arbitrary perfect matching $M'(r)$ on the set $C^1_n(r) \setminus \{k(r)\}$. $k(r)$ will play the role of new *extra point*. Define a random substitution ρ as a random partial map from the variables of PMOT^m_n and their twin variables to $\{0,1\}$ by the following random experiment:

1. Independently for each $i \in [m]$, choose uniformly at random an integer $r_i \in [5]$. Then, for each $i \in [m]$ and $k \in [n] \setminus C^*_n(r_i)$, set $\rho(x_{i,k}) = (\mathcal{B}_n)_{r_i,k}$. This assigns all the constant (0 or 1) entries of $(\mathcal{B}_n)_{r_i,k}$ in the ith row of X. The remaining variables $x_{i,k}$, where $i \in [m]$ and $k \in C^*_n(r_i)$, are left unassigned.

2. Independently for each $i \in [m]$ and each $\{k,\ell\} \subseteq C^0_n(r_i)$, ρ maps $w_{i,\{k,\ell\}}$ to 0 or 1 each with probability 1/2. These variables can be assigned to arbitrary variables since all the axioms

they appear in ((25), (27) and (29)) also contain $\neg x_{i,k}$ or $\neg x_{i,\ell}$, which we set to 1 in Item 1, satisfying these axioms.

Next, $\rho(w_{i,\{k,\ell\}}) = 1$ for every $\{k,\ell\} \in M(r_i)$, and $\rho(w_{i,\{k,\ell\}}) = 0$ for all variables $w_{i,\{k,\ell\}}$ that are not yet mapped, except for those with $\{k,\ell\} \subseteq C_n^*(r_i)$. This assignment sets all the remaining variables $\rho(w_{i,\{k,\ell\}})$ according to $M(r_i)$, leaving those with $\{k,\ell\} \subseteq C_n^*(r_i)$ unassigned.

Observe that, since $(n+1)$ is matched in $M(r_i)$, we always set all $w_{i,\{n+1,k\}}$, $k \in [n]$, to constants (exactly one of these variables to 1 and the rest to 0).

3. Independently for each $i \neq j \in [m]$ and each $\{k,\ell\} \subseteq C_n^0(r_i) \cup C_n^0(r_j)$, ρ maps $z_{\{i,j\},\{k,\ell\}}$ to 0 or 1 each with probability 1/2. This is done similarly to Item 2 since every axiom containing $z_{\{i,j\},\{k,\ell\}}$ ((22), (23) and (24)) also contains either $\neg x_{i,k} \vee \neg x_{j,k}$ or $\neg x_{i,\ell} \vee \neg x_{j,\ell}$ and both are satisfied under ρ.

4. For each $i \neq j \in [m]$ with $r_i = r_j$ and each $\{k,\ell\} \in M'(r_i)$, set $\rho(z_{\{i,j\},\{k,\ell\}}) = 1$. Set $\rho(z_{\{i,j\},\{k,\ell\}}) = 0$ for all variables with $i \neq j$ and $r_i = r_j$ that are not yet mapped, except for those with $\{k,\ell\} \subseteq C_n^*(r_i) \cup \{k(r_i)\}$.

5. For each $i \neq j \in [m]$ with $r_i \neq r_j$ and each $\{k,\ell\} \in \binom{[n]}{2}$ with $|\{k,\ell\} \cap (C_n^0(r_i) \cup C_n^0(r_j))| = 1$, set $\rho(z_{\{i,j\},\{k,\ell\}}) = 0$.

6. For any variable θ mapped to 0 or 1 by ρ in Items 1 to 5, define $\rho(\overline{\theta}) = 1 - \rho(\theta)$.

It follows from the above definition that for every variable θ of PMOT_n^m, we have $\Pr[\theta \restriction \rho = 0] \geq 1/10$ and $\Pr\left[\overline{\theta} \restriction \rho = 0\right] \geq 1/10$. Moreover, this probability depends only on the rows that θ mentions. This allows eliminating every term that mentions many rows w.h.p. This intuition is formalised in the following lemma.

Lemma 5.13. *Suppose that n is divisible by 5 and $\tilde{n} = n/5$ is a positive odd integer. Let t be a term in the variables of PMOT_n^m and let t' be a subterm of t obtained by removing all variables $w_{i,\{k,n+1\}}, i \in [m], k \in [n]$, and their twins. Let I be the set of all $i \in [m]$ that are X-, W- or Z-row mentioned by t'. Then $\Pr[t \restriction \rho \neq 0] \leq (9/10)^{|I|/2}$.*

Proof. We may assume without loss of generality that no variables from $w_{i,\{k,n+1\}}, i \in [m], k \in [n]$ or their twins appear in t. Given $q \in \{X, W, Z\}$, let $I(q)$ be the set of rows $i \in [m]$ that are X-row-mentioned, W-row-mentioned or Z-row-mentioned in t, respectively. For example, $I(X) = \{i \in [m] : \exists k \in [n], x_{i,k} \text{ or } \overline{x}_{i,k} \text{ occurs in } t\}$.

There is a set A of at least half of the elements from the set $V = I(Z) \setminus (I(X) \cup I(W))$ and an injection f from A to $\{z_{\{i,j\},\{k,\ell\}} : \{i,j\} \in \binom{[m]}{2}, \{k,\ell\} \in \binom{[n]}{2}\}$ such that for each $i \in A$, $f(i)$ mentions i and $f(i)$ or its twin occurs in t. To see this, consider a graph G with vertex set V and edge set $\{\{i,j\} \in \binom{V}{2} : \text{for some } \{k,\ell\} \in \binom{[n]}{2},\ z_{\{i,j\},\{k,\ell\}} \text{ or } \overline{z}_{\{i,j\},\{k,\ell\}} \text{ occurs in } t\}$. For each connected component of G, fix a spanning tree and a root vertex. For each vertex i in the component other than the root, let j be the neighbour of i in the tree that is closer to the root. We define $f(i)$ to be a z-variable that mentions both i and j and either occurs in t or its twin occurs in t. This finishes the definition of A and f; they clearly have the required properties.

We can extend f to a function f' defined on $A \cup I(X) \cup I(W)$ by setting $f'(i)$ for $i \in I(X) \setminus A$ to some x-variable or its twin that occurs in t and mentions i and by defining $f'(i)$ for $i \in I(W) \setminus (A \cup I(X))$ to be a w-variable that mentions i and either occurs in t or its twin occurs in t.

For every $i \in I(X) \setminus A$, define the event $\Gamma_i = (f'(i) = 0)$. By Item 1, we have $\Pr[(]\Gamma_i) \geq 1/5$.

For every $i \in I(W) \setminus (A \cup I(X))$, let $f'(i) = w_{i,\{k,\ell\}}$ and define the event $\Delta_i = (\{k,\ell\} \subseteq C_n^0(r_i) \wedge f'(i) = 0)$. It follows from the estimate $\Pr\left[\{k,\ell\} \subseteq C_n^0(r_i)\right] \geq 1/5$ (by Item 1) that $\Pr[\Xi_i] \geq 1/10$ (by Item 2).

For every $i \in A$, let $f'(i) = z^b_{\{i,j\},\{k,\ell\}}$ and define the event $\Xi_i = (\{k,\ell\} \subseteq C_n^0(r_i) \wedge f'(i) = 0)$. It follows from the estimate $\Pr\left[\{k,\ell\} \subseteq C_n^0(r_i)\right] \geq 1/5$ (by Item 1) that $\Pr[\Xi_i] \geq 1/10$ (by Item 3).

Since all the events $\{\Gamma_i : i \in I(X) \setminus A\}$, $\{\Delta_i : i \in I(W) \setminus (I(X) \cup A)\}$ and $\{\Xi_i : i \in A\}$ are independent, we have

$$\Pr[t \restriction \rho \neq 0] \leq (4/5)^{|I(X)\setminus A|} \cdot (9/10)^{|I(W)\setminus(A\cup I(X))|} \cdot (9/10)^{|I(Z)|/2} \leq (9/10)^{d/2}.$$

□

Recall that PMOT_n^m semantically encodes the following statements:

$$\sum_{k=1}^{n} x_{i,k} = 1, \qquad i \in [m],$$
$$\sum_{k=1}^{n} x_{i,k}x_{j,k} = 0, \qquad i \neq j \in [m].$$

Under ρ, the former is transformed into

$$\sum_{k\in C_n^*(r_i)} x_{i,k} = 0, \qquad i \in [m].$$

The latter depends on r_i and r_j. Let $i \neq j \in [m]$:

- If $r_i = r_j$,
$$\sum_{k\in C_n^*(r_i)} x_{i,k}x_{j,k} = 1.$$
- If $r_j - r_i \equiv 1 \pmod 5$,
$$\sum_{k\in C_n^*(r_i)} x_{i,k} = 0.$$
- If $r_j - r_i \equiv -1 \pmod 5$,
$$\sum_{k\in C_n^*(r_j)} x_{j,k} = 0.$$

Now, we demonstrate that a refutation of $\mathsf{PMOT}_n^m \restriction \rho$ can be further restricted by a substitution σ that transforms it into a refutation of $\mathsf{PMOT}_{n/5-1}^{\widetilde{m}}$ for some $\widetilde{m} \geq m/5$.

Lemma 5.14. *Let $m > n \geq 15$ with n divisible by 5 and $\tilde{n} = n/5$ odd. Let ρ be an element of the support of the above distribution of random substitutions from Definition 5.12. Then there is an integer $\widetilde{m}$ with $m/5 \leq \widetilde{m} \leq m$ and a map σ from the variables of $\mathsf{PMOT}_n^m \restriction \rho$ and their twins onto the variables of $\mathsf{PMOT}_{\tilde{n}-1}^{\widetilde{m}}$ and their twins such that $(\mathsf{PMOT}_n^m \restriction \rho) \restriction \sigma$ coincides with $\mathsf{PMOT}_{\tilde{n}-1}^{\widetilde{m}}$. Moreover, there is a function $f : [m] \to [\widetilde{m}]$ such that every variable of $\mathsf{PMOT}_n^m \restriction \rho$ that mentions rows $i, j \in [m]$ (i and j can coincide) is mapped by σ to a variable that mentions rows $f(i)$ and $f(j)$.*

Proof Sketch. Given $r \in [5]$, define

$$I(r) = \{i : r_i = r\}.$$

Let σ_1 be the substitution that replaces the columns $\{r\tilde{n} : r \in [5]\}$ with the all-ones columns. Then, under $\sigma_1 \circ \rho$, PMOT_n^m becomes the union of five disjoint instances of $\mathsf{PMOT}_{\tilde{n}-1}^{|I(r)|}$, $r \in [5]$. This step is required because ρ transforms even axioms into odd ones and vice versa.

We proceed by constructing a substitution σ_2 to unify all these disjoint formulas into a single instance of $\mathsf{PMOT}_{\tilde{n}-1}^{\widetilde{m}}$, where $\widetilde{m} = \max\{|I(r)| : r \in [5]\}$. □

Finally, we also verify that any refutation of PMOT_n^m requires large $\mathsf{PCR}_{\mathbb{F}_2}$ degree by reducing FPHP to it.

Lemma 5.15. *Every* $\mathsf{PCR}_{\mathbb{F}_2}$ *refutation of* PMOT^m_n *has a term* t *that mentions at least* $n/2+1$ *rows.*

Proof. We will reduce FPHP^m_n to PMOT^m_n. Let $p_{i,k} : i \in [m], k \in [n]$ be fresh variables.

Consider the reduction τ defined as follows.

1. For every $i \in [m]$ and $k \in [n]$, set $\tau(x_{i,k}) = p_{i,k}$ and $\tau(\overline{x}_{i,k}) = \overline{p}_{i,k}$.
2. For every $i \neq j \in [m]$ and $\{k,\ell\} \in \binom{[n]}{2}$, set $\tau(z_{\{i,j\},\{k,\ell\}}) = 0$ and $\tau(\overline{z}_{\{i,j\},\{k,\ell\}}) = 1$.
3. For every $i \in [m]$ and $\{k,\ell\} \in \binom{[n]}{2}$, set $\tau(w_{i,\{k,\ell\}}) = 0$ and $\tau(\overline{w}_{i,\{k,\ell\}}) = 1$.
4. For every $i \in [m]$ and $k \in [n]$, set $\tau(w_{i,\{n+1,k\}}) = p_{i,k}$ and $\tau(\overline{w}_{i,\{n+1,k,\}}) = \overline{p}_{i,k}$.

Let Π be a $\mathsf{PCR}_{\mathbb{F}_2}$ refutation of PMOT^m_n such that every term in Π mentions at most d rows. Then every term in $\Pi' = \Pi \restriction \tau$ mentions at most d pigeons. Now we show that each polynomial from $\mathsf{PMRank}^m_n(I_m) \restriction \tau$ has a simple derivation from FPHP^m_n.

- The axioms (23) and (24) are satisfied since we set all z-variables to zero.
- The axiom (22) becomes $p_{i,k}p_{j,k}$, which is a Hole Axiom of FPHP^m_n of the form (4).
- The axioms (25) and (28) become $p_{i,k}\overline{p}_{i,k}$ and thus trivially follow from the properties of twin variables.
- The axiom (26) becomes $\prod_{\ell \in [n]} \overline{p}_{i,\ell}$ that semantically follows from the axioms of the form (3) and (5) and has a simple derivation from them, which mentions only pigeon i.
- The axioms (27) and (29) are satisfied.
- The axiom (30) becomes $p_{i,\ell}p_{j,\ell'}$, which is a Functionality Axiom of FPHP^m_n of the form (5).

Thus, Π' can be further extended to a refutation Π'' of FPHP^m_n such that each term in Π'' mentions at most d pigeons.

The theorem follows from the lower bound on the number of pigeons from Theorem 4.8. □

Combining Lemmas 5.13 to 5.15, we proceed by proving Theorem 5.9.

Proof of Theorem 5.9. Assume for the sake of contradiction that PMOT^m_n has a refutation Π of size less than $(10/9)^{n/20} = (10/9)^{\tilde{n}/4}$. We start by sampling a random substitution ρ from Definition 5.12. It follows from Lemma 5.13 that any term that mentions more than $n/2$ rows is not set to 0 by ρ with probability at most $(9/10)^{\tilde{n}/4}$. By the union bound, there exists a substitution ρ such that every term in $\Pi \restriction \rho$ mentions at most $\tilde{n}/2$ different rows.

By Lemma 5.14 we can further restrict $\Pi \restriction \rho$ and obtain a refutation $\Pi' = \Pi \restriction \rho \restriction \sigma$ of $\mathsf{PMOT}^{\widetilde{m}}_{\tilde{n}}$ with $m/5 \leq \widetilde{m} \leq m$. Moreover, every term Π' still mentions at most $\tilde{n}/2$ rows. This contradicts the row degree bound from Lemma 5.15. □

As we mentioned earlier, for proof systems, for which the perfect matching principle is hard, the hardness of $\mathsf{PMRank}^m_n(A)$ follows from the hardness of Count^2_n. We begin by describing this reduction. We describe it for the general case $\mathsf{PMRank}^m_n(A)$, where A is arbitrary.

Lemma 5.16. *Let* A *be an arbitrary* $m \times m$ *Boolean matrix that is distinct from matrices of all ones or all zeros. Then there exists a reduction* ρ *such that* $\mathsf{PMRank}^m_n(A) \restriction \rho$ *coincides with* $\mathsf{Count}^2_n \wedge \mathsf{Count}^2_{n+1}$.

Proof. Let $u_{\{k,\ell\}} : \{k,\ell\} \in \binom{[n]}{2}$ and $v_{\{k,\ell\}} : \{k,\ell\} \in \binom{[n+1]}{2}$ be fresh variables and consider the reduction ρ defined as follows:

1. For every $i \in [m]$ and $k \in [n]$ set $\rho(x_{i,k}) = 1$ and $\rho(\overline{x}_{i,k}) = 0$.

2. For every $j \in [m]$ and $k \in [n]$ set $\rho(y_{k,j}) = 1$ and $\rho(\overline{y}_{k,j}) = 0$.

3. For every $i, j \in [m]$ with $A_{i,j} = 0$ and every $\{k, \ell\} \in \binom{[n]}{2}$, set $\rho(z_{i,j,\{k,\ell\}}) = u_{\{k,\ell\}}$.

4. For every $i, j \in [m]$ with $A_{i,j} = 1$ and every $\{k, \ell\} \in \binom{[n+1]}{2}$, set $\rho(w_{i,j,\{k,\ell\}}) = v_{\{k,\ell\}}$.

5. For every variable θ, if $\rho(\theta)$ is not a Boolean constant, set $\rho(\overline{\theta}) = \overline{\rho(\theta)}$.

This restriction substitutes X with $J_{m,n}$, Y with $J_{n,m}$, and unifies all isomorphic instances of Count^2_n and Count^2_{n+1}.

We show that $\mathsf{PMRank}^m_n(A) \restriction \rho$ becomes a union of disjoint instances of Count^2_n and Count^2_{n+1}. Let $i, j \in [m]$. We consider the following cases.

- Suppose $A_{i,j} = 0$. In this case, we use the axioms (10)–(13), which under ρ become an instance of Count^2_n in the variables $u_{\{k,\ell\}} : \{k, \ell\} \in \binom{[n]}{2}$.

- Suppose $A_{i,j} = 1$. In this case, we use the axioms (14)–(21), which under ρ become an instance of Count^2_{n+1} in the variables $v_{\{k,\ell\}} : \{k, \ell\} \in \binom{[n+1]}{2}$.

Since A contains both ones and zeros, both formulas Count^2_n and Count^2_{n+1} appear in $\mathsf{PMRank}^m_n(A) \restriction \rho$. □

This lemma immediately implies the hardness of $\mathsf{PMRank}^m_n(A)$ for proof systems, in which Count^2_n is hard.

Theorem 5.17. *Let $m > n > 0$. Let A be an arbitrary $m \times m$ Boolean matrix. Then any $\mathcal{P}$-refutation of $\mathsf{PMRank}^m_n(A)$ requires size $2^{\Omega(n)}$, where $\mathcal{P}$ is $\mathsf{PCR}_{\mathbb{F}}$ with $\mathrm{char}(F) \neq 2$, SoS, and AC^0-Frege.*

Proof. If all entries of A are all ones or all zeros, the formula is satisfiable and the theorem holds trivially. Otherwise, by applying Lemma 5.16, we conclude that there is a reduction from $\mathsf{Count}^2_n \wedge \mathsf{Count}^2_{n+1}$ to $\mathsf{PMRank}^m_n(A)$. Depending on the parity of n exactly one of these instances is unsatisfiable. They are defined on disjoint sets of variables, hence we can satisfy the other. Since Count^2_k require size $2^{\Omega(k)}$ for $\mathsf{PCR}_{\mathbb{F}}$ with $\mathrm{char}(F) \neq 2$ (a combination of degree lower bounds [17] and size-degree trade-offs [19, 39]), SoS (a combination of [33, 74] and [9]), and AC^0-Frege [48], the theorem follows. □

5.3 Bamboo Tree Encoding of the Rank Principle

To encode the rank formula $XY = A$ as a CNF, extension variables are introduced to sequentially compute all inner products involved. The extension variables for each inner product are arranged in a totally unbalanced binary tree known as a "bamboo". This natural encoding corresponds to a circuit in the sense of [4, 73], and similar encodings have been used repeatedly for parity computations [4, 73, 78].

Definition 5.18 (The CNF encoding $\mathsf{BTRank}^m_n(A)$)**.** Assume $m > n$ are positive integers and $A \in \mathbb{F}_2^{m \times m}$ is an m by m matrix over the two-element field. The CNF encoding the bamboo tree rank formula, denoted $\mathsf{BTRank}^m_n(A)$, uses input variables $x_{i,k}, y_{k,i} : i \in [m], k \in [n]$ together with extension variables $z_{i,j,k}, u_{i,j,k} : i, j \in [m], k \in [n]$, and consists of the following axioms.

Output Axioms: For every $i, j \in [m]$, the clause $u_{i,j,n}$ if $A_{i,j} = 1$ and the clause $\neg u_{i,j,n}$ if $A_{i,j} = 0$.

Binary AND Axioms: For every $i, j \in [m]$ and $k \in [n]$, $z_{i,j,k} = x_{i,k} y_{k,j}$, encoded by the clauses $x_{i,k} \vee \neg z_{i,j,k}$, $y_{k,j} \vee \neg z_{i,j,k}$, $z_{i,j,k} \vee \neg x_{i,k} \vee \neg y_{k,j}$.

Summation Base Axioms: For every $i, j \in [m]$, $u_{i,j,1} = z_{i,j,1}$, encoded by the clauses $u_{i,j,1} \vee \neg z_{i,j,1}$, $z_{i,j,1} \vee \neg u_{i,j,1}$.

Summation Axioms: For every $i, j \in [m]$, and $k \in \{2, \ldots, n\}$, $u_{i,j,k} = u_{i,j,k-1} + z_{i,j,k}$, encoded by the following four clauses:

$$z_{i,j,k} \vee \neg u_{i,j,k-1} \vee u_{i,j,k},$$
$$z_{i,j,k} \vee u_{i,j,k-1} \vee \neg u_{i,j,k},$$
$$\neg z_{i,j,k} \vee \neg u_{i,j,k-1} \vee \neg u_{i,j,k},$$
$$\neg z_{i,j,k} \vee u_{i,j,k-1} \vee u_{i,j,k}.$$

We focus on the regime where m is arbitrarily larger than n. As with related formulas like PHP^m_n, obtaining size lower bounds in this regime is challenging across various proof systems, since standard measures such as resolution width or PC degree do not appear to be effective, at least when applied directly. Our technique applies to any matrix A and provides a $\mathsf{PCR}_{\mathbb{F}_2}$ size lower bound of $2^{\Omega(n)}$. This makes $\mathsf{BTRank}^m_n(A)$ a proof complexity generator, stretching $2mn$ input bits into m^2 output bits.

Theorem 5.19. *Suppose that $m > n \geq 16$ are integers, 8 divides n, and $A \in \mathbb{F}_2^{m \times m}$ is an m by m matrix over $\mathbb{F}_2$. Then any $\mathsf{PCR}_{\mathbb{F}_2}$ refutation of $\mathsf{BTRank}^m_n(A)$ has size at least $2^{\frac{\log e}{512} n - 2}$.*

Recall that the basic strategy for the simpler algebraic encoding of the rank principle is to use a random restricting that reduces with high probability a small-size refutation into a small-degree refutation, which then leads to a contradiction with the pigeonhole principle PCR degree lower bounds. Accordingly, our goal here is to show that if $\mathsf{BTRank}^m_n(A)$ admits a small $\mathsf{PCR}_{\mathbb{F}_2}$ refutation, then it can be converted into one in which a certain *relaxed* form of degree is small. This relaxed notion of degree is carefully tailored to the structure of our formula, with distinct definitions for each variable sort. Moreover, it appears that if we require a random substitution to serve as a meaningful self-reduction (i.e., converting $\mathsf{BTRank}^m_n(A)$ to a smaller instance of the same principle), then this relaxed degree measure is close to the limit of what can be effectively decreased under such a random transformation. While the definition can be made slightly stricter, any substantial move toward the standard notion of degree (i.e., total degree of term) does not seem to yield a measure that decreases adequately under random self-reductions. This limitation seems to stem from the distinct nature of the ("extension") u-variables, whose behaviour differs from that of the other variables in the formula. Fortunately, our relaxed degree is still strong enough to yield, after an additional substitution and some proof manipulations, a $\mathsf{PCR}_{\mathbb{F}_2}$ refutation of $\mathsf{FPHP}^m_{n'}$ of degree less than $n'/2$, which is ruled out by a theorem of Razborov [69].

The initial conversion of a purported small refutation of $\mathsf{BTRank}^m_n(A)$ begins by applying two distinct random substitutions, ρ and later σ. The random substitution ρ converts (with probability 1) a refutation of $\mathsf{BTRank}^m_n(A)$ to a refutation of an instance with less rows $\mathsf{BTRank}^m_{\tilde{n}}(A)$, for some $\tilde{n} < n$. Additionally, this substitution simplifies with high probability the presence of u-variables in terms appearing in refutations.

We now define the random substitution ρ, (not to be confused with the substitution with the same notation in Section 5.2). This substitution randomly compresses the matrices X and Y from n columns to about $n/4$ columns, row by row, in a way that preserves the bamboo structure and makes different rows behave independently.

Definition 5.20 (Substitution ρ for $\mathsf{BTRank}^m_n(A)$)**.** Assume that $m > n \geq 8$ and n is divisible by 4. Let $\tilde{n} = (n-4)/4$ and $\{\tilde{x}_{i,\ell} : i \in [m], \ell \in [\tilde{n}]\} \cup \{\tilde{y}_{\ell,i} : i \in [m], \ell \in [\tilde{n}]\} \cup \{\tilde{z}_{i,j,\ell} : i, j \in [m], \ell \in [\tilde{n}]\} \cup \{\tilde{u}_{i,j,\ell} : i, j \in [m], \ell \in [\tilde{n}]\}$ be a set of fresh variables. The random substitution ρ is defined as follows. Independently and uniformly at random, choose $4m$ bits $\{p_{i,0}, p_{i,1}, q_{i,0}, q_{i,1} : i \in [m]\} \in \{0,1\}^{4m}$. These bits are used as follows: $p_{i,0}$ chooses how the boundary columns of row i in X are hard-fixed, $p_{i,1}$ chooses which half of the interior columns of row i carry $\tilde{x}$-variables (the other half become 0), $q_{j,0}$ similarly fixes boundary entries for column j in Y, $q_{j,1}$ chooses which interior blocks of column j carry $\tilde{y}$-variables (the rest become 0). See Figure 3 and Figure 4. We extend ρ to the u- and z-variables so that it agrees with what ρ already does to X and Y, and so that $\mathsf{BTRank}^m_n(A)$ restricted by ρ becomes an instance of $\mathsf{BTRank}^m_{\tilde{n}}(A)$ (with the same matrix A). Formally, this is done as follows.

1. For each $i \in [m]$ and $k \in [n]$, set

$$\rho(x_{i,k}) = \begin{cases} p_{i,0} & \text{if } k \in \{1, n-1\}, \\ 1 & \text{if } k \in \{2, n\}, \\ 0 & \text{if } k \in \{3, \dots, n-2\}, \lfloor \frac{k-3}{\tilde{n}} \rfloor \in \{0,1\} \text{ and } p_{i,1} = 0, \\ \tilde{x}_{i,((k-3) \bmod \tilde{n})+1} & \text{if } k \in \{3, \dots, n-2\}, \lfloor \frac{k-3}{\tilde{n}} \rfloor \in \{2,3\} \text{ and } p_{i,1} = 0, \\ \tilde{x}_{i,((k-3) \bmod \tilde{n})+1} & \text{if } k \in \{3, \dots, n-2\}, \lfloor \frac{k-3}{\tilde{n}} \rfloor \in \{0,1\} \text{ and } p_{i,1} = 1, \\ 0 & \text{if } k \in \{3, \dots, n-2\}, \lfloor \frac{k-3}{\tilde{n}} \rfloor \in \{2,3\} \text{ and } p_{i,1} = 1, \end{cases}$$

   and similarly, for each $k \in [n]$ and $j \in [m]$, set

$$\rho(y_{k,j}) = \begin{cases} 1 & \text{if } k \in \{1, n-1\}, \\ q_{j,0} & \text{if } k \in \{2, n\}, \\ 0 & \text{if } k \in \{3, \dots, n-2\}, \lfloor \frac{k-3}{\tilde{n}} \rfloor \in \{0,2\} \text{ and } q_{j,1} = 0, \\ \tilde{y}_{((k-3) \bmod \tilde{n})+1,j} & \text{if } k \in \{3, \dots, n-2\}, \lfloor \frac{k-3}{\tilde{n}} \rfloor \in \{1,3\} \text{ and } q_{j,1} = 0, \\ \tilde{y}_{((k-3) \bmod \tilde{n})+1,j} & \text{if } k \in \{3, \dots, n-2\}, \lfloor \frac{k-3}{\tilde{n}} \rfloor \in \{0,2\} \text{ and } q_{j,1} = 1, \\ 0 & \text{if } k \in \{3, \dots, n-2\}, \lfloor \frac{k-3}{\tilde{n}} \rfloor \in \{1,3\} \text{ and } q_{j,1} = 1. \end{cases}$$

   In other words, the first two variables $(x_{i,1}, x_{i,2})$ of the row $(x_{i,1}, \dots, x_{i,n})$ are set to $(0,1)$ if $p_{i,0} = 0$, and to $(1,1)$ if $p_{i,0} = 1$, and the same is true for the last two variables $(x_{i,n-1}, x_{i,n})$. The block of remaining variables $(x_{i,3}, \dots, x_{i,n-2})$ is set to $(0,0,1,1) \otimes (\tilde{x}_{i,1}, \dots, \tilde{x}_{i,\tilde{n}})$ if $p_{i,1} = 0$, and to $(1,1,0,0) \otimes (\tilde{x}_{i,1}, \dots, \tilde{x}_{i,\tilde{n}})$ if $p_{i,1} = 1$. Similarly, for $(y_{1,j}, \dots, y_{n,j})$, the first two (as well as the last two) variables are set to $(1,0)$ or $(1,1)$ depending on the value of $q_{j,0}$, and the remaining variables $(y_{3,j}, \dots, y_{n-2,j})$ are set to $(0,1,0,1) \otimes (\tilde{y}_{1,j}, \dots, \tilde{y}_{\tilde{n},j})$ or $(1,0,1,0) \otimes (\tilde{y}_{1,j}, \dots, \tilde{y}_{\tilde{n},j})$ depending on the value of $q_{j,1}$.

2. For each $i, j \in [m]$ and $k \in [n]$, set $z_{i,j,k}$ to the correct value as determined by the values of $\rho(x_{i,k})$ and $\rho(y_{k,j})$ just defined and by Binary AND Axioms. That is, for $k \in \{1, n-1\}$ we define $\rho(z_{i,j,k}) = p_{i,0}$, for $k \in \{2, n\}$ we set $\rho(z_{i,j,k}) = q_{j,0}$, and for $k \in \{3, \dots, n-2\}$ we have four cases based on the values of $p_{i,1}, q_{j,1}$. First, let $r_{i,j} \in \{0,1,2,3\}$ be defined by $r_{i,j} = 3 - 2p_{i,1} - q_{j,1}$. It follows from Item 1 that the following definition is consistent with the Binary AND Axioms:

$$\rho(z_{i,j,k}) = \begin{cases} \tilde{z}_{i,j,((k-3) \bmod \tilde{n})+1} & \text{if } k \in \{r_{i,j}\tilde{n} + 3, \dots, (r_{i,j}+1)\tilde{n} + 2\}, \\ 0 & \text{if } k \in \{3, \dots, n-2\} \setminus \{r_{i,j}\tilde{n} + 3, \dots, (r_{i,j}+1)\tilde{n} + 2\}. \end{cases}$$

   In other words, for $k \in \{3, \dots, n-2\}$ we define $\rho(z_{i,j,k}) = 0$ if either $\rho(x_{i,k}) = 0$ or $\rho(y_{k,j}) = 0$; otherwise it follows from the previous item that $\rho(x_{i,k}) = \tilde{x}_{i,\ell}$ and $\rho(y_{k,j}) = \tilde{y}_{\ell,j}$, where $\ell = ((k-3) \bmod \tilde{n}) + 1$, and in this case we set $\rho(z_{i,j,k}) = \tilde{z}_{i,j,\ell}$.

3. The u-variables are assigned by ρ consistently not only with Summation Base Axioms and Summation Axioms, but also with Output Axioms, taking into account that after applying ρ to $\mathsf{BTRank}_n^m(A)$ we want Output Axioms to hold for the new variables $\tilde{u}_{i,j,\tilde{n}}$. Given $i \in [m]$ and $j \in [m]$, the definition of $\rho(u_{i,j,1}), \dots, \rho(u_{i,j,n})$ splits into cases based on the values $p_{i,0}, p_{i,1}, q_{j,0}, q_{j,1}$. It follows from Item 1 that the values of the first two variables are constant, namely $\rho(u_{i,j,1}) = p_{i,0}$ and $\rho(u_{i,j,2}) = p_{i,0} \oplus q_{j,0}$. We now define the values $\rho(u_{i,j,3}), \dots, \rho(u_{i,j,n-2})$ with the help of the integer $r_{i,j}$ defined in Item 2.

$$\rho(u_{i,j,k}) = \begin{cases} \tilde{u}_{i,j,((k-3) \bmod \tilde{n})+1} & \text{if } k \in \{r_{i,j}\tilde{n} + 3, \dots, (r_{i,j}+1)\tilde{n} + 2\} \ \&\ p_{i,0} \oplus q_{j,0} = 0, \\ \overline{\tilde{u}}_{i,j,((k-3) \bmod \tilde{n})+1} & \text{if } k \in \{r_{i,j}\tilde{n} + 3, \dots, (r_{i,j}+1)\tilde{n} + 2\} \ \&\ p_{i,0} \oplus q_{j,0} = 1, \\ p_{i,0} \oplus q_{j,0} & \text{if } k \in \{3, \dots, r_{i,j}\tilde{n} + 2\}, \\ p_{i,0} \oplus q_{j,0} \oplus A_{i,j} & \text{if } k \in \{(r_{i,j}+1)\tilde{n} + 3, \dots, n-2\}. \end{cases}$$

To define ρ consistently at the last two variables, $u_{i,j,n-1}$ and $u_{i,j,n}$, we need to set $\rho(u_{i,j,n-1}) = (p_{i,0} \oplus q_{j,0} \oplus A_{i,j}) \oplus p_{i,0} = q_{j,0} \oplus A_{i,j}$ and $\rho(u_{i,j,n}) = (q_{j,0} \oplus A_{i,j}) \oplus q_{j,0} = A_{i,j}$.

4. For any variable v mapped to 0 or 1 by ρ, set $\rho(\overline{v}) = 1 - \rho(v)$.

5. For any variable v not mapped to a Boolean constant by ρ, set $\rho(\overline{v}) = \overline{\rho(v)}$.

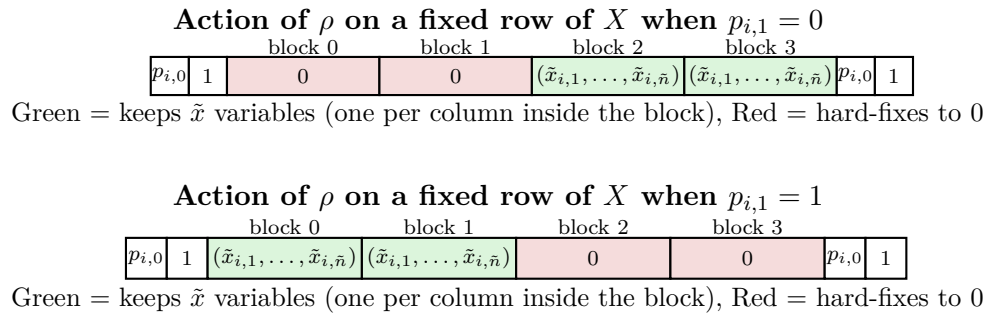


Figure 3: Action of ρ on a fixed row of X (two cases: $p_{i,1} = 0$ and $p_{i,1} = 1$).

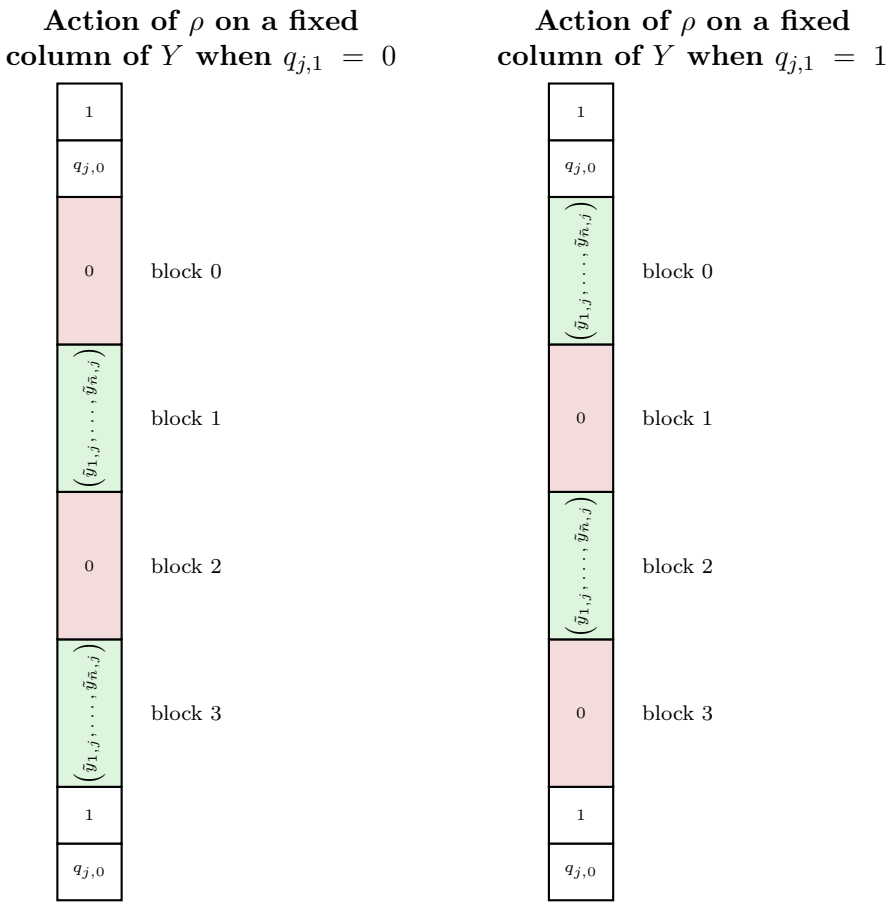


Figure 4: Action of ρ on a fixed column of Y (two cases: $q_{j,1} = 0$ and $q_{j,1} = 1$).

First, we demonstrate the desired effect of ρ on the u-variables occurring in terms.

Definition 5.21. [Row and column indices mentioned by U variables inside a term] Let t be a term in the variables of $\mathsf{BTRank}_n^m(A)$. We say that $i \in [m]$ is *U-left-row-mentioned in t* if there is $j \in [m], k \in [n]$, and $b \in \{0,1\}$ such that $u^b_{i,j,k}$ appears in t. We say that $j \in [m]$ is *U-right-row-mentioned in t* if there is $i \in [m], k \in [n]$, and $b \in \{0,1\}$ such that $u^b_{i,j,k}$ appears in t. We say that $k \in [n]$ is *U-column-mentioned in t* if there are $i, j \in [m]$ and $b \in \{0,1\}$ such that $u^b_{i,j,k}$ appears in t.

Note that row indices are those that range originally over $[m]$ while column indices range originally over $[n]$.

Lemma 5.22 (Random restriction ρ kills terms that mention many u-rows)**.** *Suppose that $m > n \geq 8$ are integers, 4 divides n, and $A \in \mathbb{F}_2^{m \times m}$ is an m by m matrix over $\mathbb{F}_2$. Suppose that t is a term in the variables of $\mathsf{BTRank}_n^m(A)$, $I \subseteq [m]$ is a set and t' is a subterm of t such that every $i \in I$ is U-left-row-mentioned in t' and no $k \in \{1, 2, n-1, n\}$ is U-column-mentioned in t'. Then, $\Pr[t \restriction \rho \neq 0] \leq (3/4)^{|I|}$.*

Proof. Let $r = |I|$. By the assumption of the lemma, t contains a subterm of the form $u^{b_1}_{i_1,j_1,k_1} u^{b_2}_{i_2,j_2,k_2} \cdots u^{b_r}_{i_r,j_r,k_r}$, where $1 \leq i_1 < i_2 < \cdots < i_r \leq m$ and for each $s \in [r]$ we have $b_s \in \{0,1\}$, $j_s \in [m]$ and $k_s \in \{3, \ldots, n-2\}$. It follows from the definition of ρ that for each row i that actually appears in the term (via some $u_{i,j,k}$ with $k \in \{3, \ldots, n-2\}$), there is a $1/4$ chance that ρ sets that u-factor to the "opposite" constant (so the whole product becomes 0), and these events are independent across the r different rows; hence the term survives with probability at most $(3/4)^r$.

More formally, by the definition of ρ for each $(a_s)_{s\in[r]} \in \{0,1\}^r$, for each $(a_{j,0}, a_{j,1})_{j\in\{j_1,\ldots,j_r\}} \in \{0,1\}^{2\cdot|\{j_1,\ldots,j_r\}|}$ and for each $h \in [r]$, we have

$$\Pr[\rho(u_{i_h,j_h,k_h}) = a_h : \text{for all } s \in [r], q_{j_s,0} = a_{j_s,0} \text{ and } q_{j_s,1} = a_{j_s,1}] \geq 1/4.$$

Moreover, these r conditional events are, for any choice of $(a_s)_{s\in[r]} \in \{0,1\}^r$ and $(a_{j,0}, a_{j,1})_{j\in\{j_1,\ldots,j_r\}} \in \{0,1\}^{2\cdot|\{j_1,\ldots,j_r\}|}$, mutually independent. The lemma follows. □

Next, we verify that ρ transforms a refutation of $\mathsf{BTRank}_n^m(A)$ into a refutation of $\mathsf{BTRank}_{\tilde{n}}^m(A)$. Namely, we reduce the number of columns in X (and accordingly, number of rows in Y). This is a structural consequence of the way the substitution is defined, and happens with probability 1: the k-indices in the input variables $x_{i,k}, y_{k,i} : i \in [m], k \in [n]$ (excluding the four boundaries ones) are partitioned into four consecutive blocks of equal size, and for each fixed row i the rule for ρ keeps exactly two of these blocks of $x_{i,k}$ as live variables while fixing the other two blocks to constants; similarly, for each fixed column j the rule for ρ keeps exactly two blocks of $y_{k,j}$ (see Figures 3 and 4). These two surviving blocks are deliberately misaligned, so that for every pair (i,j) their intersection is contained in a *single* block. Since $z_{i,j,k}$ can only remain potentially nonzero when both $x_{i,k}$ and $y_{k,j}$ survive (based on the definition of ρ, Item 2), it follows that after applying ρ the surviving z-variables (hence the relevant k-columns) for each i and j are confined to one block, i.e. to at most $(n-4)/4$ columns. Formally, we have the following.

Lemma 5.23. *Suppose that $m > n \geq 8$ are integers, 4 divides n, and $A \in \mathbb{F}_2^{m \times m}$ is an m by m matrix over $\mathbb{F}_2$. Let Π be a $\mathsf{PCR}_{\mathbb{F}_2}$ refutation of $\mathsf{BTRank}_n^m(A)$. Then $\Pi \restriction \rho$ is a $\mathsf{PCR}_{\mathbb{F}_2}$ refutation of $\mathsf{BTRank}_{(n-4)/4}^m(A)$.*

Proof. We only need to check how ρ affects (the translations into polynomials of) the clauses of $\mathsf{BTRank}_n^m(A)$. By Items 2 and 3, the clauses of each Output Axiom and each Summation Base Axiom are satisfied by ρ. Equivalently, ρ converts the translation of each such clause into the zero polynomial (which can be removed from $\Pi \restriction \rho$). Further, by Item 2, each of Binary AND Axioms is either satisfied by ρ or turned into the corresponding axiom of $\mathsf{BTRank}_{\tilde{n}}^m(A)$. Next, by Items 2 and 3, Summation Axioms for $k \in \{2, n\}$ are satisfied by ρ.

Consider now a Summation Axiom for $k = n-1$, i.e. the CNF encoding of $u_{i,j,n-1} = u_{i,j,n-2} + z_{i,j,n-1}$. By the definition of ρ, we have $\rho(z_{i,j,n-1}) = p_{i,0}$, and $\rho(u_{i,j,n-1}) = q_{j,0} \oplus A_{i,j}$. If $r_{i,j} = 3$,

we have $\rho(u_{i,j,n-2}) = \tilde{u}_{i,j,\tilde{n}}^{p_{i,0} \oplus q_{j,0} \oplus 1}$, which means that each of the four clauses encoding the axiom is either satisfied or turns into the corresponding Output Axiom clause $\tilde{u}_{i,j,\tilde{n}}^{A_{i,j}}$. If $r_{i,j} \neq 3$, then $\rho(u_{i,j,n-2}) = p_{i,0} \oplus q_{j,0} \oplus A_{i,j}$, and so all four clauses encoding the Summation Axiom are satisfied.

Finally, consider Summation Axioms for $k \in \{3, \ldots, n-2\}$. For $k = r_{i,j}\tilde{n} + 3$, the axiom turns into the corresponding Summation Base Axiom (for either value of $p_{i,0} \oplus q_{j,0}$). For $k \in \{r_{i,j}\tilde{n} + 4, \ldots, (r_{i,j}+1)\tilde{n} + 2\}$, the axiom turns into a Summation Axiom (again, for either value of $p_{i,0} \oplus q_{j,0}$). For $k \in \{3, \ldots, r_{i,j}\tilde{n} + 2\} \cup \{(r_{i,j}+1)\tilde{n} + 3, \ldots, n-2\}$, the Summation Axiom is satisfied by ρ. □

The second random substitution, denoted by σ, is intended to simplify the x-, y- and z-variable occurrences in terms while, again, turning $\mathsf{BTRank}_n^m(A)$ into a smaller instance. In contrast to the substitution ρ, which aims to reduce in each term with high probability the number of *row* indices (of X) appearing through the *u-variables* (as well as to reduce the instance from n to $\tilde{n}$ columns), the goal of σ is to reduce the number of *column* indices (of X and Y^T) involved via the *x-, y- and z-variables*. Applying ρ reduces the range of k-indices that can remain relevant from $[n]$ to a set of size $(n-4)/4$ (Lemma 5.23). However, ρ does not typically imply that a given term will involve only a small number of k-indices after restriction: a term may still mention many different k's within the surviving block via the x-, y-, and z-variables. The purpose of σ is to further reduce, for each term, the number of k-indices that remain unfixed in these variables.

Definition 5.24 (Substitution σ for $\mathsf{BTRank}_n^m(A)$)**.** Assume that $m > n \geq 3$ and $n-1$ is divisible by 2. A random substitution σ is chosen as follows.

1. Choose a subset $S \subseteq [n-1]$ uniformly at random from all $(n-1)/2$-element subsets of $[n-1]$. For each $k \in [n-1] \setminus S$ independently choose $q_k \in \{0,1\}$ at random with $\Pr[q_k = 0] = \Pr[q_k = 1] = 1/2$. For each $k \in S$, define $q_k = *$, and set $q_n = |\{\ell \in [n-1] : q_\ell = 1\}| \bmod 2$. Note that this choice of q_n makes the total number of 1s even, i.e., if for $k \in [n]$ we let $o_k = |\{\ell \in [k] : q_\ell = 1\}| \bmod 2$, then we have $o_n = 0$. Denote by $s_k = |S \cap [k]|$ the number of stars among $q_1, \ldots, q_k$.

2. For each $i, j \in [m]$ and $k \in [n]$, define

$$\sigma(x_{i,k}) = \begin{cases} q_k & \text{if } q_k \in \{0,1\}, \\ \tilde{x}_{i,s_k} & \text{if } q_k = *, \end{cases} \qquad \sigma(y_{k,j}) = \begin{cases} q_k & \text{if } q_k \in \{0,1\}, \\ \tilde{y}_{s_k,j} & \text{if } q_k = *, \end{cases}$$

   and extend σ consistently to the z- and u-variables by

$$\sigma(z_{i,j,k}) = \begin{cases} q_k & \text{if } q_k \in \{0,1\}, \\ \tilde{z}_{i,j,s_k} & \text{if } q_k = *, \end{cases}$$

$$\sigma(u_{i,j,k}) = \begin{cases} o_k & \text{if } k \in \{1, \ldots, \min(S) - 1\}, \\ \tilde{u}_{i,j,s_k}^{o_k \oplus 1} & \text{if } k \in \{\min(S), \ldots, \max(S)\}, \\ A_{i,j} \oplus o_k & \text{if } k \in \{\max(S) + 1, \ldots, n\}. \end{cases}$$

3. For any variable v mapped to 0 or 1 by σ, set $\sigma(\overline{v}) = 1 - \sigma(v)$.

4. For any variable v not mapped to a Boolean constant by σ, set $\sigma(\overline{v}) = \overline{\sigma(v)}$.

Example for Definition 5.24: choosing S and defining q_k, o_k, s_k (here $n = 9$)

k	1	2	3	4	5	6	7	8	9
q_k	1	$*$	0	$*$	1	$*$	0	$*$	0
o_k	1	1	1	1	0	0	0	0	0
s_k	0	1	1	2	2	3	3	4	4

Green $= k \in S$ (so $q_k = *$ survives), Gray $=$ constant bits (fixed by σ).
Here $S = \{2, 4, 6, 8\}$ and q_9 is chosen so that $o_9 = 0$.

Figure 5: A concrete example of the random data in Definition 5.24: the set S, the values q_k, and the derived sequences o_k and $s_k = |S \cap [k]|$.

Example: action of σ on $(x_{i,1}, \ldots, x_{i,9})$

k	1	2	3	4	5	6	7	8	9
$\sigma(x_{i,k})$	q_1	$\tilde{x}_{i,1}$	q_3	$\tilde{x}_{i,2}$	q_5	$\tilde{x}_{i,3}$	q_7	$\tilde{x}_{i,4}$	q_9

Rule: $\sigma(x_{i,k}) = q_k$ if $q_k \in \{0, 1\}$, and $\sigma(x_{i,k}) = \tilde{x}_{i,s_k}$ if $q_k = *$.

Figure 6: Example of σ on the x-variables.

Example: action of σ on $(y_{1,j}, \ldots, y_{9,j})$

k	1	2	3	4	5	6	7	8	9
$\sigma(y_{k,j})$	q_1	$\tilde{y}_{1,j}$	q_3	$\tilde{y}_{2,j}$	q_5	$\tilde{y}_{3,j}$	q_7	$\tilde{y}_{4,j}$	q_9

Rule: $\sigma(y_{k,j}) = q_k$ if $q_k \in \{0, 1\}$, and $\sigma(y_{k,j}) = \tilde{y}_{s_k,j}$ if $q_k = *$.

Figure 7: Example of σ on the y-variables.

Example: action of σ on $(u_{i,j,1}, \ldots, u_{i,j,9})$ (here $a = 2$, $b = 8$)

k	1	2	3	4	5	6	7	8	9
$\sigma(u_{i,j,k})$	o_1	$\tilde{u}_{i,j,s_2}^{o_2 \oplus 1}$	$\tilde{u}_{i,j,s_3}^{o_3 \oplus 1}$	$\tilde{u}_{i,j,s_4}^{o_4 \oplus 1}$	$\tilde{u}_{i,j,s_5}^{o_5 \oplus 1}$	$\tilde{u}_{i,j,s_6}^{o_6 \oplus 1}$	$\tilde{u}_{i,j,s_7}^{o_7 \oplus 1}$	$\tilde{u}_{i,j,s_8}^{o_8 \oplus 1}$	$A_{i,j} \oplus o_9$

Rule: $\sigma(u_{i,j,k}) = o_k$ for $k < a$; $\sigma(u_{i,j,k}) = \tilde{u}_{i,j,s_k}^{o_k \oplus 1}$ for $a \le k \le b$; $\sigma(u_{i,j,k}) = A_{i,j} \oplus o_k$ for $k > b$.

Figure 8: Example of σ on the u-chain (three regions determined by $a = \min(S)$ and $b = \max(S)$).

Definition 5.25. [Column indices mentioned in a term by X, Y and Z variables] Let t be a term in the variables of $\mathsf{BTRank}_n^m(A)$ and let $k \in [n]$. We say that k is *X-column-mentioned in t* if there is $i \in [m]$ and $b \in \{0, 1\}$ such that $x_{i,k}^b$ appears in t. We say that k is *Y^T-column-mentioned in t* if

there is $j \in [m]$ and $b \in \{0,1\}$ such that $y^b_{k,j}$ appears in t. We say that k is *Z-column-mentioned in t* if there are $i, j \in [m]$ and $b \in \{0,1\}$ such that $z^b_{i,j,k}$ appears in t.

Lemma 5.26. *Suppose that $m > n \geq 3$ are integers, 2 divides $n-1$, and $A \in \mathbb{F}_2^{m \times m}$ is an m by m matrix over $\mathbb{F}_2$. Suppose that t is a term in the variables of $\mathsf{BTRank}^m_n(A)$ and $K \subseteq [n-1]$ is a set such that every $k \in K$ is either X-column-mentioned or Y^T-column-mentioned or Z-column-mentioned in t. Then $\Pr[t \restriction \sigma \neq 0] \leq e^{-|K|/16} + 2^{-|K|/4}$.*

Proof. By the definition of σ and the Chernoff bound, $\Pr[|K \setminus S| \leq |K|/4] \leq e^{-|K|/16}$. Assuming $|K \setminus S| > |K|/4$, pick for each $k \in K \setminus S$ a single variable from t witnessing that k is X-column-mentioned or Y^T-column-mentioned or Z-column-mentioned. Notice that σ evaluates these variables independently to 0 or 1, each with probability $1/2$, and only one of at least $2^{|K|/4}$ assignments to these variables may not zero out t. □

Lemma 5.27. *Suppose that $m > n \geq 3$ are integers, 2 divides $n-1$, and $A \in \mathbb{F}_2^{m \times m}$ is an m by m matrix over $\mathbb{F}_2$. Let Π be a $\mathsf{PCR}_{\mathbb{F}_2}$ refutation of $\mathsf{BTRank}^m_n(A)$. Then $\Pi \restriction \sigma$ is a $\mathsf{PCR}_{\mathbb{F}_2}$ refutation of $\mathsf{BTRank}^m_{(n-1)/2}(A)$.*

Proof. We inspect how σ acts on (the translations into polynomials of) the clauses of $\mathsf{BTRank}^m_n(A)$. Considering Output Axioms, we know by Item 1 that $o_n = 0$, and that $n \in \{\max(S)+1, \ldots, n\}$ for any choice of S. Hence by Item 2, $\sigma(u_{i,j,n}) = A_{i,j}$, which means that Output Axioms are satisfied. Next, it is immediate by Item 2 that the Binary AND Axiom for $k \in [n]$ is either satisfied by σ (if $q_k \in \{0,1\}$) or turned into the Binary AND Axiom $\tilde{z}_{i,j,s_k} = \tilde{x}_{i,s_k}\tilde{y}_{s_k,j}$ of $\mathsf{BTRank}^m_{(n-1)/2}(A)$. Further, the Summation Base Axiom is satisfied if $1 \notin S$, since $\sigma(u_{i,j,1}) = o_1 = q_1 = \sigma(z_{i,j,1})$; otherwise $s_1 = 1$ and it turns into a Summation Base Axiom of $\mathsf{BTRank}^m_{(n-1)/2}(A)$.

Next, consider Summation Axioms. For $k \in \{2, \ldots, \min(S)-1\}$ the axiom is satisfied by σ. If $2 \leq k = \min(S)$, then each clause of the axiom is either satisfied or turned into a clause of the Summation Base Axiom of $\mathsf{BTRank}^m_{(n-1)/2}(A)$ (for either value of o_k). For $k \in \{\min(S), \ldots, \max(S)\} \setminus S$, each clause of the axiom is either satisfied or turned into $u_{i,j,s_k} \vee \neg u_{i,j,s_k}$. For $k \in S \setminus \{\min(S)\}$, the axiom turns into the Summation Axiom for s_k of $\mathsf{BTRank}^m_{(n-1)/2}(A)$ (for either value of o_k). For $k = \max(S)+1$, each clause of the axiom is either satisfied or turned into an Output Axiom of $\mathsf{BTRank}^m_{(n-1)/2}(A)$. Finally, for $k \in \{\max(S)+2, \ldots, n\}$, the Summation Axiom is satisfied by σ. □

The next lemma combines Lemmas 5.22, 5.23, 5.26 and 5.27.

Lemma 5.28. *Suppose that $m > n \geq 16$ are integers, 8 divides n, and $A \in \mathbb{F}_2^{m \times m}$ is an m by m matrix over $\mathbb{F}_2$. If Π is a $\mathsf{PCR}_{\mathbb{F}_2}$ refutation of $\mathsf{BTRank}^m_n(A)$ of size s, then there exists a $\mathsf{PCR}_{\mathbb{F}_2}$ refutation Π' of $\mathsf{BTRank}^m_{(n-8)/8}(A)$ of size at most s such that, letting $d = \frac{16}{\log e}(\log s + 1)$, every term t in Π' satisfies the following:*

1. *the number of indices $i \in [m]$ that are U-left-row-mentioned in t is less than d, and*
2. *the number of indices $k \in [\frac{n-8}{8}]$ that are X-column-mentioned or Y^T-column-mentioned or Z-column-mentioned in t is less than d.*

Proof. Applying Lemmas 5.23 and 5.27, let $\Pi_1 = \Pi \restriction \rho$ be a refutation of $\mathsf{BTRank}^m_{(n-4)/4}(A)$ and $\Pi_2 = \Pi_1 \restriction \sigma$ be a refutation of $\mathsf{BTRank}^m_{(n-8)/8}(A)$. A term t violating Item 1 can only appear in Π_2 if $t = (\hat{t} \restriction \rho) \restriction \sigma$ for some term $\hat{t}$ in Π such that there exist a set $I \subseteq [m]$ and a subterm t' of $\hat{t}$ with the following properties: $|I| \geq d$, every $i \in I$ is U-left-row-mentioned in t', and no $k \in \{1, 2, n-1, n\}$ is U-column-mentioned in t'. (The u-variables U-column-mentioning $k \in \{1, 2, n-1, n\}$ can be excluded from t' since they are set to a constant by ρ with probability 1 and hence cannot contribute to a violation of Item 1 by t.) However, for such a term $\hat{t}$ we have $\Pr[\hat{t} \restriction \rho \neq 0] \leq (3/4)^{|I|} \leq (3/4)^d$ by Lemma 5.22.

Similarly, a term t violating Item 2 can only appear in Π_2 if $t = \tilde{t} \restriction \sigma$ for some term $\tilde{t}$ in Π_1 such that there is a set $K \subseteq [\frac{n-4}{4} - 1]$ with $|K| \geq d$ and every $k \in K$ is either X-column-mentioned or Y^T-column-mentioned or Z-column-mentioned in $\tilde{t}$. (The x-, y-, and z-variables

X-, Y^T- or Z-column-mentioning the last column index $\frac{n-4}{4}$ cannot contribute to a violation of Item 2 by t as they are always evaluated to a constant by σ.) For such a term $\tilde{t}$, Lemma 5.26 gives $\Pr[\tilde{t} \restriction \sigma \neq 0] \leq e^{-|K|/16} + 2^{-|K|/4} \leq e^{-d/16} + 2^{-d/4}$.

Denote by T_r the set of all terms $\hat{t}$ in Π defined as above. In the event that all of these terms are zeroed out by ρ, there are at most $s - |T_r|$ terms $\tilde{t}$ in Π_1 defined as above. This is because $\Pi_1 = \Pi \restriction \rho$ has no more terms than Π. By the union bound, the probability that there is a term t in Π_2 that violates Item 1 or Item 2 is upper bounded by $|T_r| \cdot (3/4)^d + (s - |T_r|) \cdot (e^{-d/16} + 2^{-d/4}) \leq s \cdot (e^{-d/16} + 2^{-d/4}) < s \cdot 2^{-\frac{\log e}{16} d + 1} = 1$ for $d = \frac{16}{\log e}(\log s + 1)$. Thus, we can fix some restrictions ρ and σ such that $\Pi' = (\Pi \restriction \rho) \restriction \sigma$ has the required properties. □

Proof of Theorem 5.19. Assuming for a contradiction that a $\mathsf{PCR}_{\mathbb{F}_2}$ refutation Π of size $s < 2^{\frac{\log e}{512} n - 2}$ witnesses that the theorem fails, we let $\tilde{n} = (n-8)/8$ and construct a $\mathsf{PCR}_{\mathbb{F}_2}$ refutation of $\mathsf{FPHP}^m_{\tilde{n}}$ of degree less than $\tilde{n}/2$, thereby contradicting a theorem of Razborov [69]. By Lemma 5.28, there is a $\mathsf{PCR}_{\mathbb{F}_2}$ refutation Π_1 of $\mathsf{BTRank}^m_{\tilde{n}}(A)$ such that Items 1 and 2 hold with $d = \frac{16}{\log e}(\log s + 1) < \frac{n}{32} - \frac{16}{\log e} = \frac{8\tilde{n}+8}{32} - \frac{16}{\log e} < \frac{\tilde{n}}{4} - 10$.

Let τ be the following substitution to the variables of $\mathsf{BTRank}^m_{\tilde{n}}(A)$: $\tau(x_{i,k}) = x_{i,k}$, $\tau(y_{k,j}) = \sum_{i \in [m]} x_{i,k} A_{i,j}$ (that is, τ substitutes $X^T A$ for Y), $\tau(z_{i,j,k}) = \tau(x_{i,k})\tau(y_{k,j})$, and $\tau(u_{i,j,k}) = \sum_{\ell \in [k]} \tau(z_{i,j,\ell})$. Extend τ to negations by $\tau(\overline{v}) = 1 + \tau(v)$ for any variable v of $\mathsf{BTRank}^m_{\tilde{n}}(A)$. Let $\Pi_2 = \Pi_1 \restriction \tau$.

Consider a term t occurring in a proof line of Π_1. We can write $t = t_1 t_2$, where t_1 consists of all x-, y- and z- variables and their twins that appear in t, and t_2 consists of all u-variables and their twins appearing in t.

Claim 5.29. *Every term of the polynomial $t_1 \restriction \tau$ either has a degree less than d, or is a multiple of a Hole Axiom of $\mathsf{FPHP}^m_{\tilde{n}}$.*

Proof. Let C denote the set of all indices $k \in [\tilde{n}]$ that are X-column-mentioned or Y^T-column-mentioned or Z-column-mentioned in t_1. By the choice of Π_1, we have $|C| < d$. Further, it is immediate from the definition of τ that the set $\{k \in [\tilde{n}] : k \text{ is } X\text{-column-mentioned in some term of the polynomial } t_1 \restriction \tau\}$ is a subset of C. Thus, if a term t' in $t_1 \restriction \tau$ has degree at least d, then, by the pigeonhole principle, t' must be a multiple of a Hole Axiom of $\mathsf{FPHP}^m_{\tilde{n}}$. ◇

Claim 5.30. *Every term of the polynomial $t_2 \restriction \tau$ either has a degree less than d, or is a multiple of either a Hole Axiom or a Functionality Axiom of $\mathsf{FPHP}^m_{\tilde{n}}$.*

Proof. Denote by R the set of all indices $i \in [m]$ that are U-left-row-mentioned in t_2. By the choice of Π_1, $|R| < d$. Assume that $u^{1-b}_{i,j,k}$ appears in t_2 for some $i \in R, j \in [m], k \in [\tilde{n}]$ and $b \in \{0,1\}$. Then

$$\begin{aligned}\tau(u^{1-b}_{i,j,k}) &= b + \sum_{\ell \in [k]} \tau(z_{i,j,\ell}) = b + \sum_{\ell \in [k]} \tau(x_{i,\ell})\tau(y_{\ell,j}) = b + \sum_{\ell \in [k]} x_{i,\ell} \sum_{i' \in [m]} x_{i',\ell} A_{i',j} \\ &= b + \sum_{\ell \in [k]} \sum_{i' \in [m]} x_{i,\ell} x_{i',\ell} A_{i',j}.\end{aligned}$$

For every $\ell \in [k]$ and every $i' \in [m]$ such that $i' \neq i$ and $A_{i',j} \neq 0$, the summand $x_{i,\ell} x_{i',\ell} A_{i',j}$ in the last expression is a Hole Axiom. Since such summands only give rise to terms in $t_2 \restriction \tau$ that are multiples of a Hole Axiom, we can continue the above calculation modulo Hole Axioms, obtaining $b + \sum_{\ell \in [k]} x_{i,\ell} x_{i,\ell} A_{i,j} = b + A_{i,j} \sum_{\ell \in [k]} x_{i,\ell}$. Thus, modulo Hole Axioms, $t_2 \restriction \tau$ is either 0 or can be written as a product of degree-1 polynomials of the form

$$b + \sum_{\ell \in [k]} x_{i,\ell},$$

where $b \in \{0,1\}, k \in [\tilde{n}]$, and $i \in R$. Whenever this product gives rise to a term of degree at least d, it follows from $|R| < d$ by the pigeonhole principle that such a term is a multiple of a Functionality Axiom of $\mathsf{FPHP}^m_{\tilde{n}}$. $\diamond$

Combining the two claims, we see that every term of the polynomial $t \restriction \tau = (t_1 \restriction \tau)(t_2 \restriction \tau)$ either has a degree at most $2d$, or is a multiple of either a Hole Axiom or a Functionality Axiom of $\mathsf{FPHP}^m_{\tilde{n}}$. The same conclusion holds for every term appearing in $\Pi_2 = \Pi_1 \restriction \tau$, since t was an arbitrary term occurring in Π_1.

The next step is to transform the sequence of polynomials Π_2 into a $\mathsf{PC}_{\mathbb{F}_2}$ refutation of $\mathsf{FPHP}^m_{\tilde{n}}$.

First, we inspect the effect of τ on the axioms of Π_1. By definition, τ satisfies all Complementarity Axioms. Additionally, τ satisfies the polynomial translation of every clause in the CNF encoding of Binary AND Axioms, Summation Base Axioms, and Summation Axioms. This can be verified by noting that each such clause is a semantic consequence of the algebraic version of the corresponding Binary AND Axiom (i.e., $z_{i,j,k} = x_{i,k}y_{k,j}$ for some $i, j \in [m]$ and $k \in [n]$), Summation Base Axiom (i.e., $u_{i,j,1} = z_{i,j,1}$ for some $i, j \in [m]$), or Summation Axiom (i.e., $u_{i,j,k} = u_{i,j,k-1} + z_{i,j,k}$ for some $i, j \in [m]$ and $k \in \{2, \ldots, n\}$), and all of these are clearly satisfied by τ.

Each Output Axiom in Π_1 is converted by τ into one of the axioms algebraically encoding $XX^TA = A$. Each of the latter axioms is a sum of some axioms of $XX^T = I_m$, which is the algebraic oddtown formula $\mathsf{OT}^m_{\tilde{n}}$. Each of the axioms of $\mathsf{OT}^m_{\tilde{n}}$ is a sum of some axioms of $\mathsf{FPHP}^m_{\tilde{n}}$. We append the degree-2 derivation just described to each axiom in Π_2 that is the result of an application of τ to an Output Axiom in Π_1.

Next, we examine the non-axiom proof lines of Π_1. The addition rule is not affected by τ, since if a polynomial p was inferred in Π_1 as a sum of q and r, then $p \restriction \tau$ is a sum of $q \restriction \tau$ and $r \restriction \tau$. Regarding the multiplication rule, suppose that p and q are proof lines in Π_1, and let p be inferred from q by multiplying q with v, where v is a variable or the negation of a variable of $\mathsf{BTRank}^m_{\tilde{n}}(A)$. Then $p \restriction \tau = (q \restriction \tau)(v \restriction \tau)$, and $v \restriction \tau$ is a polynomial of degree at most 2. We add to Π_2 a derivation of $p \restriction \tau$ from $q \restriction \tau$, each term of which is a term of $q \restriction \tau$ multiplied by at most two variables.

Let Π_3 denote the sequence of polynomials resulting from Π_2 by the modifications introduced in the last two paragraphs. It follows that Π_3 is a $\mathsf{PC}_{\mathbb{F}_2}$ refutation of $\mathsf{FPHP}^m_{\tilde{n}}$. Moreover, every term appearing in Π_3 either has a degree at most $2d + 2$, or is a multiple of either a Hole Axiom or a Functionality Axiom of $\mathsf{FPHP}^m_{\tilde{n}}$.

Finally, using Hole Axioms and Functionality Axioms of $\mathsf{FPHP}^m_{\tilde{n}}$, we transform Π_3 into a $\mathsf{PC}_{\mathbb{F}_2}$ refutation of $\mathsf{FPHP}^m_{\tilde{n}}$ in which each term has a degree at most $2d + 3 \leq \frac{\tilde{n}}{2} - 17 < \frac{\tilde{n}}{2}$, which is the desired contradiction. This can be done as follows. Delete from Π_3 each term that is a multiple of either a Hole Axiom or a Functionality Axiom. Then, for each line p that is an incorrect conclusion of the multiplication rule—which can only happen if p is missing some terms each of degree at most $2d + 3$ and having either exactly one row mentioned twice or exactly one column mentioned twice—insert the correct conclusion p' of the rule before p and use Functionality Axioms and Hole Axioms to derive p from p'. $\square$

5.4 Iterated Generators

In the previous sections, we proved that the low-rank generator $g\colon \mathbb{F}_2^{2mn} \to \mathbb{F}_2^{m^2}$ is a hard proof complexity generator against $\mathsf{PCR}_{\mathbb{F}_2}$. However, even when m is arbitrarily large compared to n, the stretch of this generator is at most quadratic. In this section, we *iterate* g (in the sense of [50, 73]) to obtain a proof complexity generator of arbitrarily large stretch that is still hard against $\mathsf{PCR}_{\mathbb{F}_2}$.

5.4.1 Iterability of $\mathsf{Rank}^m_n(A)$

Here we iterate the algebraic version of the rank principle. We will use a more limited notion of iterability, which is sufficient for the argument used by Razborov in [73].

We will denote by $\Sigma^{\leq \kappa}$ the set of strings of length at most h over the alphabet Σ. Similarly, $\Sigma^{< \kappa}$ denotes the strings of length less than h over the alphabet Σ. We use () to denote the empty

string.

Definition 5.31 (The iterated formula $\mathsf{IRank}_n^m(\mathbf{A}, \kappa, \Sigma)$)**.** Let $m > n > 0$ and $\kappa \geq 0$ be integer parameters and Σ a finite alphabet. For every string $\pi \in \Sigma^{\leq \kappa}$, let $X^{(\pi)} = (x_{i,k}^{(\pi)})_{i\in[m],k\in[n]}$ be a variable matrix. Let $Y = (y_{k,i})_{k\in[n],i\in[m]}$ be a variable matrix. Let $\mathbf{A} = \{A^{(\pi)} : \pi \in \Sigma^{\leq \kappa}\}$ be a collection of $m \times m$ matrices, where, for every $\pi \in \Sigma^{\leq \kappa}$ and $i, j \in [m]$, the entry $A_{i,j}^{(\pi)}$ is either a Boolean constant or a variable from $X^{(\pi')}$ for some $\pi' \in \Sigma^{\leq \kappa}$ with $|\pi'| > |\pi|$. In particular, all entries of $A^{(\pi)}$, where $\pi \in \Sigma^{\kappa}$, are constant. The *iterated rank formula* $\mathsf{IRank}_n^m(\mathbf{A}, \kappa, \Sigma)$ is the polynomial system $\bigcup_{\pi\in\Sigma^{\leq\kappa}} X^{(\pi)}Y = A^{(\pi)}$.

Note that the formula $\mathsf{IRank}_n^m(\mathbf{A}, 0, \Sigma)$, where $\mathbf{A} = \{A^{()}\}$, is the formula $\mathsf{Rank}_n^m(A^{()})$. The iteration structure differs from the iteration from [50, 73]: here we impose that different copies of Rank form a $|\Sigma|$-ary tree, whereas the original definition assumes the flat linear structure, i.e., $|\Sigma| = 1$. Our lower bound will depend on the number of iterations κ, and for the application, we will need Σ with $|\Sigma| = n^{\Omega(1)}$.

We need the following measure, which describes how many rows are mentioned in a term.

Definition 5.32. Let t be a term in the variables of $\mathsf{IRank}_n^m(\mathbf{A}, \kappa, \Sigma)$. We say that $i \in [m]$ is *$X^{(\pi)}$-row-mentioned in t* if there is $k \in [n]$ such that $x_{i,k}^{(\pi)}$ or $\overline{x}_{i,k}^{(\pi)}$ appears in t. We say that $j \in [m]$ is *Y^T-row-mentioned in t* if there is $k \in [n]$ such that $y_{k,j}$ or $\overline{y}_{k,j}$ appears in t.

Definition 5.33 (Row degree)**.** Let t be a term in the variables of $\mathsf{IRank}_n^m(\mathbf{A}, \kappa, \Sigma)$. For every $\pi \in \Sigma^{\leq \kappa}$, let $I^{(\pi)}$ be the set of all $i \in [m]$ that are $X^{(\pi)}$-row-mentioned in t. Similarly, let J be the set of all $j \in [m]$ that are Y^T-row-mentioned in t. We say that t *mentions* rows $(\{I^{(\pi)} : \pi \in \Sigma^{\leq \kappa}\}, J)$. The *row degree* of t is defined as the sum $\sum_{\pi\in\Sigma^{\leq\kappa}} |I^{(\pi)}| + |J|$.

We will construct the restriction that w.h.p. evaluates to zero any term with a large row degree. We need the following auxiliary matrices.

$$\mathcal{D} = \begin{pmatrix} 1 & * & 1 & 0 & 0 & * & * & * \\ 0 & 1 & * & 1 & * & * & * & 0 \\ * & * & 0 & * & 1 & 0 & 1 & * \\ * & 0 & * & * & * & 1 & 0 & 1 \end{pmatrix}, \quad \mathcal{E} = \begin{pmatrix} 1 & 0 & 0 & 1 & * & * & * & * \\ 0 & * & 1 & * & 1 & * & 0 & * \\ * & 1 & * & 0 & * & 0 & * & 1 \\ * & * & * & * & 0 & 1 & 1 & 0 \end{pmatrix}.$$

We will construct a random substitution ρ to reduce the row degree, and then follow with a substitution σ to reduce the total degree.

Definition 5.34 (Substitution ρ)**.** Assume $m > n \geq 16$ and n divisible by 16. Let $\tilde{n} = n/8$ and then let $\tilde{X}^{(\pi)} = (\tilde{x}_{i,k}^{(\pi)})_{i\in[m],k\in[\tilde{n}}$, where $\pi \in \Sigma^{\leq \kappa}$, and $\tilde{Y} = (\tilde{y}_{k,i})_{k\in[\tilde{n}],i\in[m]}$ be fresh variables. A random substitution ρ is chosen as follows.

1. For each $i \in [m]$ uniformly and independently sample $r_i^{(\pi)} \in [4]$, where $\pi \in \Sigma^{\leq \kappa}$, and $s_i \in [4]$.
2. For each $\pi \in \Sigma^{\leq \kappa}$, $i \in [m]$ and $k \in [n]$, let $\nu = \lfloor \frac{k-1}{\tilde{n}} \rfloor + 1$ and set
$$\rho(x_{i,k}^{(\pi)}) = \begin{cases} \tilde{x}_{i,((k-1) \bmod \tilde{n})+1}^{(\pi)} & \text{if } \mathcal{D}_{r_i^{(\pi)},\nu} = *, \\ \mathcal{D}_{r_i^{(\pi)},\nu} & \text{if } \mathcal{D}_{r_i^{(\pi)},\nu} \in \{0,1\}. \end{cases}$$
3. For each $j \in [m]$ and $k \in [n]$, let $\nu = \lfloor \frac{k-1}{\tilde{n}} \rfloor + 1$ and set
$$\rho(y_{k,j}) = \begin{cases} \tilde{y}_{((k-1) \bmod \tilde{n})+1,j} & \text{if } \mathcal{E}_{s_j,\nu} = *, \\ \mathcal{E}_{s_j,\nu} & \text{if } \mathcal{E}_{s_j,\nu} \in \{0,1\}. \end{cases}$$
4. For any variable θ mapped to 0 or 1 by ρ, set $\rho(\overline{\theta}) = 1 - \rho(\theta)$.

5. For any variable θ not mapped to a Boolean constant by ρ, set $\rho(\overline{\theta}) = \overline{\rho(\theta)}$.

Lemma 5.35. *Assume $\kappa \geq 0$, $m > n \geq 16$, n divisible by 16 and $\mathbf{A} = \{A^{(\pi)} : \pi \in \Sigma^{\leq\kappa}\}$ is a collection of $m \times m$ matrices as in the definition of IRank. Let t be a term in the variables of $\mathsf{IRank}_n^m(\mathbf{A}, \kappa, \Sigma)$ that mentions rows $(\{I^{(\pi)} : \pi \in \Sigma^{\leq\kappa}\}, J)$. Then $\Pr[t \restriction \rho \neq 0] \leq (3/4)^{\sum_{\pi\in\Sigma^{\leq\kappa}} |I^{(\pi)}|+|J|}$.*

Proof. Assume w.l.o.g. that for each i from the set $I^{(\pi)}$ there is a single variable $\gamma_i^{(\pi)}$ in t that mentions row i, and for each j from the set J there is a single variable δ_k in t. Let $\Gamma_i^{(\pi)}$ be the event that $(\gamma_i^{(\pi)} \restriction \rho \neq 0)$ and Δ_k the event that $(\delta_k \restriction \rho \neq 0)$. Then $\bigcup_{\pi\in\Sigma^{\leq\kappa}}\{\Gamma_i^{(\pi)} : i \in I^{(\pi)}\} \cup \{\Delta_k : k \in K\}$ is a set mutually independent events and each of them happens with probability at most $3/4$. □

The substitution ρ transforms any refutation of $\mathsf{IRank}_n^m(\mathbf{A}, \kappa, \Sigma)$ into a refutation of $\mathsf{IRank}_n^m(\mathbf{A} \restriction \rho, \kappa, \Sigma)$.

Lemma 5.36. *Assume $\kappa \geq 0$, $m > n \geq 16$, n is divisible by 16 and $\mathbf{A} = \{A^{(\pi)} : \pi \in \Sigma^{\leq\kappa}\}$ is a collection of $m \times m$ matrices as in the definition of IRank. Let $\tilde{\mathbf{A}}$ be a collection of matrices defined as*

$$\tilde{\mathbf{A}} = \{A^{(\pi)} \restriction \rho : \pi \in \Sigma^{\leq\kappa}\}.$$

Then for every $\mathsf{PCR}_{\mathbb{F}_2}$ refutation Π of $\mathsf{IRank}_n^m(\mathbf{A}, \kappa, \Sigma)$, $\Pi \restriction \rho$ is a refutation of $\mathsf{IRank}_{n/8}^m(\tilde{\mathbf{A}}, \kappa, \Sigma)$.

Proof. The proof is straightforward: each axiom $\sum_{k\in[n]} x_{i,k}^{(\pi)} y_{k,j} = A_{i,j}$ of $\mathsf{IRank}_n^m(\mathbf{A}, \kappa, \Sigma)$ transforms into an axiom $\sum_{k\in[n/8]} \tilde{x}_{i,k}^{(\pi)} \tilde{y}_{k,j} = \tilde{A}_{i,j}$ of $\mathsf{IRank}_{n/8}^m(\tilde{\mathbf{A}}, \kappa, \Sigma)$. □

We also construct a substitution σ that reduces the total degree of any term with small row degree. The construction is analogous to Definition 5.4.

Definition 5.37 (Substitution σ)**.** Assume $\kappa \geq 0$, $m > n \geq 2$ and $\mathbf{A} = \{A^{(\pi)} : \pi \in \Sigma^{\leq\kappa}\}$ is a collection of $m \times m$ matrices as in the definition of IRank. A random substitution σ is chosen as follows.

1. For each $k \in [n-1]$, uniformly and independently sample $c_k \in \{*, 1, 0\}$. Then set $c_n = |\{k \in [n-1] : c_k = 1\}| \bmod 2$. This guarantees that $|\{k \in [n] : c_k = 1\}|$ is even.
2. Let $\tilde{n} = |\{k \in [n] : c_k = *\}|$ and let $\tilde{X}^{(\pi)} = (\tilde{x}_{i,k}^{(\pi)})_{i\in[m],k\in[\tilde{n}]}$, where $\pi \in \Sigma^{\leq\kappa}$, and $\tilde{Y} = (\tilde{y}_{k,j})_{k\in[\tilde{n}],j\in[m]}$ be fresh variables.
3. Let ι be a bijection between $\{k \in [n] : c_k = *\}$ and $[\tilde{n}]$.
4. For each $\pi \in \Sigma^{\leq\kappa}$, $i \in [m]$ and $k \in [n]$ set

$$\sigma(x_{i,k}^{(\pi)}) = \begin{cases} \tilde{x}_{i,\iota(k)}^{(\pi)} & \text{if } c_k = *, \\ c_k & \text{if } c_k \in \{0,1\}. \end{cases}$$

5. For each $j \in [m]$ and $k \in [n]$ set

$$\sigma(y_{k,j}) = \begin{cases} \tilde{y}_{\iota(k),j} & \text{if } c_k = *, \\ c_k & \text{if } c_k \in \{0,1\}. \end{cases}$$

6. For any variable θ mapped to 0 or 1 by σ, set $\sigma(\overline{\theta}) = 1 - \sigma(\theta)$.
7. For any variable θ not mapped to a Boolean constant by σ, set $\sigma(\overline{\theta}) = \overline{\sigma(\theta)}$.

σ behaves similarly to the substitution from Definition 5.4. We have the following analogue of Lemma 5.5.

Lemma 5.38. *Assume $\kappa \geq 0$, $m > n \geq 2$ and $\mathbf{A} = \{A^{(\pi)} : \pi \in \Sigma^{\leq \kappa}\}$ is a collection of $m \times m$ matrices as in the definition of* IRank. *Let t be a term in the variables of $\mathsf{IRank}_n^m(\mathbf{A}, \kappa, \Sigma)$ of degree d that mentions rows $(\{I^{(\pi)} : \pi \in \Sigma^{\leq \kappa}\}, J)$. Then $\Pr[t \restriction \sigma \neq 0] \leq (2/3)^{\frac{d}{2(\sum_{\pi \in \Sigma^{\leq \kappa}} |I^{(\pi)}| + |J|)}}$.*

Furthermore, $\Pr[\tilde{n} < (n-1)/6)] \leq e^{-\frac{n-1}{24}}$.

Proof. Let $K^{(\pi)}$ be the set of all $k \in [n]$ such that for some $i \in [m]$, either $x_{i,k}^{(\pi)}$ or $\overline{x}_{i,k}^{(\pi)}$ appears in t. Let L be the set of all $\ell \in [n]$ such that for some $j \in [m]$, either $y_{\ell,j}$ or $\overline{y}_{\ell,j}$ appears in t.

The degree of t is then upper-bounded by

$$2\left(\sum_{\pi \in \Sigma^{\leq \kappa}} |I^{(\pi)}| \cdot |K^{(\pi)}| + |J| \cdot |L|\right) \leq 2\left(\sum_{\pi \in \Sigma^{\leq \kappa}} |I^{(\pi)}| + |J|\right) \cdot \max(\{|K^{(\pi)}| : \pi \in \Sigma^{\leq \kappa}\} \cup \{|L|\})$$

By the pigeonhole principle, one of the sets $\{K^{(\pi)} : \pi \in \Sigma^{\leq \kappa}\} \cup \{L\}$ must have size at least $d' = \frac{d}{2(\sum_{\pi \in \Sigma^{\leq \kappa}} |I^{(\pi)}| + |J|)}$. Let S be such a set and $\{\gamma_s : s \in S\}$ some variables in t corresponding to S. For every $s \in S$, let Γ_s be the event that $(\gamma_s \restriction \sigma \neq 0)$. Then $\{\Gamma_s : s \in S\}$ is a set of d' mutually independent events, each of which happens with probability at most $2/3$.

The proof of the latter statement is the same as the proof of Lemma 5.5. □

The substitution σ transforms any refutation of $\mathsf{IRank}_n^m(\mathbf{A}, \kappa, \Sigma)$ into a refutation of $\mathsf{IRank}_{\tilde{n}}^m(\mathbf{A} \restriction \sigma, \kappa, \Sigma)$.

Lemma 5.39. *Assume $\kappa \geq 0$, $m > n \geq 2$ and $\mathbf{A} = \{A^{(\pi)} : \pi \in \Sigma^{\leq \kappa}\}$ is a collection of $m \times m$ matrices as in the definition of* IRank. *Let $\tilde{\mathbf{A}}$ be a collection of matrices defined as*

$$\tilde{\mathbf{A}} = \{A^{(\pi)} \restriction \sigma : \pi \in \Sigma^{\leq \kappa}\}.$$

Then for every $\mathsf{PCR}_{\mathbb{F}_2}$ refutation Π of $\mathsf{IRank}_n^m(\mathbf{A}, \kappa, \Sigma)$, $\Pi \restriction \sigma$ is a refutation of $\mathsf{IRank}_{n/8}^m(\tilde{\mathbf{A}}, \kappa, \Sigma)$.

Proof. The proof is the same as the proof of Lemma 5.6. □

We also give a lower bound on the degree of $\mathsf{PCR}_{\mathbb{F}_2}$ refutations of $\mathsf{IRank}_n^m(\mathbf{A}, \kappa, \Sigma)$ by constructing a reduction to a single copy of $\mathsf{Rank}_n^m(I_m)$.

Definition 5.40 (Reduction τ)**.** Assume $\kappa \geq 0$, $m > n > 0$. Let $X = (x_{i,k})_{i \in [m], k \in [n]}$ be fresh variables. A substitution τ is defined inductively on $|\pi|$ in decreasing order.

1. For each $i \in [m]$ and $k \in [n]$ set

$$\tau(x_{i,k}^{(\pi)}) = ((A^{(\pi)} \restriction \tau)X)_{i,k} = \sum_{s \in [m]} \tau(A_{i,s}^{(\pi)}) x_{s,k},$$

$$\tau(y_{k,i}) = y_{k,i}.$$

2. For any variable θ, set $\tau(\overline{\theta}) = 1 - \tau(\theta)$[5].

Note that $A^{(\pi)} \restriction \tau = A^{(\pi)}$ for every $\pi \in \Sigma^{\kappa}$ since the entries of $A^{(\pi)}$ can only be constant.

Lemma 5.41. *Assume $\kappa \geq 0$, $m > n > 0$ and $\mathbf{A} = \{A^{(\pi)} : \pi \in \Sigma^{\leq \kappa}\}$ is a collection of $m \times m$ matrices as in the definition of* IRank. *Then for any $\mathsf{PCR}_{\mathbb{F}_2}$ refutation Π of $\mathsf{IRank}_n^m(\mathbf{A}, \kappa, \Sigma)$ with degree d, $\Pi\tau$ can be transformed into a refutation of $\mathsf{Rank}_n^m(I_m)$ with degree at most $d(\kappa + 1)$.*

Proof. Let Π be a $\mathsf{PCR}_{\mathbb{F}_2}$ refutation of $\mathsf{IRank}_n^m(\mathbf{A}, \kappa, \Sigma)$.

It follows by induction on $|\pi|$, that for every $\pi \in \Sigma^{\leq \kappa}$, $i \in [m]$, and $k \in [n]$, $\tau(x_{i,k}^{(\pi)})$ (and thus $\tau(\overline{x_{i,k}^{(\pi)}})$) is a polynomial of degree at most $\kappa - |\pi| + 1$.

[5]The proof size may increase arbitrarily after applying such a substitution; however, the degree can at most double. The resulting refutation will still be a PC refutation.

It implies that all polynomials from $\mathsf{IRank}_n^m(\mathbf{A}, \kappa, \Sigma) \restriction \tau$ can be easily derived from the axioms of $\mathsf{Rank}_n^m(I_m)$.

Claim 5.42. *Every polynomial from* $\mathsf{IRank}_n^m(\mathbf{A}, \kappa, \Sigma) \restriction \tau$ *has a degree-*$(\kappa + 2)$ *proof from* $\mathsf{Rank}_n^m(I_m)$.

Proof. Fix $\pi \in \Sigma^{\leq \kappa}$. As shown above, all the entries of $A^{(\pi)} \restriction \tau$ are polynomials of degree at most $\kappa - |\pi|$.

Let $i, j \in [m]$. The (i, j)th axiom of $\mathsf{IRank}_n^m(\mathbf{A}, \kappa, \Sigma)$ under τ transforms as follows

$$\begin{aligned}\left(\sum_{k\in[n]} x_{i,k}^{(\pi)} y_{k,j} + A_{i,j}^{(\pi)}\right) \restriction \tau &= \sum_{k\in[n]} \left(\sum_{s\in[m]} \tau(A_{i,s}^{(\pi)}) x_{s,k}\right) y_{k,j} + \tau(A_{i,j}^{(\pi)}) \\ &= \sum_{s\in[m]} \tau(A_{i,s}^{(\pi)}) \left(\sum_{k\in[n]} x_{s,k} y_{k,j}\right) + \tau(A_{i,j}^{(\pi)}) \\ &= \sum_{s\in[m]\setminus\{j\}} \tau(A_{i,s}^{(\pi)}) \left(\sum_{k\in[n]} x_{s,k} y_{k,j}\right) + \tau(A_{i,j}^{(\pi)}) \left(\sum_{k\in[n']} x_{j,k} y_{k,j} + 1\right),\end{aligned}$$

which is trivially derivation of degree at most $\kappa - |\pi| + 2$ from $\mathsf{Rank}_n^m(I_m)$. ◇

Thus, we can extend $\Pi \restriction \tau$ to a refutation of $\mathsf{Rank}_n^m(I_m)$ of degree at most $d(\kappa + 1)$. □

Now we have all the components for proving the lower bound on the iterated formula $\mathsf{IRank}_n^m(\mathbf{A}, \kappa, \Sigma)$.

Theorem 5.43. *Assume* $\kappa > 0$, $m > n \geq 8 + 192(\kappa + 1)$, $(n - 8)$ *is divisible by* $192(\kappa + 1)$ *and* $\mathbf{A} = \{A^{(\pi)} : \pi \in \Sigma^{\leq \kappa}\}$ *is a collection of* $m \times m$ *matrices as in the definition of* IRank. *Then any* $\mathsf{PCR}_{\mathbb{F}_2}$ *refutation of* $\mathsf{IRank}_n^m(\mathbf{A}, \kappa, \Sigma)$ *requires size* $2^{\Omega(\sqrt{n/h})}$.

Proof. Let

$$d_1 = \frac{n - 8}{192(\kappa + 1)},$$
$$d_2 = \sqrt{d_1} = \sqrt{\frac{n - 8}{192(\kappa + 1)}}.$$

Assume, for the sake of contradiction, that $\mathsf{IRank}_n^m(\mathbf{A}, \kappa, \Sigma)$ has a refutation Π of size less than $(4/3)^{d_2} = 2^{\Theta(\sqrt{n/h})}$.

By the union bound and Lemmas 5.35 and 5.36, there exists a substitution ρ such that $\Pi \restriction \rho$ has *row degree* less than d_2, and it is a refutation of $\mathsf{IRank}_{n/8}^m(\mathbf{A} \restriction \rho, \kappa), \Sigma$.

By the union bound and Lemmas 5.38 and 5.39 (with $d = d_1$), there exists a substitution σ such that every term of $\Pi \restriction \rho \restriction \sigma$ has *degree* less than $2d_1$, and, furthermore, $\Pi \restriction \rho \restriction \sigma$ is a refutation of $\mathsf{IRank}_{\tilde{n}}^m(\mathbf{A} \restriction \rho \restriction \sigma, \kappa, \Sigma)$ with $\tilde{n} \geq \frac{n/8-1}{6} = \frac{n-8}{48}$.

By Lemma 5.41, we can extend $\Pi \restriction \rho \restriction \sigma \restriction \tau$ to a refutation of $\mathsf{Rank}_{\tilde{n}}^m(I_m)$ with degree less than $2d_1(\kappa + 1) \leq \tilde{n}/2$, which contradicts Lemma 5.3. □

5.4.2 Iterability of $\mathsf{BTRank}_n^m(A)$

Definition 5.44. Given two sequences $(a_1, \ldots, a_n)$ and $(b_1, \ldots, b_m)$, we write $a \cup b$ to denote their concatenation $(a_1, \ldots, a_n, b_1, \ldots, b_m)$.

Here we define a specific variant of the rank principle, where the structure of the matrix Y is based on a graph. When this graph is an expander, each axiom $\sum_k x_{i,k} y_{k,j}$ depends only on a few entries and therefore does not require too many extension variables. Formally, the instance is defined as follows.

Definition 5.45 (The iterated formula $\psi_G(\mathbf{A}, \kappa)$)**.** Let $m, n > 0$ and $\kappa \geq 0$ be integer parameters and let G be an $m \times n$ bipartite graph.

We define a formula $\psi_G(\mathbf{A}, \kappa)$ that encodes the statement of the form $\bigcup_{\pi \in \{0,1\}^{\leq \kappa}} X^{(\pi)} Y^{(\pi)} = A^{(\pi)}$, using extension variables that form a binary tree to compute partial parities. The structure of each matrix $Y^{(\pi)}$ is based on G.

The formula uses the following variables:

$$\bigcup_{\pi \in \{0,1\}^{\leq \kappa}} \Bigg[\bigcup_{\mu \in [4]} \Bigg(\{x_{i,k}^{(\pi,\mu)} : i \in [m], k \in [n]\} \\ \cup \{y_{k,j}^{(\pi,\mu)} : j \in [m], k \in \mathcal{N}_G(j)\} \\ \cup \{z_{i,j,k}^{(\pi,\mu)} : i, j \in [m], k \in \mathcal{N}_G(j)\} \\ \cup \{u_{i,j,\Sigma}^{(\pi,\mu)} : i, j \in [m], \Sigma \text{ is a non-empty initial segment of } \mathcal{N}_G(j)\} \Bigg) \\ \cup \{w_{i,j,\ell}^{(\pi)} : i, j \in [m], \ell \in \{0,1,2\}\} \Bigg].$$

Let $\mathbf{A} = \{A^{(\pi)} : \pi \in \{0,1\}^{\leq \kappa}\}$ be a collection of $m \times m$ matrices, where, for every $\pi \in \{0,1\}^{\leq \kappa}$ and $i, j \in [m]$, the entry $A_{i,j}^{(\pi)}$ is either a Boolean constant or a variable of the form $x_{i',k'}^{(\pi',\mu')}$ or $y_{k',j'}^{(\pi',\mu')}$ for some $i', j' \in [m]$, $k' \in [n]$, $\mu' \in [4]$ and $\pi' \in \{0,1\}^{\leq \kappa}$ with $|\pi'| > |\pi|$. In particular, all entries of $A^{(\pi)}$, where $\pi \in \{0,1\}^{\kappa}$, are constant.

The *iterated formula* $\psi_G(\mathbf{A}, \kappa)$ is a polynomial system consisting of the following axioms.

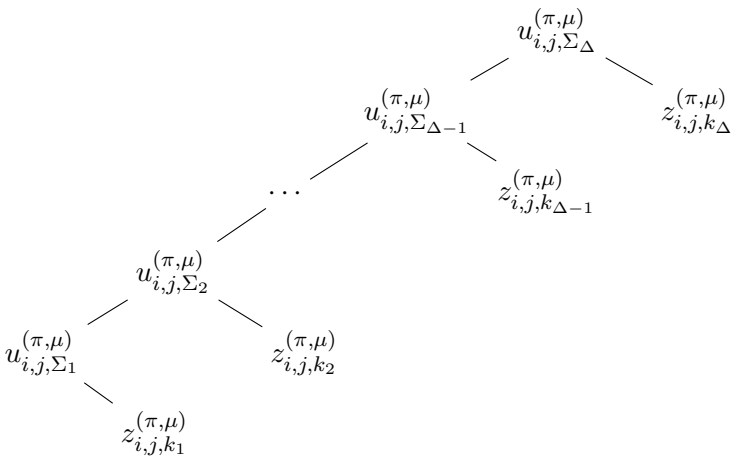
Binary AND Axiom: For every $\pi \in \{0,1\}^{\leq \kappa}$, $\mu \in [4]$, $i, j \in [m]$, $k \in \mathcal{N}_G(j)$, the polynomial $z_{i,j,k}^{(\pi,\mu)} = x_{i,k}^{(\pi,\mu)} y_{k,j}^{(\pi,\mu)}$.

Summation Base Axiom: For every $\pi \in \{0,1\}^{\leq \kappa}$, $\mu \in [4]$, $i, j \in [m]$, the polynomial $u_{i,j,(1)}^{(\pi,\mu)} = z_{i,j,1}^{(\pi,\mu)}$.

Summation Axiom: For every $\pi \in \{0,1\}^{\leq \kappa}$, $i, j \in [m]$ and every initial segment $\Sigma \cup (k)$ of $\mathcal{N}_G(j)$ with $\Sigma \neq \varnothing$, the polynomial

$$u_{i,j,\Sigma \cup (k)}^{(\pi,\mu)} = u_{i,j,\Sigma}^{(\pi,\mu)} \oplus z_{i,j,k}^{(\pi,\mu)}.$$

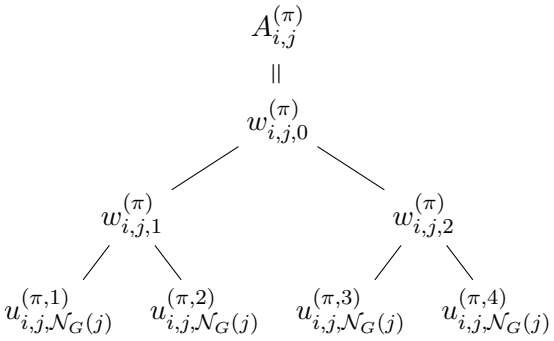
Graphically, the last two types of axioms can be represented as follows. Let $\mathcal{N}_G(j) = (k_1, \ldots, k_\Delta)$, $\Sigma_1 = (k_1)$ and for every $\ell \in \{2, \ldots, \Delta\}$, $\Sigma_\ell = \Sigma_{\ell-1} \cup (k_\ell)$. Then they form the bamboo tree as follows.



Output Axioms: For every $\pi \in \{0,1\}^{\leq \kappa}$, $i, j \in [m]$, the following four axioms:

$$\begin{aligned} w^{(\pi)}_{i,j,1} &= u^{(\pi,1)}_{i,j,\mathcal{N}_G(j)} \oplus u^{(\pi,2)}_{i,j,\mathcal{N}_G(j)}, \\ w^{(\pi)}_{i,j,2} &= u^{(\pi,3)}_{i,j,\mathcal{N}_G(j)} \oplus u^{(\pi,4)}_{i,j,\mathcal{N}_G(j)}, \\ w^{(\pi)}_{i,j,0} &= w^{(\pi)}_{i,j,1} \oplus w^{(\pi)}_{i,j,2}, \\ w^{(\pi)}_{i,j,0} &= A^{(\pi)}_{i,j}. \end{aligned}$$

Graphically, these axioms can be represented as follows.



Although we defined $\psi_G(\mathbf{A}, \kappa)$ as a polynomial system, it can be easily encoded as a CNF since each axiom of $\psi_G(\mathbf{A}, \kappa)$ depends only on a constant number of variables.

We will also need the following lower bound on the PC degree of $\mathsf{FPHP}(G)$.

Proposition 5.46 ([55])**.** *Let G be an (r, c)-boundary expander with left-degree at most Δ_{max}. Then any $\mathsf{PCR}_{\mathbb{F}}$ refutation of $\mathsf{FPHP}(G)$ requires degree strictly larger than $\frac{cr}{2\Delta_{max}}$.*

In our applications, we assume the setting from Lemma 4.15 to simplify the computations.

Given a term t and $\theta_1, \ldots, \theta_k \in \{x, y, z, u, w\}$, let $t_{\theta_1,\ldots,\theta_k}$ be the projection of t on the corresponding variables.

Definition 5.47. Let t be a term in the variables of $\psi_G(\mathbf{A}, \kappa)$. We say that $i \in [m]$ is *$U^{(\pi)}$-left-row-mentioned in t* if there are $\mu \in [4]$, $j \in [m]$ and $k \in [n]$ such that $u^{(\pi)}_{i,j,k}$ or $\overline{u}^{(\pi)}_{i,j,k}$ appears in t. We say that $j \in [m]$ is *$U^{(\pi)}$-right-row-mentioned in t* if there are $\mu \in [4]$, $i \in [m]$ and $k \in [n]$ such that $u^{(\pi)}_{i,j,k}$ or $\overline{u}^{(\pi)}_{i,j,k}$ appears in t.

We begin by defining a restriction ρ_1 that w.h.p. eliminates any term t that $U^{(\pi)}$-left-row-mentions or $U^{(\pi)}$-right-row-mention a lot of rows. Moreover, it is defined such that ρ_1 substitutes all w-variables with either constants or x- or y-variables. The construction uses the following auxiliary matrices.

$$\mathcal{B} = \begin{pmatrix} * & * & 0 & 0 \\ 0 & 0 & * & * \end{pmatrix}, \quad \mathcal{C} = \begin{pmatrix} * & 0 & * & 0 \\ 0 & * & 0 & * \end{pmatrix}.$$

We will define ρ_1 only for graphs with two all-ones columns in their adjacency matrix.

Definition 5.48 (Graph $P(G)$)**.** Let $m, n > 0$ and let G be an $m \times n$ bipartite graph. Given an adjacency matrix M_G of G, define $P(G)$ as the $m \times (n+2)$ bipartite graph with the adjacency matrix

$$M_{P(G)} = \begin{bmatrix} 1 & 1 & \\ \vdots & \vdots & M_G \\ 1 & 1 & \end{bmatrix}.$$

Definition 5.49 (Substitution ρ_1 for $\psi_{P(G)}(\mathbf{A}, \kappa)$)**.** Let $\kappa \geq 0$, $m, n > 0$ and let G be an $m \times n$ bipartite graph with parts $[m]$ and $[n]$.

For every $\pi \in \{0,1\}^{\leq\kappa}$, let $\{x_{i,k}^{(\pi)} : i \in [m], k \in [n]\}$, $\{y_{k,j}^{(\pi)} : j \in [m], k \in \mathcal{N}_G(j)\}$, $\{z_{i,j,k}^{(\pi)} : i,j \in [m], k \in \mathcal{N}_G(j)\}$ and $\{u_{i,j,\Sigma}^{(\pi)} : i,j \in [m], \Sigma \text{ is a non-empty initial segment of } \mathcal{N}_G(j)\}$ be fresh variables. The random substitution ρ_1 for $\psi_{P(G)}(\mathbf{A},\kappa)$ is defined as follows. For every $\pi \in \{0,1\}^{\leq\kappa}$:

1. For each $i \in [m]$, independently and uniformly sample $b_i^{(\pi)}, c_i^{(\pi)} \in [2]$ and $\alpha_i^{(\pi)}, \beta_i^{(\pi)} \in \{0,1\}$.
2. For each $\mu \in [4]$, $i \in [m]$, $k \in [n+2]$, set
$$\rho_1(x_{i,k}^{(\pi,\mu)}) = \begin{cases} \alpha_i^{(\pi)} & \text{if } k = 1, \\ 1 & \text{if } k = 2, \\ 0 & \text{if } k \geq 3 \text{ and } \mathcal{B}_{b_i^{(\pi)},\mu} = 0, \\ x_{i,k-2}^{(\pi)} & \text{if } k \geq 3 \text{ and } \mathcal{B}_{b_i^{(\pi)},\mu} = *. \end{cases}$$
3. For each $\mu \in [4]$, $j \in [m]$, $k \in \mathcal{N}_{P(G)}(j)$, set
$$\rho_1(y_{k,j}^{(\pi,\mu)}) = \begin{cases} 1 & \text{if } k = 1, \\ \beta_j^{(\pi)} & \text{if } k = 2, \\ 0 & \text{if } k \geq 3 \text{ and } \mathcal{C}_{c_j^{(\pi)},\mu} = 0, \\ y_{k-2,j}^{(\pi)} & \text{if } k \geq 3 \text{ and } \mathcal{C}_{c_j^{(\pi)},\mu} = *. \end{cases}$$
4. For each $\mu \in [4]$, $i,j \in [m]$, $k \in \mathcal{N}_{P(G)}(j)$, set
$$\rho_1(z_{i,j,k}^{(\pi,\mu)}) = \begin{cases} \alpha_i^{(\pi)} & \text{if } k = 1, \\ \beta_j^{(\pi)} & \text{if } k = 2, \\ 0 & \text{if } k \geq 3 \text{ and either } \mathcal{B}_{b_i^{(\pi)},\mu} = 0 \text{ or } \mathcal{C}_{c_j^{(\pi)},\mu} = 0, \\ z_{i,j,k-2}^{(\pi)} & \text{if } k \geq 3 \text{ and } \mathcal{B}_{b_i^{(\pi)},\mu} = \mathcal{C}_{c_j^{(\pi)},\mu} = *. \end{cases}$$
5. For each $\mu \in [4]$, $i,j \in [m]$ and every non-empty initial segment Σ of $\mathcal{N}_{P(G)}(j)$, set
$$\rho_1(u_{i,j,\Sigma}^{(\pi,\mu)}) = \begin{cases} \alpha_i^{(\pi)} & \text{if } \Sigma = (1), \\ \alpha_i^{(\pi)} \oplus \beta_j^{(\pi)} & \text{if } \Sigma = (1,2), \\ u_{i,j,\Sigma\setminus\{1,2\}}^{(\pi)} & \text{if } \Sigma \setminus \{1,2\} \neq \varnothing, \mathcal{B}_{b_i^{(\pi)},\mu} = \mathcal{C}_{c_j^{(\pi)}} = * \text{ and } \alpha_i^{(\pi)} = \beta_j^{(\pi)}, \\ \overline{u}_{i,j,\Sigma\setminus\{1,2\}}^{(\pi)} & \text{if } \Sigma \setminus \{1,2\} \neq \varnothing, \mathcal{B}_{b_i^{(\pi)},\mu} = \mathcal{C}_{c_j^{(\pi)}} = * \text{ and } \alpha_i^{(\pi)} \neq \beta_j^{(\pi)}, \\ \alpha_i^{(\pi)} \oplus \beta_j^{(\pi)} & \text{otherwise.} \end{cases}$$
6. For each $\mu \in [4]$, $i,j \in [m]$, set
$$\rho_1(w_{i,j,0}^{(\pi)}) = A_{i,j}^{(\pi)},$$
$$\rho_1(w_{i,j,1}^{(\pi)}) = \begin{cases} A_{i,j}^{(\pi)} & \text{if } b_i^{(\pi)} = 1, \\ 0 & \text{if } b_i^{(\pi)} = 2, \end{cases}$$
$$\rho_1(w_{i,j,2}^{(\pi)}) = \begin{cases} 0 & \text{if } b_i^{(\pi)} = 1, \\ A_{i,j}^{(\pi)} & \text{if } b_i^{(\pi)} = 2. \end{cases}$$
7. For any variable θ mapped to 0 or 1 by ρ_1, set $\rho_1(\overline{\theta}) = 1 - \rho_1(\theta)$.
8. For any variable θ not mapped to a Boolean constant by ρ_1, set $\rho_1(\overline{\theta}) = \overline{\rho_1(\theta)}$.

Lemma 5.50. *Let $\kappa \geq 0$, $m, n > 0$ and let G be an $m \times n$ bipartite graph with parts $[m]$ and $[n]$ and the maximum left-degree at most Δ_{max}. Let $\mathbf{A} = \{A^{(\pi)} : \pi \in \Sigma^{\leq \kappa}\}$ be a collection of $m \times m$ matrices as in the definition of ψ. Let t be a term in the variables of $\psi_{P(G)}(\mathbf{A}, \kappa)$ and t' a subterm of t such that no index from $\{1, 2\}$ is $U^{(\pi)}$-left-row-mentioned or $U^{(\pi)}$-right-row-mentioned in t'. Then*

$$\Pr[t \upharpoonright \rho_1 \neq 0] \leq (\sqrt{3/4})^{\sqrt{\frac{\deg(t'_u)}{4\Delta_{max}}}}.$$

Proof. For each $\pi \in \{0,1\}^{\leq \kappa}$, let $I^{(\pi)}$ be the set of indices $i \in [m]$ that are U-left-row-mentioned in t, and let $J^{(\pi)}$ be the set of indices $j \in [m]$ that are U-right-row-mentioned un t. Let $D = \sum_{\pi \in \{0,1\}^{\leq \kappa}} (|I^{(\pi)}| + |J^{(\pi)}|)$. Then $\deg(t'_u) \leq 4D^2\Delta_{max}$, which implies that $D \geq \sqrt{\frac{\deg(t'_u)}{4\Delta_{max}}}$.

Let t'' be a minimal subterm of t'_u that for each $\pi \in \{0,1\}^{\leq \kappa}$, U-left-row-mentions $I^{(\pi)}$ and U-right-row-mentions $J^{(\pi)}$. If we think of the variables $u^{(\pi,\mu)}_{i,j,\Sigma}$ (or their negations) appearing in t'' as undirected edges $\{(\pi, i), (\pi, j)\}$ in a bipartite graph, then t'' corresponds to a minimal edge cover of such a graph. This cover cannot contain a path of length three, thus its connected components are stars of the form $\prod_{(\pi,j,\mu,\Sigma)\in P} u^{(\pi,\mu)}_{i_0,j,\Sigma} \prod_{(\pi,j,\mu,\Sigma)\in N} \overline{u}^{(\pi,\mu)}_{i_0,j,\Sigma}$ or $\prod_{(\pi,i,\mu,\Sigma)\in P} u^{(\pi,\mu)}_{i,j_0,\Sigma} \prod_{(\pi,i,\mu,\Sigma)\in N} \overline{u}^{(\pi,\mu)}_{i,j_0,\Sigma}$, and each of these stars mentions its own disjoint set of indices.

Assume that we have a star with r rays, say $s = \prod_{(\pi,j,\mu,\Sigma)\in P} u^{(\pi,\mu)}_{i_0,j,\Sigma} \prod_{(\pi,j,\mu,\Sigma)\in N} \overline{u}^{(\pi,\mu)}_{i_0,j,\Sigma}$. For every $b^{(\pi)} \in [2] : \pi \in \{0,1\}^{\leq \kappa}$, $\alpha^{(\pi)} \in \{0,1\} : \pi \in \{0,1\}^{\leq \kappa}$, the events

$$\left(u^{(\pi,\mu)}_{i_0,j,\Sigma} \upharpoonright \rho_1 \neq 0 \mid \bigwedge_{\pi\in\{0,1\}^{\leq\kappa}} b^{(\pi)}_{i_0} = b^{(\pi)}, \bigwedge_{\pi\in\{0,1\}^{\leq\kappa}} \alpha^{(\pi)}_{i_0} = \alpha^{(\pi)} \right), \text{ where } (\pi, j, \mu, \Sigma) \in P,$$

and

$$\left(\overline{u}^{(\pi,\mu)}_{i_0,j,\Sigma} \upharpoonright \rho_1 \neq 0 \mid \bigwedge_{\pi\in\{0,1\}^{\leq\kappa}} b^{(\pi)}_{i_0} = b^{(\pi)}, \bigwedge_{\pi\in\{0,1\}^{\leq\kappa}} \alpha^{(\pi)}_{i_0} = \alpha^{(\pi)} \right), \text{ where } (\pi, j, \mu, \Sigma) \in N,$$

are independent and each happens with probability at most $3/4$. Thus, all of them simultaneously happen with probability at most $(3/4)^r \leq (\sqrt{3/4})^{r+1}$. It implies that

$$\Pr[t \upharpoonright \rho_1 \neq 0] \leq (\sqrt{3/4})^D \leq (\sqrt{3/4})^{\sqrt{\frac{\deg(t'_u)}{4\Delta_{max}}}}. \qquad \square$$

We define another polynomial system $\phi_G(\mathbf{A}, \kappa)$, which is analogous to $\psi^m_n(\mathbf{A}, \kappa, G)$. The substitution ρ_1 transforms any refutation of $\psi_{P(G)}(\mathbf{A}, \kappa)$ into a refutation of $\phi_G(\mathbf{A} \upharpoonright \rho_1, \kappa)$.

Definition 5.51 (Formula $\phi_G(\mathbf{A}, \kappa)$)**.** Let $m, n > 0$ and $\kappa \geq 0$ be integer parameters and let G be an $m \times n$ bipartite graph.

$\phi_G(\mathbf{A}, \kappa)$ uses the variables $\{x^{(\pi)}_{i,k} : i \in [m], k \in [n]\}$, $\{y^{(\pi)}_{k,j} : j \in [m], k \in \mathcal{N}_G(j)\}$, $\{z^{(\pi)}_{i,j,k} : i, j \in [m], k \in \mathcal{N}_G(j)\}$ and $\{u^{(\pi)}_{i,j,\Sigma} : i, j \in [m], \Sigma \text{ is a non-empty initial segment of } \mathcal{N}_G(j)\}$. It consists of the following polynomial axioms.

Binary AND Axiom: For every $\pi \in \{0,1\}^{\leq \kappa}$, $i, j \in [m]$, $k \in \mathcal{N}_G(j)$, the polynomial $z^{(\pi)}_{i,j,k} = x^{(\pi)}_{i,k} y^{(\pi)}_{k,j}$.

Summation Base Axiom: For every $\pi \in \{0,1\}^{\leq \kappa}$, $i, j \in [m]$, the polynomial $u^{(\pi)}_{i,j,(1)} = z^{(\pi)}_{i,j,1}$.

Summation Axiom: For every $\pi \in \{0,1\}^{\leq \kappa}$, $i, j \in [m]$ and every non-empty initial segment $\Sigma \cup (k)$ of $\mathcal{N}_G(j)$, the polynomial $u^{(\pi)}_{i,j,\Sigma\cup(k)} = u^{(\pi)}_{i,j,\Sigma} \oplus z^{(\pi)}_{i,j,k}$.

Output Axiom: For every $\pi \in \{0,1\}^{\leq \kappa}$, $i, j \in [m]$, the polynomial $u^{(\pi)}_{i,j,\mathcal{N}_G(j)} = A^{(\pi)}_{i,j}$.

Lemma 5.52. *Let $\kappa \geq 0$, $m, n > 0$ and let G be an $m \times n$ bipartite graph. Let $\mathbf{A} = \{A^{(\pi)} : \pi \in \Sigma^{\leq \kappa}\}$ be a collection of $m \times m$ matrices as in the definition of ψ. Let $\tilde{\mathbf{A}}$ be a collection of matrices defined as*

$$\tilde{\mathbf{A}} = \{A^{(\pi)} \restriction \rho_1 : \pi \in \{0,1\}^{\leq \kappa}\}.$$

Then for every $\mathsf{PCR}_{\mathbb{F}_2}$ refutation Π of $\psi_{P(G)}(\mathbf{A}, \kappa)$, $\Pi \restriction \rho_1$ is a refutation of $\phi_G(\tilde{\mathbf{A}}, \kappa)$ (modulo the axioms for twin variables $\theta + \overline{\theta} + 1$.

Proof. Follows from the definition of ρ_1. Under ρ_1, the axioms of $\psi_{P(G)}(\mathbf{A}, \kappa)$ are either satisfied or become axioms of the same type for $\phi_G(\tilde{\mathbf{A}}, \kappa)$. Since ρ_1 sometimes substitutes variables with negated variables, we need to apply the twin variables' axioms $\theta + \overline{\theta} + 1$ to replace such occurrences of $\overline{\theta}$ with $\theta + 1$. This can lead to an insignificant increase in the refutation size, which we can safely ignore. □

Next, we define a random restriction ρ_2 that w.h.p. turns any term t that mentions many columns into 0. Similarly, to ρ_1, we will not apply it to general graphs G but only to those that have a specific structure.

Definition 5.53 (Graph $H(G)$)**.** Let $m, n > 0$ and let G be an $m \times n$ bipartite graph. Given an adjacency matrix M_G of G, define $H(G)$ as the $m \times (8n + 8)$ bipartite graph with the adjacency matrix

$$M_{H(G)} = \left[\underbrace{\begin{array}{cccccccccccccccc} & 1 & & 1 & & 1 & & 1 & & 1 & & 1 & & 1 & & 1 \\ M_G & \vdots & M_G & \vdots & M_G & \vdots & M_G & \vdots & M_G & \vdots & M_G & \vdots & M_G & \vdots & M_G & \vdots \\ & 1 & & 1 & & 1 & & 1 & & 1 & & 1 & & 1 & & 1 \end{array}}_{8} \right].$$

Definition 5.54. Let t be a term in the variables of $\phi_{H(G)}(\mathbf{A}, \kappa)$. Let $N = 8n + 8$. Given $k \in [N]$, let $\iota(k) = ((k-1) \bmod (n+1)) + 1$ and $\nu(k) = \lfloor \frac{k-1}{n+1} \rfloor + 1$.

We say that $k \in [n]$ is $X^{(\pi)}$*-column-mentioned in* t if there are $i \in [m]$ and $\ell \in [N]$ with $\iota(\ell) = k$ such that $x_{i,\ell}^{(\pi)}$ or $\overline{x}_{i,\ell}^{(\pi)}$ appears in t. We say that $k \in [n]$ is $(Y^{(\pi)})^T$*-column-mentioned in* t if there are $j \in [m]$ and $\ell \in [N]$ with $\iota(\ell) = k$ such that $y_{\ell,j}^{(\pi)}$ or $\overline{y}_{\ell,j}^{(\pi)}$ appears in t. We say that $k \in [n]$ is $Z^{(\pi)}$*-column-mentioned in* t if there are $i, j \in [m]$ and $\ell \in [N]$ with $\iota(\ell) = k$ such that $z_{i,j,\ell}^{(\pi)}$ or $\overline{z}_{i,j,\ell}^{(\pi)}$ appears in t.

Definition 5.55 (Substitution ρ_2)**.** Let $\kappa \geq 0$, $m, n > 0$, $N = 8n + 8$ and let G be an $m \times n$ bipartite graph with parts $[m]$ and $[n]$.

The random substitution ρ_2 for $\phi_{H(G)}(\mathbf{A}, \kappa)$ is defined as follows.

1. For each $k \in [n]$, independently and uniformly sample $c_k \in \{*, 1, 0\}$. Assign $c_{n+1} = *$.
2. Let $\tilde{K} = \{k \in [N] : c_{\iota(k)} \in \{0,1\}\}$ and let $\tilde{G} = G \setminus \{k \in [n] : c_k \in \{0,1\}\}$. Note that $\mathcal{N}_{H(\tilde{G})}(j) = \mathcal{N}_{H(G)}(j)$ for all $j \in [m]$.
3. For every $\pi \in \{0,1\}^{\leq \kappa}$:
   (a) Let $\{\tilde{u}_{i,j,\Sigma}^{(\pi)} : i, j \in [m], \Sigma \text{ is a non-empty initial segment of } \mathcal{N}_{H(\tilde{G})}(j)\}$ be fresh extension variables.
   (b) For every $i \in [m]$, and $k \in [N]$, set

$$\rho_2(x_{i,k}^{(\pi)}) = \begin{cases} c_{\iota(k)} & \text{if } c_{\iota(k)} \in \{0,1\}, \\ x_{i,k}^{(\pi)} & \text{otherwise.} \end{cases}$$

(c) For every $j \in [m]$, and $k \in \mathcal{N}_{H(G)}(j)$, set

$$\rho_2(y^{(\pi)}_{k,j}) = \begin{cases} c_{\iota(k)} & \text{if } c_{\iota(k)} \in \{0,1\}, \\ y^{(\pi)}_{k,j} & \text{otherwise.} \end{cases}$$

(d) For every $i, j \in [m]$, and $k \in \mathcal{N}_{H(G)}(j)$, set

$$\rho_2(z^{(\pi)}_{i,j,k}) = \begin{cases} c_{\iota(k)} & \text{if } c_{\iota(k)} \in \{0,1\}, \\ z^{(\pi)}_{i,j,k} & \text{otherwise.} \end{cases}$$

(e) For every $i, j \in [m]$ and every non-empty initial segment Σ of $\mathcal{N}_{H(G)}(j)$, set

$$\rho_2(u^{(\pi)}_{i,j,\Sigma}) = \begin{cases} 0 & \text{if } \Sigma \setminus \tilde{K} = \varnothing \text{ and } |\{k \in \Sigma : c_{\iota(k)} = 1\}| \text{ is even,} \\ 1 & \text{if } \Sigma \setminus \tilde{K} = \varnothing \text{ and } |\{k \in \Sigma : c_{\iota(k)} = 1\}| \text{ is odd,} \\ \tilde{u}^{(\pi)}_{i,j,(\Sigma \setminus \tilde{K})} & \text{if } \Sigma \setminus \tilde{K} \neq \varnothing \text{ and } |\{k \in \Sigma : c_{\iota(k)} = 1\}| \text{ is even,} \\ \overline{\tilde{u}}^{(\pi)}_{i,j,(\Sigma \setminus \tilde{K})} & \text{if } \Sigma \setminus \tilde{K} \neq \varnothing \text{ and } |\{k \in \Sigma : c_{\iota(k)} = 1\}| \text{ is odd.} \end{cases}$$

(f) For any variable θ mapped to 0 or 1 by ρ_2, set $\rho_2(\overline{\theta}) = 1 - \rho_2(\theta)$.

(g) For any variable θ not mapped to a Boolean constant by ρ_2, set $\rho_2(\overline{\theta}) = \overline{\rho_2(\theta)}$.

We show that under ρ_2 every term that mentions many columns becomes zero w.h.p.

Lemma 5.56. *Let $\kappa \geq 0$, $m, n > 0$ and let G be an $m \times n$ bipartite graph with parts $[m]$ and $[n]$. Let t be a term in the variables of $\phi_{H(G)}(\mathbf{A}, \kappa)$. Let K be the set of all $k \in [n]$ that are $X^{(\pi)}$-column-mentioned, $(Y^{(\pi)})^T$-column-mentioned or $Z^{(\pi)}$-column-mentioned in t, for some $\pi \in \{0,1\}^{\leq \kappa}$. Then $\Pr[t \restriction \rho_2 \neq 0] \leq (2/3)^{|K|}$.*

Proof. For every variable x-, y- or z-variable θ appearing in t, $\Pr[\rho_2(\theta) \neq 0] = 2/3$, which happens independently for distinct columns. Thus, $(t \restriction \rho_2 \neq 0)$ occurs with probability at most $(2/3)^{|K|}$. □

When G is an expander with sufficiently large minimum left-degree, the graph $\tilde{G}$ defined in Definition 5.55 remains a good expander due to Lemma 4.16.

Proposition 5.57. *Let $\kappa \geq 0$, $n > 0$, $N = 8n + 8$, $m = 16(N + 2)$ and let G be an $m \times n$ (n^δ, d)-lossless expander with parts $[m]$ and $[n]$, the minimum left-degree at least $\Delta_{min} = 50 \log n$ and the maximum left-degree at most $\Delta_{max} = 150 \log n$. Then with probability at least $1/2$, the graph $\tilde{G}$ from Definition 5.55 is an (n^δ, c)-boundary expander, where $c = \Delta_{min}/6 - d$.*

We show that ρ_2 transforms any refutation of $\phi_{H(G)}(\mathbf{A}, \kappa)$ into a refutation of $\phi_{H(\tilde{G})}(\mathbf{A} \restriction \rho_2, \kappa)$.

Lemma 5.58. *Let $\kappa \geq 0$, $m, n > 0$ and let G be an $m \times n$ bipartite graph with parts $[m]$ and $[n]$. Let $\mathbf{A} = \{A^{(\pi)} : \pi \in \Sigma^{\leq \kappa}\}$ be a collection of $m \times m$ matrices as in the definition of ϕ. Let $\tilde{\mathbf{A}}$ be a collection of matrices defined as*

$$\tilde{\mathbf{A}} = \{A^{(\pi)} \restriction \rho_2 : \pi \in \{0,1\}^{\leq \kappa}\}.$$

Then for every $\mathsf{PCR}_{\mathbb{F}_2}$ refutation Π of $\phi_{H(G)}(\mathbf{A}, \kappa)$, $\Pi \restriction \rho_2$ is a refutation of $\phi_{H(\tilde{G})}(\tilde{\mathbf{A}}, \kappa)$.

Proof. Can be verified straightforwardly from the definition of ρ_2, similarly to Lemma 5.39. □

Now we define a random restriction ρ_3 that reduces the total *degree* of the terms in any refutation of $\phi_($$\mathbf{A}, \kappa)$ if such a refutation has certain restrictions on its u-degree and column degree. We

need the following matrices.

$$\mathcal{D} = \begin{pmatrix} 1 & * & 1 & 0 & 0 & * & * & * \\ 0 & 1 & * & 1 & * & * & * & 0 \\ * & * & 0 & * & 1 & 0 & 1 & * \\ * & 0 & * & * & * & 1 & 0 & 1 \end{pmatrix}, \quad \mathcal{E} = \begin{pmatrix} 1 & 0 & 0 & 1 & * & * & * & * \\ 0 & * & 1 & * & 1 & * & 0 & * \\ * & 1 & * & 0 & * & 0 & * & 1 \\ * & * & * & * & 0 & 1 & 1 & 0 \end{pmatrix}.$$

Definition 5.59 (Substitution ρ_3)**.** Let $\kappa \geq 0$, $m, n > 0$, $N = 8n + 8$, and let G be an $m \times n$ bipartite graph with parts $[m]$ and $[n]$. Given $k \in [N]$, let $\iota(k) = ((k-1) \bmod (n+1)) + 1$ and $\nu(k) = \lfloor \frac{k-1}{n+1} \rfloor + 1$.

The substitution ρ_3 for $\phi_{H(G)}(\mathbf{A}, \kappa)$ is defined as follows. For every $\pi \in \{0,1\}^{\leq \kappa}$:

1. For every $i \in [m]$ uniformly and independently sample $s_i^{(\pi)} \in [4]$ and $r_i^{(\pi)} \in [4]$.
2. For each $i \in [m]$ and $k \in [N]$, set

$$\rho_3(x_{i,k}^{(\pi)}) = \begin{cases} 1 & \text{if } \iota(k) = n+1 \text{ and } \mathcal{D}_{s_i^{(\pi)},\nu(k)} = 1, \\ 0 & \text{if } \iota(k) = n+1 \text{ and } \mathcal{D}_{s_i^{(\pi)},\nu(k)} \neq 1, \\ x_{i,\iota(k)}^{(\pi)} & \text{if } \iota(k) \neq n+1 \text{ and } \mathcal{D}_{s_i^{(\pi)},\nu(k)} = *, \\ \mathcal{D}_{s_i^{(\pi)},\nu(k)} & \text{if } \iota(k) \neq n+1 \text{ and } \mathcal{D}_{s_i^{(\pi)},\nu(k)} \in \{0,1\}. \end{cases}$$

3. For each $j \in [m]$ and $k \in \mathcal{N}_{H(G)}(j)$, set

$$\rho_3(y_{k,j}^{(\pi)}) = \begin{cases} |\mathcal{N}_{G'}(j)| \bmod 2 & \text{if } \iota(k) = n+1 \text{ and } \mathcal{E}_{r_j^{(\pi)},\nu(k)} = 1, \\ 0 & \text{if } \iota(k) = n+1 \text{ and } \mathcal{E}_{r_j^{(\pi)},\nu(k)} \neq 1, \\ y_{\iota(k),j}^{(\pi)} & \text{if } \iota(k) \neq n+1 \text{ and } \mathcal{E}_{r_j^{(\pi)},\nu(k)} = *, \\ \mathcal{E}_{r_j^{(\pi)},\nu(k)} & \text{if } \iota(k) \neq n+1 \text{ and } \mathcal{E}_{r_j^{(\pi)},\nu(k)} \in \{0,1\}. \end{cases}$$

4. For each $i, j \in [m]$ and $k \in \mathcal{N}_{H(G)}(j)$ set

$$\rho_3(z_{i,j,k}^{(\pi)}) = \rho_3(x_{i,k}^{(\pi)}) \rho_3(y_{k,j}^{(\pi)}).$$

5. For each $i, j \in [m]$ and every non-empty initial segment Σ of $\mathcal{N}_{H(G)}(j)$, set

$$\rho_3(u_{i,j,\Sigma}^{(\pi)}) = \sum_{k \in \Sigma} \rho_3(z_{i,j,k}^{(\pi)}).$$

6. For every variable θ assigned by ρ_3, set $\rho_3(\overline{\theta}) = 1 - \rho_3(\theta)$.

Note that ρ_3 does not substitute any negated variables and expands the extension variables as polynomials. It can be trivially extended to a PC refutation. The *size* of the resulting refutation can grow exponentially, but we will prove that its *degree* becomes small w.h.p.

For every refutation Π of $\phi_{H(G)}(\mathbf{A}, \kappa)$, $\Pi \restriction \rho_3$ can be transformed into a refutation of $\tilde{\phi}_G(\mathbf{A} \restriction \rho_3, \kappa)$, which is the algebraic analogue of $\phi_G(\mathbf{A} \restriction \rho_3, \kappa)$. That is, $\tilde{\phi}_G(\mathbf{A}, \kappa)$ is the polynomial system

$$\bigcup_{\pi \in \{0,1\}^{\leq \kappa}} \bigcup_{i,j \in [m]} \{ \sum_{k \in \mathcal{N}_G(j)} x_{i,k}^{(\pi)} y_{k,j}^{(\pi)} = A_{i,j}^{(\pi)} \}.$$

In order to handle z-variables, we need to define a transformation R_d. It is a linear mapping defined on the terms in the variables of $\phi_G(\mathbf{A}, \kappa)$.

Definition 5.60. Let t be a term in the variables of $\phi_G(\mathbf{A}, \kappa)$. We define $R_d(t)$ by *contracting* every subterm of the form $\prod_{j\in J} \overline{z}^{(\pi)}_{i_0,j,k}$ and $\prod_{i\in I} \overline{z}^{(\pi)}_{i,j_0,k}$, where $|I|, |J| \geq d$. Let $t = t_1 t_2$, where t_1 contains only negated z-variables and t_2 contains the rest. Let

$$S_{left} = \{(\pi, i_0, \{j \in [m] : \overline{z}^{(\pi)}_{i_0,j,k} \in \mathrm{vars}(t_1)\}, k) : \pi \in \{0,1\}^{\leq\kappa}, i_0 \in [m], k \in [n]\},$$
$$S_{right} = \{(\pi, \{i \in [m] : \overline{z}^{(\pi)}_{i,j_0,k} \in \mathrm{vars}(t_1)\}, j_0, k) : \pi \in \{0,1\}^{\leq\kappa}, j_0 \in [m], k \in [n]\}$$

and define

$$t_{left} = \left(\prod_{\substack{(\pi,i_0,J,k)\in S_{left}\\ |J|<d}} \prod_{j\in J} \overline{z}^{(\pi)}_{i_0,j,k} \right) \left(\prod_{\substack{(\pi,i_0,J,k)\in S_{left}\\ |J|\geq d}} \overline{x}^{(\pi)}_{i_0,k} \right),$$
$$t_{right} = \left(\prod_{\substack{(\pi,I,j_0,k)\in S_{right}\\ |I|<d}} \prod_{i\in I} \overline{z}^{(\pi)}_{i,j_0,k} \right) \left(\prod_{\substack{(\pi,I,j_0,k)\in S_{right}\\ |I|\geq d}} \overline{y}^{(\pi)}_{k,j_0} \right).$$

Then

$$R_d(t) = t_{left} \cdot t_{right} \cdot t_2.$$

We proceed by extending R_d to polynomials linearly.

Lemma 5.61. *Let $\kappa \geq 0$, $m, n > 0$, $\tilde{d} > 0$ and let G be an $m \times n$ bipartite graph with parts $[m]$ and $[n]$ with the maximum right-degree Δ_{max}. Let t be a term in the variables of $\phi_{H(G)}(\mathbf{A}, \kappa)$. Let K be the set of all $k \in [n]$ that are $X^{(\pi)}$-column-mentioned, $(Y^{(\pi)})^T$-column-mentioned or $Z^{(\pi)}$-column-mentioned in t, for some $\pi \in \{0,1\}^{\leq\kappa}$. Then $\Pr[R_{\tilde{d}}(t) \restriction \rho_3 \neq 0] \leq (15/16)^{\frac{\deg((R_{\tilde{d}}(t))_{x,y,z})}{24\tilde{d}(|K|+\Delta_{max})}}$.*

Proof. Suppose that $\deg((R_{\tilde{d}}(t))_{x,y}) \geq \deg((R_{\tilde{d}}(t))_{x,y,z})/3$. For every $\pi \in \{0,1\}^{\leq\kappa}$, let

$$I^{(\pi)}_x = \{i \in [m] : \exists k \in [n] \colon x^{(\pi)}_{i,k} \text{ or } \overline{x}^{(\pi)}_{i,k} \text{ appears in } t\},$$
$$J^{(\pi)}_y = \{j \in [m] : \exists k \in [n] \colon y^{(\pi)}_{k,j} \text{ or } \overline{y}^{(\pi)}_{k,j} \text{ appears in } t\}.$$

Then

$$\deg((R_{\tilde{d}}(t))_{x,y,z})/3 \leq \deg((R_{\tilde{d}}(t))_{x,y}) \leq 8(|K| + \Delta_{max}) \sum_{\pi\in\{0,1\}^{\leq\kappa}} (|I^{(\pi)}_x| + |J^{(\pi)}_y|).$$

For every $i \in I^{(\pi)}_x$ there is a variable in $R_{\tilde{d}}(t)$ that is independently set to 0 with probability $1/4$ by ρ_3. Similarly, for every $j \in J^{(\pi)}_y$, there is a variable in $R_{\tilde{d}}(t)$ that is also set to 0 by ρ_3 with the same probability. It implies that

$$\Pr\Big[(R_{\tilde{d}}(t))_{x,y} \restriction \rho_3 \neq 0\Big] \leq (3/4)^{\frac{\deg(R(t)_{x,y,z})}{24(|K|+\Delta_{max})}}.$$

Otherwise, it must be that $\deg((R_{\tilde{d}}(t))_z) \geq 2\deg((R_{\tilde{d}}(t))_{x,y,z})/3$. Let $(R_{\tilde{d}}(t))_z = s_1 s_2$, where s_1 and s_2 consist of all the positive and negative occurrences of the z-variables in $R_{\tilde{d}}(t)$, respectively.

Suppose that $\deg(s_1) \geq \deg((R_{\tilde{d}}(t))_{x,y,z})/3$. For every $\pi \in \{0,1\}^{\leq\kappa}$, let

$$I^{(\pi)}_z = \{i \in [m] : \exists j \in [m], k \in [n] \colon z^{(\pi)}_{i,j,k} \text{ or } \overline{z}^{(\pi)}_{i,j,k} \text{ appears in } t\},$$
$$J^{(\pi)}_z = \{i \in [m] : \exists i \in [m], k \in [n] \colon z^{(\pi)}_{i,j,k} \text{ or } \overline{z}^{(\pi)}_{i,j,k} \text{ appears in } t\}.$$

Then

$$\deg(s_1) \le 8\Delta_{max} \sum_{\pi\in\{0,1\}^{\le\kappa}} (|I_z^{(\pi)}| + |J_z^{(\pi)}|) \le 16\Delta_{max} \sum_{\pi\in\{0,1\}^{\le\kappa}} \max\{|I_z^{(\pi)}|, |J_z^{(\pi)}|\}.$$

The term s_1 contains at least $\sum_{\pi\in\{0,1\}^{\le\kappa}} \max\{|I_z^{(\pi)}|, |J_z^{(\pi)}|\}$ variables that are assigned independently by ρ, and each does not become zero with probability at most $(3/4)^2$. It implies that

$$\Pr[s_1 \restriction \rho_3 \neq 0] \le (3/4)^{\frac{\deg((R_{\tilde{d}}(t))_{x,y,z})}{24\Delta_{max}}}.$$

Finally, consider the remaining case $\deg(s_2) \ge \deg((R_{\tilde{d}}(t))_{x,y,z})/3$. We will greedily identify a large set of variables in s_2 that are independently set to 0 by ρ_3 w.h.p. Initially set $S = \mathrm{vars}(s_2)$ and $T = \varnothing$.

- Pick any variable $\overline{z}_{i,j,k}^{(\pi)} \in S$.
- Add $\overline{z}_{i,j,k}^{(\pi)}$ to T.
- Remove all variables $\{\overline{z}_{i,j',k'}^{(\pi)} : j' \in [m], k' \in [n]\} \cup \{\overline{z}_{i',j,k'}^{(\pi)} : i' \in [m], k' \in [n]\}$ from S.
- Repeat until S is empty.

Observe that each variable in T mentions its own indices: for every $\pi \in \{0,1\}^{\le\kappa}$ and $\ell \in [m]$, there is at most one variable of the form $\overline{z}_{i,\ell,k}^{(\pi)}$ and at most one of the form $\overline{z}_{\ell,j,k}^{(\pi)}$. Thus, every variable from T independently becomes zero under ρ_3 with probability at least $1/16$. It remains to show that the size of T is sufficiently large. At each step we remove at most $8\tilde{d}(|K| + \Delta_{max})$ z-variables from S due to the properties of $R_{\tilde{d}}$, therefore the size of T is at least $\frac{\deg((R_{\tilde{d}}(t))_{x,y,z})}{24\tilde{d}(|K|+\Delta_{max})}$. It implies that

$$\Pr[s_2 \restriction \rho_3 \neq 0] \le (15/16)^{\frac{\deg((R_{\tilde{d}}(t))_{x,y,z})}{24\tilde{d}(|K|+\Delta_{max})}}.$$

□

We proceed by showing that for every $\mathsf{PCR}_{\mathbb{F}_2}$ refutation Π of $\phi_{H(G)}(\mathbf{A}, \kappa)$ of degree d, $R_{\tilde{d}}(\Pi) \restriction \rho_3$ can be extended to a refutation of $\tilde{\phi}_G(\mathbf{A}, \kappa)$ of degree at most $d + 1$.

Lemma 5.62. *Let $\kappa \ge 0$, $m, n > 0$, $N = 8n + 8$, $\tilde{d} > 0$ and let G be an $m \times n$ bipartite graph with parts $[m]$ and $[n]$ with the maximum right-degree Δ_{max}. Let Π be a $\mathsf{PCR}_{\mathbb{F}_2}$ refutation of $\phi_{H(G)}(\mathbf{A}, \kappa)$ of degree d and size at most $\frac{(4/3)^{\tilde{d}}}{4m_{\tilde{d}}N2^{\kappa}}$. Then, with probability at least $1/2$, $R_{\tilde{d}}(\Pi) \restriction \rho_3$ can be extended to a valid PC refutation $\tilde{\Pi}$ of $\tilde{\phi}_G(\mathbf{A}, \kappa)$ of degree at most $d + 1$.*

Proof. We begin by observing the following property of ρ_3.

Claim 5.63. *Let $\pi \in \{0,1\}^{\le\kappa}$ and $k \in [N]$. For every $i \in [m]$ and $J \subseteq [m]$,*

$$\Pr\left[\forall \ell \in J : \rho_3(\overline{z}_{i,\ell,k}^{(\pi)}) \neq \rho_3(\overline{x}_{i,k}^{(\pi)})\right] \le (3/4)^{|L|}.$$

Similarly, for every $j \in [m]$ and $I \subseteq [m]$,

$$\Pr\left[\forall \ell \in I : \rho_3(\overline{z}_{\ell,j,k}^{(\pi)}) \neq \rho_3(\overline{y}_{k,j}^{(\pi)})\right] \le (3/4)^{|L|}.$$

Proof. We will show the first statement, and the second is symmetrical. Fix $s_i^{(\pi)}$ and thus $\rho_3^{(\pi)}(x_{i,k})$. Then $\rho_3(\overline{z}_{i,\ell,k}^{(\pi)}) = \rho_3(\overline{x}_{i,k}^{(\pi)})$ when $\rho_3(y_{k,\ell}^{(\pi)}) = 1$, which happens with probability at least $1/4$ independently for each $\ell \in J$. By averaging, the claim holds. ◇

There is at most $2mN2^{\kappa}|\Pi|$ different maximal stars in Π: for every term t choose a triple (π, ℓ, k) and consider two induced stars $\{\overline{z}^{(\pi)}_{i,\ell,k} : i \in [m]\} \cap \mathrm{vars}(t)$ and $\{\overline{z}^{(\pi)}_{\ell,j,k} : j \in [m]\} \cap \mathrm{vars}(t)$. Together with the union bound, the above claim shows that with probability at least $1/2$, the following holds for every term t appearing in Π:

- For every $\pi \in \{0,1\}^{\leq \kappa}$, $k \in [N]$, $i \in [m]$, if the star $\{\overline{z}^{(\pi)}_{i,j,k} : j \in [m]\} \cap \mathrm{vars}(t)$ has at least $\tilde{d}$ rays, then for some $\tilde{j} \in [m]$ there is a variable $\overline{z}^{(\pi)}_{i,\tilde{j},k}$ appearing in t with $\rho_3(\overline{z}^{(\pi)}_{i,\tilde{j},k}) = \rho_3(\overline{x}^{(\pi)}_{i,k})$.
- For every $\pi \in \{0,1\}^{\leq \kappa}$, $k \in [N]$, $j \in [m]$, if the star $\{\overline{z}^{(\pi)}_{i,j,k} : i \in [m]\} \cap \mathrm{vars}(t)$ has at least $\tilde{d}$ rays, then for some $\tilde{i} \in [m]$ there is a variable $\overline{z}^{(\pi)}_{\tilde{i},j,k}$ appearing in t with $\rho_3(\overline{z}^{(\pi)}_{\tilde{i},j,k}) = \rho_3(\overline{y}^{(\pi)}_{k,j})$.

For the rest of the proof, fix such ρ_3.

We prove the lemma by induction on the proof lines in Π. Let f be a proof line in Π.

If f is an axiom, then $R_{\tilde{d}}(f) = f$.

If f is obtained from polynomials g and h as $f = \alpha g + \beta h$, then clearly $R_{\tilde{d}}(f) = R_{\tilde{d}}(g) + R_{\tilde{d}}(h)$ by linearity of $R_{\tilde{d}}$.

The interesting case is when $f = g \cdot \theta$ for some variable θ. It is possible that $(R(f) \restriction \rho_3) \neq (R(g) \restriction \rho_3) \cdot \rho_3(\theta)$. In particular, this happens when there is a term $t \in g$ such that $(R(t \cdot \theta) \restriction \rho_3) \neq (R(t) \restriction \rho_3) \cdot \rho_3(\theta)$. From the construction of R it must be the case that θ is a negated z-variable, say $\theta = \overline{z}^{(\pi)}_{i,j,k}$. This occurs because t contains as a subterm at least one of the following subterms.

- $t_1 = \prod_{\ell \in J} \overline{z}^{(\pi)}_{i,\ell,k}$ such that $R(t_1) = t_1$, $R(t_1 \overline{z}^{(\pi)}_{i,j,k}) = \overline{x}^{(\pi)}_{i,k}$ and $(t_1 \overline{z}^{(\pi)}_{i,j,k}) \restriction \rho_3 \neq \overline{x}^{(\pi)}_{i,k} \restriction \rho_3$.
- $t_2 = \prod_{\ell \in I} \overline{z}^{(\pi)}_{\ell,j,k}$ such that $R(t_2) = t_2$, $R(t_2 \overline{z}^{(\pi)}_{i,j,k}) = \overline{y}^{(\pi)}_{k,j}$ and $(t_2 \overline{z}^{(\pi)}_{i,j,k}) \restriction \rho_3 \neq \overline{y}^{(\pi)}_{k,j} \restriction \rho_3$.
- $t_3 = \prod_{\ell \in J} \overline{z}^{(\pi)}_{i,\ell,k} \cdot \prod_{\ell \in I} \overline{z}^{(\pi)}_{\ell,j,k}$ such that $R(t_3) = t_3$, $R(t_3 \overline{z}^{(\pi)}_{i,j,k}) = \overline{x}^{(\pi)}_{i,k} \overline{y}^{(\pi)}_{k,j}$ and $(t_3 \overline{z}^{(\pi)}_{i,j,k}) \restriction \rho_3 \neq \overline{x}^{(\pi)}_{i,k} \overline{y}^{(\pi)}_{k,j} \restriction \rho_3$.

Suppose that t contains t_1. By our choice of ρ_3, there must be $\tilde{j} \in J \cup \{j\}$ with $\rho_3(\overline{z}^{(\pi)}_{i,\tilde{j},k}) = \rho_3(\overline{x}^{(\pi)}_{i,k})$. Consider the term $\tilde{t}_1 = \overline{x}^{(\pi)}_{i,k} \prod_{\ell \in J \cup \{j\} \setminus \{\tilde{j}\}} \overline{z}^{(\pi)}_{i,\ell,k}$, which is obtained by replacing $\overline{z}^{(\pi)}_{i,\tilde{j},k}$ with $\overline{x}^{(\pi)}_{i,k}$ in $t_1 \overline{z}^{(\pi)}_{i,j,k}$. Then $\overline{z}^{(\pi)}_{i,\tilde{j},k} \restriction \rho_3 = \tilde{t}_1 \restriction \rho_3$.

1. Suppose $\rho_3(\overline{x}^{(\pi)}_{i,k}) = 1$. Then $\rho_3(\overline{z}^{(\pi)}_{i,\ell,k}) = 1$ for all $\ell \in J \cup \{j\}$ and $(t_1 \overline{z}^{(\pi)}_{i,j,k}) \restriction \rho_3 = \overline{x}^{(\pi)}_{i,k} \restriction \rho_3 = 1$, contradicting our choice of t_1.
2. Suppose $\rho_3(\overline{x}^{(\pi)}_{i,k}) = 0$. Then $\rho_3(\overline{z}^{(\pi)}_{i,\tilde{j},k}) = 0$ and $(t_1 \overline{z}^{(\pi)}_{i,j,k}) \restriction \rho_3 = \overline{x}^{(\pi)}_{i,k} \restriction \rho_3 = 0$, contradicting our choice of t_1.
3. Suppose $\rho_3(\overline{x}^{(\pi)}_{i,k}) = 1 - x^{(\pi)}_{i,\iota(k)}$. We show how to derive the polynomial $(\overline{x}^{(\pi)}_{i,k} - t_1 \overline{z}^{(\pi)}_{i,j,k}) \restriction \rho_3$. It coincides with the polynomial $(\overline{x}^{(\pi)}_{i,k} - \tilde{t}_1) \restriction \rho_3$.

   For every $\ell \in J \cup \{j\} \setminus \{\tilde{j}\}$, from $z^{(\pi)}_{i,\ell,k} - x^{(\pi)}_{i,k} y^{(\pi)}_{k,\ell}$ we can first derive $\overline{x}^{(\pi)}_{i,k} - \overline{x}^{(\pi)}_{i,k} \overline{z}^{(\pi)}_{i,\ell,k}$. Then we use these polynomials telescopically to derive $\overline{x}^{(\pi)}_{i,k} - \tilde{t}_1$. Applying ρ_3 to such a derivation, we obtain a proof of $(\overline{x}^{(\pi)}_{i,k} - t_1 \overline{z}^{(\pi)}_{i,j,k}) \restriction \rho_3$.

Thus, we can derive $R(t \overline{z}^{(\pi)}_{i,j,k}) \restriction \rho_3$ from $R(t) \restriction \rho_3$ by multiplying it with $\rho_3(\overline{z}^{(\pi)}_{i,j,k})$ and then using $(\overline{x}^{(\pi)}_{i,k} - t_1 \overline{z}^{(\pi)}_{i,j,k}) \restriction \rho_3$.

The case when t contains t_2 is symmetrical. When t contains t_3, we can analogously show how to derive $(\overline{x}^{(\pi)}_{i,k} \overline{y}^{(\pi)}_{k,j} - t_3 \overline{z}^{(\pi)}_{i,j,k}) \restriction \rho_3$, which then can be used to derive $R(t \overline{z}^{(\pi)}_{i,j,k}) \restriction \rho_3$ from $R(t) \restriction \rho_3$. $\square$

Finally, we show how $\tilde{\phi}_G(\mathbf{A}, \kappa)$ can be reduced to $\mathsf{FPHP}(G)$.

Definition 5.64 (Reduction τ)**.** Let $\kappa \geq 0$, $m, n > 0$ and let G be an $m \times n$ bipartite graph with parts $[m]$ and $[n]$. Let $P = (p_{i,k})_{i\in[m],k\in\mathcal{N}_G(i)}$ be fresh variables. The reduction τ for $\tilde{\phi}_G(\mathbf{A}, \kappa)$ is defined as follows. For every $\pi \in \{0,1\}^{\leq\kappa}$ in the decreasing order:

1. For each $i \in [m]$ and $k \in [n]$ set

$$\tau(x_{i,k}^{(\pi)}) = \sum_{\substack{s\in[m] \\ \text{such that } k\in N_G(s)}} \tau(A_{i,s}^{(\pi)})p_{s,k}\text{[6]}.$$

2. For each $j \in [m]$ and $k \in \mathcal{N}_G(j)$ set

$$\tau(y_{k,j}^{(\pi)}) = p_{j,k}.$$

This definition is well-defined: $A^{(\pi)} \restriction \tau = A^{(\pi)}$ for every $\pi \in \{0,1\}^{\kappa}$, because $A^{(\pi)}$ only contain constants in these cases.

Lemma 5.65. *Let $\kappa \geq 0$, $m, n > 0$ and let G be an $m \times n$ bipartite graph with parts $[m]$ and $[n]$. Let $\mathbf{A} = \{A^{(\pi)} : \pi \in \Sigma^{\leq\kappa}\}$ be a collection of $m \times m$ matrices as in the definition of $\tilde{\phi}$. Then for any $\mathsf{PCR}_{\mathbb{F}_2}$ refutation Π of $\tilde{\phi}_G(\mathbf{A}, \kappa)$ with degree d, $\Pi\tau$ can be transformed into a refutation of $\mathsf{FPHP}(G)$ with degree at most $d(\kappa + 1)$.*

Proof. It follows by induction on $|\pi|$, that for every $\pi \in \{0,1\}^{\leq\kappa}$, $i \in [m]$, and $k \in [n] \setminus K$, $\tau(x_{i,k}^{(\pi)})$ (and thus $\tau(\overline{x_{i,k}^{(\pi)}})$) is a polynomial of degree at most $\kappa - |\pi| + 1$.

It implies that all polynomials from $\tilde{\phi}_G(\mathbf{A}, \kappa) \restriction \tau$ can be easily derived from the axioms of $\mathsf{FPHP}(G)$.

Claim 5.66. *Every polynomial from $\tilde{\phi}_G(\mathbf{A}, \kappa) \restriction \tau$ has a degree-$(\kappa + 2)$ proof from $\mathsf{FPHP}(G)$.*

Proof. Fix $\pi \in \{0,1\}^{\leq\kappa}$. As shown above, all the entries of $A^{(\pi)} \restriction \tau$ are polynomials of degree at most $\kappa - |\pi|$.

Let $i, j \in [m]$. The (i, j)th axiom of $\tilde{\phi}_G(\mathbf{A}, \kappa)$ under τ transforms as follows:

$$\begin{aligned}
\left(\sum_{k\in\mathcal{N}_G(j)} x_{i,k}^{(\pi)} y_{k,j}^{(\pi)} + A_{i,j}^{(\pi)}\right) \restriction \tau &= \sum_{k\in\mathcal{N}_G(j)} \left(\sum_{\substack{s\in[m] \\ \text{such that } k\in N_G(s)}} \tau(A_{i,s}^{(\pi)})p_{s,k}\right) p_{j,k} + \tau(A_{i,j}^{(\pi)}) \\
&= \sum_{s\in[m]} \tau(A_{i,s}^{(\pi)}) \left(\sum_{k\in\mathcal{N}_G(j)\cap N_G(s)} p_{s,k}p_{j,k}\right) + \tau(A_{i,j}^{(\pi)}) \\
&= \sum_{s\in[m]\setminus\{j\}} \tau(A_{i,s}^{(\pi)}) \left(\sum_{k\in\mathcal{N}_G(j)\cap N_G(s)} p_{s,k}p_{j,k}\right) \\
&\quad + \tau(A_{i,j}^{(\pi)}) \left(\sum_{k\in\mathcal{N}_G(j)} p_{j,k} + 1\right),
\end{aligned}$$

which is trivially derivable in degree $\kappa - |\pi| + 2$ from the hole axioms $p_{s,k}p_{j,k}$ and the polynomial

$$\sum_{k\in\mathcal{N}_G(j)} p_{j,k} + 1.$$

[6] It is useful to think of P as an $m \times n$ variable matrix, where $P_{i,k} = 0$ for all $i \in [m]$ and $k \notin \mathcal{N}_G(i)$. Then $\tau(x_{i,k}^{(\pi)}) = ((A^{(\pi)} \restriction \tau)P)_{i,k}$.

Note that the latter is an immediate consequence of the pigeon axiom for pigeon j together with its functional axioms, and thus has a derivation of degree at most Δ_{max} from $\mathsf{FPHP}(G)$.

Thus, we can extend $\Pi \restriction \tau$ to a refutation of $\mathsf{FPHP}(G)$ of degree at most $d(\kappa+1)$. ◇

□

Theorem 5.67. *Let $n > 0$, $N = 8n+8$, $m = 16(N+2)$, $\kappa \leq n^{\alpha}$, for some $\alpha < 1$, and let G be an $m \times n$ (n^{δ}, d)-lossless expander with parts $[m]$ and $[n]$, the minimum left-degree at least $\Delta_{min} = 50 \log n$ and the maximum left-degree at most $\Delta_{max} = 150 \log n$. Let $\mathbf{A} = \{A^{(\pi)} : \pi \in \Sigma^{\leq \kappa}\}$ be a collection of $m \times m$ matrices as in the definition of ψ. Then any $\mathsf{PCR}_{\mathbb{F}_2}$ refutation of $\psi_{P(H(G))}(\mathbf{A}, \kappa)$ requires size $2^{\Omega((n^{\delta}/\kappa)^{1/3})}$.*

Proof. Let

$$
\begin{aligned}
c &= \Delta_{min}/6 - d, \\
d_1 &= \frac{cn^{\delta}}{8\Delta_{max}(\kappa+1)}, \\
d_2 &= d_1^{1/3} = \left(\frac{cn^{\delta}}{8\Delta_{max}(\kappa+1)}\right)^{1/3}.
\end{aligned}
$$

Note that $d_1 = \Theta(n^{\delta}/\kappa)$ and $d_2 = \Theta((n^{\delta}/\kappa)^{1/3})$ due to our choice of Δ_{min} and Δ_{max}.

Let Π be a $\mathsf{PCR}_{\mathbb{F}_2}$ refutation of $\psi_{P(H(G))}(\mathbf{A}, \kappa)$. Suppose, for the sake of contradiction, that $|\Pi| \leq 2^{\epsilon d_2}$ for some small $\epsilon > 0$. We will fix the value of ϵ later.

We start with applying the restriction ρ_1 from Definition 5.49 to Π. Let $\Pi_1 = \Pi \restriction \rho_1$. By Lemma 5.50 and the union bound, there exists ρ_1 such that for every term t in Π_1, $\deg(t_u) < d_1$. This holds since the maximum left-degree of $H(G)$ is $8\Delta_{max}+8$ and the size of Π is less than $(4/3)^{\sqrt{\frac{d_1}{4(8\Delta_{max}+8)}}} = 2^{\Theta((\frac{d_1}{\log n})^{1/2})}$ for sufficiently small ϵ. By Lemma 5.52, Π_1 is a refutation of $\phi_{H(G)}(\mathbf{A} \restriction \rho_1, \kappa)$.

We proceed by applying the restriction ρ_2 from Definition 5.55 to Π_1. Let $\Pi_2 = \Pi \restriction \rho_2$. By Lemma 5.56 and the union bound, with probability bigger than $1/2$, for every term t in Π_2 it holds that $t_{x,y,z}$ mentions less than d_2 columns; that is, there is a set $K \subseteq [n]$ such that no $k \notin K$ is $X^{(\pi)}$-column-mention, $(Y^{(\pi)})^T$-column-mentioned or $Z^{(\pi)}$-column-mentioned in t. This holds since the size of Π_1 is less than $\frac{1}{2}(3/2)^{d_2} = 2^{\Theta(d_2)}$ for sufficiently small ϵ. By Proposition 5.57, the graph G' is an (n^{δ}, c)-boundary expander with probability at least $1/2$. Thus, by the union bound, there is ρ_2 for which both of these events happen. By Lemma 5.58, Π_2 is a refutation of $\phi_{H(G')}(\mathbf{A} \restriction \rho_1 \restriction \rho_2, \kappa)$.

Next, we apply the restriction ρ_3 from Definition 5.59 to Π_2. Let $\tilde{d} = d_2$ and $\Pi' = R_{d_2}(\Pi_2) \restriction \rho_3$. By Lemma 5.61 and the union bound, with probability larger than $1/2$, for every term t in $R(\Pi_2)$, $\deg(t_{x,y,z}) < d_1$. This holds since $|K|$ in Lemma 5.61 is less than d_2 due to ρ_2, and the size of Π' is less than $\frac{1}{2}16/15^{\frac{d_1}{24d_2(d_2+\Delta_{max})}} = 2^{(\Theta(d_2))}$ for sufficiently small ϵ. Therefore, the degree of any term in Π' is at most $4d_1 - 4$: every term in $R(\pi_2)$ has degree at most $2d_1 - 2$, and the degree can grow by at most the factor of 2 due to ρ_3. By Lemma 5.62, Π' can be extended to a refutation Π_3 of $\tilde{\phi}(\mathbf{A} \restriction \rho_1 \restriction \rho_2 \restriction \rho_3, \kappa)$ by increasing the degree by at most 1. Thus, by the union bound, there is ρ_3 for which both of the above events happen. In this case, Π_3 has degree at most $4d_1$.

Finally, we apply the restriction τ from Definition 5.64 to Π_3. By Lemma 5.65, $\Pi_3 \restriction \tau$ can be extended to a refutation Π_4 of $\mathsf{FPHP}(G')$. The degree of Π_4 is at most $4d_1(\kappa+1) = \frac{cn^{\delta}}{2\Delta_{max}}$. This contradicts the degree bound from Proposition 5.46. □

6 Proof Complexity Generators for SA

In this section, we will state our results for a stronger formula $\mathsf{BT}^\bullet\mathsf{Rank}_n^m(A)$, which is similar to $\mathsf{BTRank}_n^m(A)$ except that it does not use z-variables. Formally, it is defined as follows.

Definition 6.1 (The CNF encoding $\mathsf{BT}^\bullet\mathsf{Rank}_n^m(A)$)**.** Assume $m > n$ are positive integers and $A \in \{0,1\}^{m\times m}$ is an m by m Boolean matrix. The CNF encoding the (simple) bamboo tree rank formula, denoted $\mathsf{BT}^\bullet\mathsf{Rank}_n^m(A)$, uses input variables $x_{i,k}, y_{k,i} : i \in [m], k \in [n]$ together with extension variables $u_{i,j,k} : i,j \in [m], k \in [n]$, and consists of the following axioms.

Output Axioms: For every $i,j \in [m]$, the clause $u_{i,j,n}$ if $A_{i,j} = 1$ and the clause $\neg u_{i,j,n}$ if $A_{i,j} = 0$.

Summation Base Axioms: For every $i,j \in [m]$, $u_{i,j,1} = x_{i,1}y_{1,j}$, encoded by the clauses $u_{i,j,1} \vee \neg x_{i,1} \vee \neg y_{1,j}$, $x_{i,1} \vee \neg u_{i,j,1}$ and $y_{1,j} \vee \neg u_{i,j,1}$.

Summation Axioms: For every $i,j \in [m]$, and $k \in \{2,\dots,n\}$, $u_{i,j,k} = u_{i,j,k-1} \oplus x_{i,k}y_{k,j}$, encoded by the following six clauses:

$$
\begin{aligned}
&x_{i,k} \vee \neg u_{i,j,k-1} \vee u_{i,j,k},\\
&x_{i,k} \vee u_{i,j,k-1} \vee \neg u_{i,j,k},\\
&y_{k,j} \vee \neg u_{i,j,k-1} \vee u_{i,j,k},\\
&y_{k,j} \vee u_{i,j,k-1} \vee \neg u_{i,j,k},\\
&\neg x_{i,k} \vee \neg y_{k,j} \vee \neg u_{i,j,k-1} \vee \neg u_{i,j,k},\\
&\neg x_{i,k} \vee \neg y_{k,j} \vee u_{i,j,k-1} \vee u_{i,j,k}.
\end{aligned}
$$

We will also consider the substitution instance of $\mathsf{BT}^\bullet\mathsf{Rank}$, denoted as $\mathsf{BT}^\bullet\mathsf{Rank}'$. In this instance, the last row of X and the last column of Y are substituted with ones. Specifically, for every $k \in [n]$, we assign $x_{m,k} = y_{k,m} = 1$ and $u_{m,m,k} = k \bmod 2$.

Instead of reducing $\mathsf{BT}^\bullet\mathsf{Rank}_n^m(A)$ to PHP, we can perform a reduction to $\mathsf{BT}^\bullet\mathsf{Rank}'^{\tilde{m}}_{\tilde{n}}(\tilde{A})$ and explicitly prove the degree lower bound for the latter formula.

6.1 Row Degree Lower Bound

We start by proving the degree bound on $\mathsf{BT}^\bullet\mathsf{Rank}'^m_n(A)$.

Definition 6.2. Let t be a term in the variables of $\mathsf{BT}^\bullet\mathsf{Rank}'^m_n(A)$. We say that $i \in [m-1]$ is *X-row-mentioned in t* if there are $k \in [n]$ and $b \in \{0,1\}$ such that $x^b_{i,k}$ appears in t. We say that $j \in [m-1]$ is *Y^T-row-mentioned in t* if there are $k \in [n]$ and $b \in \{0,1\}$ such that $y^b_{k,j}$ appears in t. We say that $i \in [m-1]$ is *U-left-row-mentioned in t* if there are $j \in [m]$, $k \in [n]$ and $b \in \{0,1\}$ such that $u^b_{i,j,k}$ appears in t. We say that $j \in [m-1]$ is *U-right-row-mentioned in t* if there are $i \in [m]$, $k \in [n]$ and $b \in \{0,1\}$ such that $u^b_{i,j,k}$ appears in t.

Definition 6.3 (Row degree)**.** Let t be a term in the variables of $\mathsf{BT}^\bullet\mathsf{Rank}'^m_n(A)$. Let I be the set of all $i \in [m-1]$ that are either X-row-mentioned or U-left-row-mentioned in t. Similarly, let J be the set of all $j \in [m-1]$ that are either Y^T-row-mentioned or U-right-row-mentioned in t. We say that t *mentions* rows (I,J). The *row degree* of t is defined as the sum $|I| + |J|$.

Lower bounds on the SA degree are typically established by constructing a *pseudoexpectation*, which is a linear mapping that satisfies the following properties: it maps all low-degree multilinear polynomials to $\mathbb{R}$, vanishes on multiples of the axioms, and is non-zero on the constant-1 polynomial. We present such a mapping for multilinear terms with small row degree.

Lemma 6.4. *For every $m > n$ and every $A \in \{0,1\}^{m\times m}$ with $A_{m,m} = n \bmod 2$ and $A_{i,m} = A_{m,i} = 1$, for all $i \in [m-1]$, every* SA *refutation of $\mathsf{BT}^\bullet\mathsf{Rank}'^m_n(A)$ requires row degree $n-1$.*

Proof. We construct a linear mapping

$$R\colon \mathbb{R}[\vec{x},\vec{y},\vec{u}]/(\vec{x}^2-\vec{x},\vec{y}^2-\vec{y},\vec{u}^2-\vec{u}) \to \mathbb{R}$$

that satisfies the following properties.

1. $R(1) = 1$.
2. $R(t) \geq 0$ for every term t with row degree at most n.
3. For every axiom axiom and every term t such that $\mathsf{axiom} \cdot t$ mentions at most n rows, $R(\mathsf{axiom} \cdot t) = 0$.

This mapping rules out the existence of a refutation of $\mathsf{BT}^{\bullet}\mathsf{Rank}_n'^m(A)$ with row degree at most n. Indeed, in any SA refutation of $\mathsf{BT}^{\bullet}\mathsf{Rank}_n'^m(A)$, the left-hand side becomes non-negative under R, while the right-hand side evaluates to $R(-1) = -1$, leading to a contradiction.

Let $I, J \subseteq \{2, \ldots, m\}$ with $d = |I| + |J| \leq n$. We define the random partial assignment $\rho_{I,J}$ as follows.

1. Sample random matrices $M \in \{0,1\}^{I \cup \{m\} \times [n]}$ and $N \in \{0,1\}^{[n] \times J \cup \{m\}}$ of full rank such that $MN = A_{I \cup \{m\}, J \cup \{m\}}$ and for every $k \in [n]$, $M_{m,k} = N_{k,m} = 1$.
2. Assign $\rho(X_{I,[n]}) = M$, meaning that for every $i \in I$ and $k \in [n]$, set $\rho(x_{i,k}) = M_{i,k}$. Similarly, assign $\rho(Y_{[n],J}) = N$: for every $j \in J$ and $k \in [n]$, set $\rho(y_{k,j}) = N_{k,j}$.
3. For every $(i,j) \in ((I \cup \{m\}) \times (J \cup \{m\}) \setminus \{(1,1)\})$, and $k \in [n]$, set $\rho(u_{i,j,k}) = \sum_{\ell=1}^{k} M_{i,\ell} N_{\ell,j} \bmod 2$.
4. For every variable θ assigned by ρ, set $\rho(\overline{\theta}) = 1 - \rho(\theta)$.

Let t be a term in the variables of $\mathsf{BT}^{\bullet}\mathsf{Rank}_n'^m(A)$ with row degree at most $n-2$; namely, it mentions rows (I,J) with $|I| + |J| \leq n-2$. We define $R(t) = \Pr[\rho_{I,J}(t) = 1]$. Note that $\rho_{I,J}$ assigns values to all the variables in t, which implies that $\rho_{I,J}(t) \in \{0,1\}$.

A key property of R is that $\rho_{I,J}$ remains consistent when extended to larger sets of rows. Let $I, J \subseteq [m-1]$ with $|I| + |J| < n-2$ and let $J' = J \cup \{j_0\}$. We show how to inductively sample the pair of matrices (M, N'), where $M \in \{0,1\}^{I \cup \{m\} \times [n]}$ and $N' \in \{0,1\}^{[n] \times J' \cup \{m\}}$, such that $MN' = A_{I \cup \{m\}, J' \cup \{m\}}$ and for every $k \in [n]$, $M_{m,k} = N'_{k,m} = 1$.

1. Sample full-rank matrices $M \in \{0,1\}^{I \cup \{m\} \times [n]}$ and $N \in \{0,1\}^{[n] \times J \cup \{m\}}$, such that $MN = A_{I \cup \{m\}, J \cup \{m\}}$ and for every $k \in [n]$, $M_{m,k} = N_{k,m} = 1$.
2. Sample a vector $v \in \{0,1\}^n$ such that $Mv = A_{I \cup \{m\}, j_0}$, and the matrix $N' = \begin{bmatrix} N & v \end{bmatrix}$ has full rank, i.e., $\operatorname{rank}(N') = |J| + 2$.

This process is equivalent to just sampling (M, N') uniformly. Indeed, for a fixed pair of matrices (M, N), the number of choices for v is independent of the choice of the pair (M, N). We demonstrate this as follows. Since M has full rank, there are $2^{n-|I|-1}$ possible choices for v that satisfy $Mv = A_{I \cup \{m\}, j_0}$. The rank of N' can be either $|J|+1$ or $|J|+2$. It equals $|J|+1$ if and only if v is linearly dependent with the rows of N, i.e., there exists a vector $\mu \in \{0,1\}^{J \cup \{m\}}$ such that $N\mu = v$. Moreover, each such μ corresponds uniquely to a v since N has full rank. Substituting $N\mu = v$ into $Mv = A_{I,j_0}$, we find that μ must satisfy $MN\mu = A_{I,j_0}$, which simplifies to $A_{I,J}\mu = A_{I,j_0}$ due to our choice of M and N. Let ν denote the number of solutions to the linear system $A_{I,J}\mu = A_{I,j_0}$ and observe that $\nu \leq 2^{|J|+1}$. Therefore, there are $2^{n-|I|-1} - \nu$ choices for v that satisfy $Mv = A_{I,j_0}$ and ensure $\operatorname{rank}(N') = |J| + 2$. This number is positive when $2^{n-|I|-1} > 2^{|J|+1} \geq \nu$, which holds when $|I| + |J| < n-2$. Clearly, ν depends only on A and is independent of the specific choice of M and N.

Similarly, by symmetry, we can sample $M' \in \{0,1\}^{I' \cup \{m\} \times [n]}$ and $N \in \{0,1\}^{[n] \times J \cup \{m\}}$, where $I' = I \cup \{i_0\}$, if we can sample M and N.

This implies that the matrices M and N in the definition of $\rho_{I,J}$ always exist. For the base case $I = J = \varnothing$, we have $M = (1, \ldots, 1)$ and $N = (1, \ldots, 1)^T$ and the inductive steps follows from the reasoning above.

Similarly, for every term t with row degree at most $n-2$ that mentions rows (I,J), and for every $I' \supseteq I$ and $J' \supseteq J$ with $|I'|+|J'| \le n-2$, it holds that $\Pr[\rho_{I,J}(t)=1] = \Pr[\rho_{I',J'}(t)=1]$. This can be proved by induction on $|I' \setminus I| + |J' \setminus J|$. The base case, where $I=I'$ and $J=J'$, is trivial. The inductive step again follows from the above inductive construction.

The last property simplifies verifying the properties of R. Let t be a term and axiom an axiom of $\mathsf{BT}^{\bullet}\mathsf{Rank}_n^m(A)$. Suppose the polynomial $t \cdot \mathsf{axiom}$ mentions rows I of X and rows J of Y^T, with $|I|+|J| \le n$. Expanding $t \cdot \mathsf{axiom}$ as a sum of monomials $\sum_{\ell=1}^{q} t_\ell$, where each monomial t_ℓ mentions rows $I_\ell \subseteq I$ and $J_\ell \subseteq J$, we have:

$$\begin{aligned} R(t \cdot \mathsf{axiom}) &= R(\sum_{\ell=1}^{q} t_\ell) = \sum_{\ell=1}^{q} R(t_\ell) = \sum_{\ell=1}^{q} \Pr[\rho_{I_\ell,J_\ell}(t)=1] = \sum_{\ell=1}^{q} \Pr[\rho_{I,J}(t)=1] \\ &= \sum_{\ell=1}^{q} \mathbb{E}[\rho_{I,J}(t)] = \mathbb{E}[\sum_{\ell=1}^{q} \rho_{I,J}(t)] = \mathbb{E}[\rho_{I,J}(t \cdot \mathsf{axiom})] = 0. \end{aligned}$$

The last equality holds because $t \cdot \mathsf{axiom}$ evaluates to zero under *every* choice of matrices M and N in $\rho_{I,J}$. □

6.2 Size to Row Degree Reduction

We need the matrices $\mathcal{D}$ and $\mathcal{E}$ (they are used in the iterated BTRank bound).

$$\mathcal{D} = \begin{pmatrix} 1 & * & 1 & 0 & 0 & * & * & * \\ 0 & 1 & * & 1 & * & * & * & 0 \\ * & * & 0 & * & 1 & 0 & 1 & * \\ * & 0 & * & * & * & 1 & 0 & 1 \end{pmatrix}, \quad \mathcal{E} = \begin{pmatrix} 1 & 0 & 0 & 1 & * & * & * & * \\ 0 & * & 1 & * & 1 & * & 0 & * \\ * & 1 & * & 0 & * & 0 & * & 1 \\ * & * & * & * & 0 & 1 & 1 & 0 \end{pmatrix}.$$

The following definition is similar to Definition 5.20.

Definition 6.5 (Random substitution ρ)**.** Assume $m > n \ge 20$ and $(n-4)$ is divisible by 16. Let $\tilde{n} = (n-4)/8$ and $\{\tilde{x}_{i,k} : i \in [m], k \in [\tilde{n}]\}$, $\{\tilde{y}_{k,j} : j \in [m], k \in [\tilde{n}]\}$ and $\{\tilde{u}_{i,j,k} : i,j \in (([m+1] \times [m+1]) \setminus (1,1)), k \in [\tilde{n}]\}$ be fresh variables. Given $k \in \{3,\dots,n-2\}$, let $\iota(k) = ((k-3) \bmod \tilde{n})+1$ and $\nu(k) = \lfloor \frac{k-3}{\tilde{n}} \rfloor + 1$. A random substitution ρ is chosen as follows.

1. For each $i \in [m]$, uniformly and independently sample $s_i, r_i \in [4]$ and $\alpha_i, \beta_i \in \{0,1\}$.
2. For each $i \in [m]$ and $k \in [n]$, set

$$\rho(x_{i,k}) = \begin{cases} \alpha_i & \text{if } k \in \{1, n-1\}, \\ 1 & \text{if } k \in \{2, n\}, \\ \tilde{x}_{i,\iota(k)} & \text{if } k \in \{3,\dots,n-2\} \text{ and } \mathcal{D}_{s_i,\nu(k)} = *, \\ \mathcal{D}_{s_i,\nu(k)} & \text{if } k \in \{3,\dots,n-2\} \text{ and } \mathcal{D}_{s_i,\nu(k)} \in \{0,1\}. \end{cases}$$

3. For each $j \in [m]$ and $k \in [n]$, set

$$\rho(y_{k,j}) = \begin{cases} 1 & \text{if } k \in \{1, n-1\}, \\ \beta_j & \text{if } k \in \{2, n\}, \\ \tilde{y}_{\iota(k),j} & \text{if } k \in \{3,\dots,n-2\} \text{ and } \mathcal{E}_{r_j,\nu(k)} = *, \\ \mathcal{E}_{r_j,\nu(k)} & \text{if } k \in \{3,\dots,n-2\} \text{ and } \mathcal{E}_{r_j,\nu(k)} \in \{0,1\}. \end{cases}$$

4. For each $i,j \in [m]$ and $k \in [n]$, we define $\rho(u_{i,j,k})$ according to $\sum_{\ell=1}^{k} \rho(x_{i,\ell})\rho(y_{\ell,j}) \bmod 2$. Given $k \in \{3,\dots,n-2\}$, let $p_{i,j,k} = \sum_{\ell=1}^{(\nu(k)-1)\tilde{n}+2} \rho(x_{i,\ell})\rho(y_{\ell,j}) \bmod 2$ simplified under the assumptions $\sum_{\ell=1}^{\tilde{n}} \tilde{x}_{i,\ell}\tilde{y}_{\ell,j} = A_{i,j} \bmod 2$, $\sum_{\ell=1}^{\tilde{n}} \tilde{x}_{i,\ell} = 1 \bmod 2$ and $\sum_{\ell=1}^{\tilde{n}} \tilde{y}_{\ell,j} = 1 \bmod 2$. Then

for each $i, j \in [m]$ and $k \in [n]$, set

$$\rho(u_{i,j,k}) = \begin{cases} \alpha_i & \text{if } k = 1, \\ \alpha_i \oplus \beta_j & \text{if } k = 2, \\ A_{i,j} \oplus \beta_j & \text{if } k = n-1, \\ A_{i,j} & \text{if } k = n, \\ \tilde{u}_{i,j,\iota(k)}^{1-p_{i,j,k}} & \text{if } k \in \{3,\dots,n-2\}, \mathcal{D}_{s_i,\nu(k)} = \mathcal{E}_{r_j,\nu(k)} = *, \\ \tilde{u}_{i,m+1,\iota(k)}^{1-p_{i,j,k}} & \text{if } k \in \{3,\dots,n-2\}, \mathcal{D}_{s_i,\nu(k)} = *, \mathcal{E}_{r_j,\nu(k)} = 1, \\ \tilde{u}_{m+1,j,\iota(k)}^{1-p_{i,j,k}} & \text{if } k \in \{3,\dots,n-2\}, \mathcal{D}_{s_i,\nu(k)} = 1, \mathcal{E}_{r_j,\nu(k)} = *, \\ p_{i,j,k} \oplus (\iota(k) \bmod 2) & \text{if } k \in \{3,\dots,n-2\}, \mathcal{D}_{s_i,\nu(k)} = \mathcal{E}_{r_j,\nu(k)} = 1, \\ p_{i,j,k} & \text{if } k \in \{3,\dots,n-2\}, \mathcal{D}_{s_i,\nu(k)} = 0 \text{ or } \mathcal{E}_{r_j,\nu(k)} = 0. \end{cases}$$

Lemma 6.6. *Assume $m > n \geq 20$, $(n-4)$ is divisible by 16 and $A \in \{0,1\}^{m \times m}$ is a Boolean matrix. Let t be a term in the variables of $\mathsf{BT}^\bullet\mathsf{Rank}_n^m(A)$ and t' be a subterm of t such that t' does not mention columns $\{1, 2, n-1, n\}$ but mentions rows (I, J) for some $I, J \subseteq [m]$. Then $\Pr[t \restriction \rho \neq 0] \leq (\sqrt{7/8})^{|I|+|J|}$.*

Proof. Consider the bipartite graph G with parts I and J and edges

$$\{(i,j) : \exists b \in \{0,1\}, k \in [n] \text{ such that } u_{i,j,k}^b \text{ appears in } t'\}.$$

Let t'' be a minimal subterm of t' that mentions rows (I, J). In terms of G, the term t'' corresponds to one of its minimal edge covers. Such a cover does not contain any paths of length three, thus its connected components are

- isolated vertices $x_{i,k}^b$ or $y_{k,j}^b$,
- stars $\prod_{(j,k)\in P} u_{i_0,j,k} \prod_{(j,k)\in N} \overline{u}_{i_0,j,k}$ and $\prod_{(i,k)\in P} u_{i,j_0,k} \prod_{(i,k)\in N} \overline{u}_{i,j_0,k}$,

and each of these components mentions its own disjoint set of indices.

In the first case, for every $b \in \{0,1\}$, we have $\Pr\left[\rho(x_{i,k}^b) \neq 0\right] = \Pr\left[\rho(y_{k,j}^b) \neq 0\right] = 3/4$.

In the second case, assume that we have a star with r rays, say $s = \prod_{(j,k)\in P} u_{i_0,j,k} \prod_{(j,k)\in N} \overline{u}_{i_0,j,k}$ where $|P|+|N| = r$. This star U-left-row-mentions index $i_0 \in I$ and U-right-row-mentions r indices $\{j : \exists k \in N \colon (j,k) \in P \sqcup N\} \subseteq J$. For every $s \in [4]$ and $\alpha \in \{0,1\}$, the events

$$(u_{i_0,j,k} \restriction \rho \neq 0 \mid s_{i_0} = s, \alpha_{i_0} = \alpha), \text{ where } (j,k) \in P,$$

and

$$(\overline{u}_{i_0,j,k} \restriction \rho \neq 0 \mid s_{i_0} = s, \alpha_{i_0} = \alpha), \text{ where } (j,k) \in N,$$

are independent and each happen with probability at most $7/8$. Thus, all of them simultaneously do not happen with probability at most $(7/8)^r \leq (\sqrt{7/8})^{r+1}$. It implies that

$$\Pr[t' \restriction \rho \neq 0] \leq \Pr[t'' \restriction \rho \neq 0] \leq (\sqrt{7/8})^{|I|+|J|}. \qquad \square$$

The substitution ρ transforms any refutation of $\mathsf{BT}^\bullet\mathsf{Rank}$ into a refutation of $\mathsf{BT}^\bullet\mathsf{Rank}'$.

Lemma 6.7. *Assume $m > n \geq 20$, $(n-4)$ is divisible by 16 and $A \in \{0,1\}^{m \times m}$ is a Boolean matrix. Let $\tilde{A}$ be an $(m+1) \times (m+1)$ Boolean matrix defined as*

$$\tilde{A}_{i,j} = \begin{cases} A_{i,j} & i \in [m] \text{ and } j \in [m], \\ n \bmod 2 & \text{if } i = m+1 \text{ and } j = m+1, \\ 1 & \text{if } i = m+1 \text{ and } j \in [m], \\ 1 & \text{if } i \in [m] \text{ and } j = m+1. \end{cases}$$

Then for every SA *refutation* Π *of* $\mathsf{BT}^\bullet\mathsf{Rank}_n^m(A)$, $\Pi \upharpoonright \rho$ *is a refutation of* $\mathsf{BT}^\bullet\mathsf{Rank}'^{m+1}_{(n-4)/8}(\tilde{A})$.

Proof. Every Output Axiom $u_{i,j,n}^{A_{i,j}}$ is either satisfied, or becomes the Output Axiom of the form $\tilde{u}_{i,j,\tilde{n}}^{A_{i,j}}$, $\tilde{u}_{i,m+1,\tilde{n}}$ or $\tilde{u}_{j,m+1,\tilde{n}}$.

Every set of Summation Base Axioms encoding $u_{i,j,1} = x_{i,1}y_{1,j}$ is either satisfied or encodes the statement of the form $\tilde{u}_{i,j,1} = \tilde{x}_{i,1}\tilde{y}_{1,j}$, $\tilde{u}_{i,m+1,1} = \tilde{x}_{i,1}$ or $\tilde{u}_{m+1,j,1} = \tilde{y}_{1,j}$.

Every set of Summation Axioms encoding $u_{i,j,k} = u_{i,j,k-1} \oplus x_{i,k}y_{k,j}$ is

- either satisfied,
- encodes the statement of the form $\tilde{u}_{i,j,\iota(k)} = \tilde{u}_{i,j,\iota(k)-1} \oplus \tilde{x}_{i,\iota(k)}\tilde{y}_{\iota(k),j}$, $\tilde{u}_{i,m+1,\iota(k)} = \tilde{u}_{i,j,\iota(k)-1} \oplus \tilde{x}_{i,\iota(k)}$ or $\tilde{u}_{m+1,j,\iota(k)} = \tilde{u}_{i,j,\iota(k)-1} \oplus \tilde{y}_{\iota(k),j}$, or
- becomes the Output Axiom of the form $\tilde{u}_{i,j,\tilde{n}}^{A_{i,j}}$, $\tilde{u}_{i,m+1,\tilde{n}}$ or $\tilde{u}_{j,m+1,\tilde{n}}$. □

Theorem 6.8. *Assume* $m > n \geq 20$, $(n-4)$ *is divisible by* 16 *and* $A \in \{0,1\}^{m\times m}$ *is a Boolean matrix. Then any* SA *refutation of* $\mathsf{BT}^\bullet\mathsf{Rank}_n^m(A)$ *requires size* $(\sqrt{8/7})^{(n-4)/8-1}$.

Proof. Let $\tilde{n} = (n-4)/8$ and suppose, for the sake of contradiction, that there exists a refutation Π of $\mathsf{BT}^\bullet\mathsf{Rank}_n^m(A)$ with size $|\Pi| < (\sqrt{8/7})^{\tilde{n}-1}$. By Lemma 6.7, $\Pi \upharpoonright \rho$ is a refutation of $\mathsf{BT}^\bullet\mathsf{Rank}'^{m+1}_{\tilde{n}}(\tilde{A})$, which requires row degree $\tilde{n}-1$ by Lemma 6.4. By the union bound and Lemma 6.6, there exists ρ such that every term of row degree at least $\tilde{n}-1$ vanishes from $\Pi \upharpoonright \rho$. This leads to a contradiction. □

7 Structural Results

7.1 Amplification of the Rank Principle

In this section, we prove an amplification theorem for the weak rank principle, namely that the proof complexity of Rank_n^m is robust for different choices of parameters (m,n), under low-degree algebraic reductions and assuming that m and n are not too close. The proof is an adaptation of known amplification theorems for weak pigeonhole principles [42, 61, 80]. This result should be regarded as a basic property of the weak rank principle that essentially follows from previous constructions. Nonetheless, it plays a foundational role in later sections, and we include it here for completeness. Moreover, this result provides another aspect in which the weak rank principle behaves similarly to the weak pigeonhole principles.

Theorem 7.1. *Let* $m > 2n$ *be positive integers,* $\epsilon > 0$, *and* $d = O(\epsilon^{-1}\log(m/n))$, *then there is a degree-*d *algebraic reduction*

$$\mathsf{Rank}_n^{(1+\epsilon)n} \leq_d^{\mathrm{alg}} \mathsf{Rank}_n^m.$$

We prove Theorem 7.1 in two steps. First, we reduce Rank_n^{2n} to Rank_n^m for arbitrarily large m.

Theorem 7.2. *Let* $m > 2n$ *be positive integers and* $d = \lceil \log(m/n) \rceil$. *Then there is a degree-*d *algebraic reduction*

$$\mathsf{Rank}_n^{2n} \leq_d^{\mathrm{alg}} \mathsf{Rank}_n^m.$$

Proof. Let $X \in \mathbb{F}^{2n\times n}$ and $Y \in \mathbb{F}^{n\times 2n}$ be the variables of Rank_n^{2n}. For every positive integer i, we will build a reduction from Rank_n^{2n} to $\mathsf{Rank}_n^{2^i n}$ inductively. Let $X^{(i)} \in \mathbb{F}^{2^i n\times n}$ and $Y^{(i)} \in \mathbb{F}^{n\times 2^i n}$ be the variables of $\mathsf{Rank}_n^{2^i n}$. Abusing notation, we will also specify our reduction $R_i : \mathbb{F}^{4n^2} \to \mathbb{F}^{2^{i+1}n^2}$ by defining the following two matrices $X^{(i)} \in \mathbb{F}^{2^i n\times n}$ and $Y^{(i)} \in \mathbb{F}^{n\times 2^i n}$ whose entries are polynomials over (X,Y).

This is done inductively. First, $X^{(1)} = X$ and $Y^{(1)} = Y$. For each $i > 1$:

$$X^{(i+1)} = \underbrace{\begin{pmatrix} X^{(i)} & 0 \\ 0 & X^{(i)} \end{pmatrix}}_{2^{i+1}n\times 2n} \cdot \underbrace{X}_{2n\times n}, \quad Y^{(i+1)} = \underbrace{Y}_{n\times 2n} \cdot \underbrace{\begin{pmatrix} Y^{(i)} & 0 \\ 0 & Y^{(i)} \end{pmatrix}}_{2n\times 2^{i+1}n}.$$

The idea underlying our reduction is that if $XY = I_{2n}$, then $X^{(i)}Y^{(i)} = I_{2^i n}$ for every $i \geq 1$. This is easily seen by an induction on i:

$$\begin{aligned} X^{(i+1)}Y^{(i+1)} &= \begin{pmatrix} X^{(i)} & 0 \\ 0 & X^{(i)} \end{pmatrix} XY \begin{pmatrix} Y^{(i)} & 0 \\ 0 & Y^{(i)} \end{pmatrix} \\ &= \begin{pmatrix} X^{(i)} & 0 \\ 0 & X^{(i)} \end{pmatrix} \begin{pmatrix} Y^{(i)} & 0 \\ 0 & Y^{(i)} \end{pmatrix} \\ &= I_{2^{i+1}n}. \end{aligned}$$

It is easy to see that each entry of $X^{(i)}$ ($Y^{(i)}$ respectively) is a degree-i polynomial over X (Y respectively). Now we prove that each axiom of $\mathsf{Rank}_n^{2^i n}$, when composed with our reduction R, admits a degree-$2i$ NS-proof from the axioms of Rank_n^{2n}. Again, this is via an induction on i. The case when $i = 1$ is trivial; assuming this is true for $\mathsf{Rank}_n^{2^i n}$, we prove this for $\mathsf{Rank}_n^{2^{i+1} n}$:

$$\begin{aligned} & X^{(i+1)}Y^{(i+1)} - I_{2^{i+1}n} \\ &= \begin{pmatrix} X^{(i)} & 0 \\ 0 & X^{(i)} \end{pmatrix} XY \begin{pmatrix} Y^{(i)} & 0 \\ 0 & Y^{(i)} \end{pmatrix} - I_{2^{i+1}n} \\ &= \begin{pmatrix} X^{(i)} & 0 \\ 0 & X^{(i)} \end{pmatrix} \begin{pmatrix} Y^{(i)} & 0 \\ 0 & Y^{(i)} \end{pmatrix} + \begin{pmatrix} X^{(i)} & 0 \\ 0 & X^{(i)} \end{pmatrix} (XY - I_{2n}) \begin{pmatrix} Y^{(i)} & 0 \\ 0 & Y^{(i)} \end{pmatrix} - I_{2^{i+1}n} \\ &= \underbrace{\begin{pmatrix} X^{(i)}Y^{(i)} - I_{2^i n} & 0 \\ 0 & X^{(i)}Y^{(i)} - I_{2^i n} \end{pmatrix}}_{\text{(Part I)}} + \underbrace{\begin{pmatrix} X^{(i)} & 0 \\ 0 & X^{(i)} \end{pmatrix} (XY - I_{2n}) \begin{pmatrix} Y^{(i)} & 0 \\ 0 & Y^{(i)} \end{pmatrix}}_{\text{(Part II)}}. \end{aligned}$$

By our induction hypothesis, each entry of (Part I) admits a degree-$2i$ NS-proof from the axioms of Rank_n^{2n}. Since the axioms of Rank_n^{2n} only express $XY = I_{2n}$, and each $X^{(i)}$ and $Y^{(i)}$ are degree-i polynomials over (X, Y), it follows that each entry of (Part II) also admits a degree-$2i$ NS-proof from the axioms of Rank_n^{2n}. This proves our claim for $i + 1$.

Now we wrap up the proof. Let $k = \lceil \log(m/n) \rceil$ be the smallest integer such that $2^k n \geq m$. Let $X' \in \mathbb{F}^{m \times n}$ and $Y' \in \mathbb{F}^{n \times m}$ be the variables of Rank_n^m. Given (X, Y), our reduction sets X' to be the first m rows of $X^{(k)}$ and sets Y' to be the first m columns of $Y^{(k)}$. It is easy to see that the reduction can be computed in degree k and that each axiom of Rank_n^m admits a degree-$2k$ NS-proof from the axioms of Rank_n^{2n}. □

Now we reduce $\mathsf{Rank}_n^{(1+\epsilon)n}$ to Rank_n^{2n}. The proof idea is very similar to that of Theorem 7.2 but we include the full proof here for completeness.

Theorem 7.3. *Let n be a positive integer, $\epsilon > 0$ such that ϵn is an integer, and $d = \lceil 1/\epsilon \rceil$. Then there is a degree-d algebraic reduction*

$$\mathsf{Rank}_n^{(1+\epsilon)n} \leq_d^{\text{alg}} \mathsf{Rank}_n^{2n}.$$

Proof. Let $X \in \mathbb{F}^{(1+\epsilon)n \times n}$ and $Y \in \mathbb{F}^{n \times (1+\epsilon)n}$ be the variables of $\mathsf{Rank}_n^{(1+\epsilon)n}$. For every positive integer i, we will build a reduction from $\mathsf{Rank}_n^{(1+\epsilon)n}$ to $\mathsf{Rank}_n^{(1+i\epsilon)n}$ inductively. Let $X^{(i)} \in \mathbb{F}^{(1+i\epsilon)n \times n}$ and $Y^{(i)} \in \mathbb{F}^{n \times (1+i\epsilon)n}$ be the variables of $\mathsf{Rank}_n^{(1+i\epsilon)n}$. Abusing notation, we will also specify our reduction $R : \mathbb{F}^{2(1+\epsilon)n^2} \to \mathbb{F}^{2(1+i\epsilon)n^2}$ by defining the following two matrices $X^{(i)}$ and $Y^{(i)}$ whose entries are polynomials over (X, Y).

This is done inductively. First, $X^{(1)} = X$ and $Y^{(1)} = Y$. For each $i > 1$:

$$X^{(i+1)} = \underbrace{\begin{pmatrix} X^{(i)} & 0 \\ 0 & I_{\epsilon n} \end{pmatrix}}_{(1+(i+1)\epsilon)n \times (1+\epsilon)n} \cdot \underbrace{X}_{(1+\epsilon)n \times n}, \quad Y^{(i+1)} = \underbrace{Y}_{n \times (1+\epsilon)n} \cdot \underbrace{\begin{pmatrix} Y^{(i)} & 0 \\ 0 & I_{\epsilon n} \end{pmatrix}}_{(1+\epsilon)n \times (1+(i+1)\epsilon)n}.$$

For the sake of intuition, let us see that if $XY = I_{(1+\epsilon)n}$, then $X^{(i)}Y^{(i)} = I_{(1+i\epsilon)n}$ for every $i \geq 1$. This is via an induction over i:

$$\begin{aligned} X^{(i+1)}Y^{(i+1)} &= \begin{pmatrix} X^{(i)} & 0 \\ 0 & I_{\epsilon n} \end{pmatrix} XY \begin{pmatrix} Y^{(i)} & 0 \\ 0 & I_{\epsilon n} \end{pmatrix} \\ &= \begin{pmatrix} X^{(i)} & 0 \\ 0 & I_{\epsilon n} \end{pmatrix} \begin{pmatrix} Y^{(i)} & 0 \\ 0 & I_{\epsilon n} \end{pmatrix} \\ &= \begin{pmatrix} I_{(1+i\epsilon)n} & 0 \\ 0 & I_{\epsilon n} \end{pmatrix} \\ &= I_{(1+(i+1)\epsilon)n}. \end{aligned}$$

It is easy to see that each entry of $X^{(i)}$ ($Y^{(i)}$ respectively) is a degree-i polynomial over X (Y respectively). Now we prove that each axiom of $\mathsf{Rank}_n^{(1+i\epsilon)n}$, when composed with our reduction R, admits a degree-$2i$ NS-proof from the axioms of $\mathsf{Rank}_n^{(1+\epsilon)n}$. Again, this is via an induction on i. The case that $i = 1$ is trivial; assuming this is true for $\mathsf{Rank}_n^{(1+i\epsilon)n}$, we prove this for $\mathsf{Rank}_n^{(1+(i+1)\epsilon)n}$:

$$\begin{aligned} & X^{(i+1)}Y^{(i+1)} - I_{(1+(i+1)\epsilon)n} \\ &= \begin{pmatrix} X^{(i)} & 0 \\ 0 & I_{\epsilon n} \end{pmatrix} XY \begin{pmatrix} Y^{(i)} & 0 \\ 0 & I_{\epsilon n} \end{pmatrix} - I_{(1+(i+1)\epsilon)n} \\ &= \begin{pmatrix} X^{(i)} & 0 \\ 0 & I_{\epsilon n} \end{pmatrix} (XY - I_{(1+\epsilon)n}) \begin{pmatrix} Y^{(i)} & 0 \\ 0 & I_{\epsilon n} \end{pmatrix} + \begin{pmatrix} X^{(i)} & 0 \\ 0 & I_{\epsilon n} \end{pmatrix} \begin{pmatrix} Y^{(i)} & 0 \\ 0 & I_{\epsilon n} \end{pmatrix} - I_{(1+(i+1)\epsilon)n} \\ &= \underbrace{\begin{pmatrix} X^{(i)} & 0 \\ 0 & I_{\epsilon n} \end{pmatrix} (XY - I_{(1+\epsilon)n}) \begin{pmatrix} Y^{(i)} & 0 \\ 0 & I_{\epsilon n} \end{pmatrix}}_{\text{(Part I)}} + \underbrace{\begin{pmatrix} X^{(i)}Y^{(i)} - I_{(1+i\epsilon)n} & 0 \\ 0 & 0 \end{pmatrix}}_{\text{(Part II)}} \end{aligned}$$

By our induction hypothesis, each entry of (Part II) admits a degree-$2i$ NS-proof from the axioms of $\mathsf{Rank}_n^{(1+\epsilon)n}$. Since the axioms of $\mathsf{Rank}_n^{(1+\epsilon)n}$ only express $XY = I_{(1+\epsilon n)}$, and each $X^{(i)}$ and $Y^{(i)}$ are degree-i polynomials over (X, Y), it follows that each entry of (Part I) also admits a degree-$2i$ NS-proof from the axioms of $\mathsf{Rank}_n^{(1+\epsilon)n}$. This proves our claim for $i + 1$.

Now we wrap up the proof. Let $k = \lceil 1/\epsilon \rceil$ be the smallest integer such that $(1+k\epsilon)n \geq 2n$. Let $X' \in \mathbb{F}^{2n \times n}$ and $Y' \in \mathbb{F}^{n \times 2n}$ be the variables of Rank_n^{2n}. Given (X, Y), our reduction sets X' to be the first $2n$ rows of $X^{(k)}$ and sets Y' to be the first $2n$ columns of $Y^{(k)}$. It is easy to see that the reduction can be computed in degree k and that each axiom of Rank_n^{2n} admits a degree-$2k$ proof from the axioms of $\mathsf{Rank}_n^{(1+\epsilon)n}$. □

The takeaway message from the above two reductions is that the proof complexity of weak rank formulas Rank_n^m are robust (in the regime when m and n are not *too close*), in the sense that they can be reduced to each other via low-degree reductions.

Theorem 7.1. *Let $m > 2n$ be positive integers, $\epsilon > 0$, and $d = O(\epsilon^{-1} \log(m/n))$, then there is a degree-d algebraic reduction*

$$\mathsf{Rank}_n^{(1+\epsilon)n} \leq_d^{\text{alg}} \mathsf{Rank}_n^m.$$

Proof Sketch. This follows from Theorem 7.2, Theorem 7.3, and Fact 4.7. □

7.2 Low-Degree Reductions for WRank in Strong Proof Systems

For sufficiently strong proof systems closed under low-degree reductions, we show that it is enough to prove the hardness of WRank with $A = I$ to get a generator (namely, hardness of WRank for every A). We demonstrate this simple property for the bamboo-tree encoding $\mathsf{BT}^\bullet\mathsf{Rank}_n^m(A)$.

We show that the the formula $\mathsf{BT}^\bullet\mathsf{Rank}_n^m(A)$ can be reduced to $\mathsf{BT}^\bullet\mathsf{Rank}_n^r(I_r)$, where $r > n$, by a degree-1 reduction. The main idea consists of substitution $X' = AX$ and $Y' = Y$ into the statement $X'Y' = A$, thus obtaining $AXY = A$, which is derivable from $XY = I_r$.

Lemma 7.4. *Let $A \in \{0,1\}^{m\times m}$ be an arbitrary matrix of rank r with $r > n$. Then there is a degree-1 reduction from $\mathsf{BT}^\bullet\mathsf{Rank}^r_n(I_r)$ to $\mathsf{BT}^\bullet\mathsf{Rank}^m_n(A)$.*

Proof. Let the variables of $\mathsf{BT}^\bullet\mathsf{Rank}^r_n(I_r)$ be $X = (x_{i,k})_{i\in[r],k\in[n]}$, $Y = (y_{k,j})_{k\in[n],j\in[r]}$, and $U = (u_{i,j,k})_{i,j\in[r],k\in[n]}$, and the variables of $\mathsf{BT}^\bullet\mathsf{Rank}^m_n(A)$ be $X' = (x'_{i,k})_{i\in[m],k\in[n]}$, $Y' = (y'_{k,j})_{k\in[n],j\in[m]}$, and $U' = (u'_{i,j,k})_{i,j\in[m],k\in[n]}$. Here we are going to slightly abuse the notation of degree-1 reductions: we are going to construct the reduction R that substitutes (X', Y', U') with degree-1 polynomials in (X, Y, U), but the axioms of $\mathsf{BT}^\bullet\mathsf{Rank}^m_n(A) \circ R$ will have *constant degree* NS-proofs from the axioms of $\mathsf{BT}^\bullet\mathsf{Rank}^r_n(I_r)$. Since the axioms of $\mathsf{BT}^\bullet\mathsf{Rank}$ are themselves have constant degrees, this does not pose any problems and such a reduction is sufficient for our applications.

We can consider the following degree-1 reduction R that computes (X', Y', E') from (X, Y, E):

- for every $i \in [m], k \in [n]$, $x'_{i,k} = x_{i,k}$;
- for every $k \in [n], j \in [m]$, $y'_{k,j} = \sum_{b\in[r]} y_{k,b}A_{b,j}$;
- for every $i, j \in [m]$ and $k \in [n]$, $u'_{i,j,k} = \sum_{b\in[r]} A_{b,j}u_{i,b,k}$.

We show that $\mathsf{BT}^\bullet\mathsf{Rank}^r_n(I_r)$ reduces to $\mathsf{BT}^\bullet\mathsf{Rank}^m_n(A)$ under R.

Recall that in algebraic proof systems, we encode a clause $C = \bigvee_{i\in P} v_i \vee \bigvee_{i\in N} \neg v_i$ as the polynomial $\prod_{i\in P}(1 + v_i)\prod_{i\in N} v_i$. We give the following names to the axioms in $\mathsf{BT}^\bullet\mathsf{Rank}^r_n(I_r)$:

$$\begin{aligned}
\mathsf{OutAx}_{i,j} &= \delta_{i,j} + u_{i,j,n}, && i,j \in [r],\\
\mathsf{MultBaseAx}_{i,j} &= u_{i,j,0}, && i,j \in [r],\\
\mathsf{MultAx}^1_{i,j,k} &= (1 + x_{i,k})u_{i,j,k-1}(1 + u_{i,j,k}), && i,j \in [r], k \in [n],\\
\mathsf{MultAx}^2_{i,j,k} &= (1 + x_{i,k})(1 + u_{i,j,k-1})u_{i,j,k}, && i,j \in [r], k \in [n],\\
\mathsf{MultAx}^3_{i,j,k} &= (1 + y_{k,j})u_{i,j,k-1}(1 + u_{i,j,k}), && i,j \in [r], k \in [n],\\
\mathsf{MultAx}^4_{i,j,k} &= (1 + y_{k,j})(1 + u_{i,j,k-1})u_{i,j,k}, && i,j \in [r], k \in [n],\\
\mathsf{MultAx}^5_{i,j,k} &= x_{i,k}y_{k,j}u_{i,j,k-1}u_{i,j,k}; && i,j \in [r], k \in [n],\\
\mathsf{MultAx}^6_{i,j,k} &= x_{i,k}y_{k,j}(1 + u_{i,j,k-1})(1 + u_{i,j,k}), && i,j \in [r], k \in [n].
\end{aligned}$$

To simplify the proofs, we also consider the following three types of auxiliary polynomials:

$$\begin{aligned}
\mathsf{MultAx}^7_{i,j,k} &= (1 + x_{i,k})(u_{i,j,k-1} + u_{i,j,k}), && i,j \in [r], k \in [n],\\
\mathsf{MultAx}^8_{i,j,k} &= (1 + y_{k,j})(u_{i,j,k-1} + u_{i,j,k}), && i,j \in [r], k \in [n],\\
\mathsf{MultAx}^9_{i,j,k} &= x_{i,k}y_{k,j}(1 + u_{i,j,k-1} + u_{i,j,k}), && i,j \in [r], k \in [n].
\end{aligned}$$

It is easy to see that for all $i, j \in [r]$ and $k \in [n]$ (over characteristic 2):

$$\begin{aligned}
\mathsf{MultAx}^7_{i,j,k} &= \mathsf{MultAx}^1_{i,j,k} + \mathsf{MultAx}^2_{i,j,k},\\
\mathsf{MultAx}^8_{i,j,k} &= \mathsf{MultAx}^3_{i,j,k} + \mathsf{MultAx}^4_{i,j,k},\\
\mathsf{MultAx}^9_{i,j,k} &= \mathsf{MultAx}^5_{i,j,k} + \mathsf{MultAx}^6_{i,j,k}.
\end{aligned}$$

Let axiom be any polynomial from $\mathsf{BT}^\bullet\mathsf{Rank}^m_n(A)$. There are the following cases:

- **Output Axioms:** Suppose $\mathsf{axiom} = A_{i,j} + u'_{i,j,n}$, where $i, j \in [m]$. Then

$$\begin{aligned}
\mathsf{axiom} \circ R &= A_{i,j} + \sum_{b\in[r]} A_{b,j}u_{i,b,n}\\
&= \sum_{b\in[r]} C_{b,j}((\delta_{i,b} + u_{i,b,n}) + \delta_{i,b}) + A_{i,j}\\
&= \sum_{b\in[r]} A_{b,j}\mathsf{OutAx}_{i,b},
\end{aligned}$$

which is a linear combination of the axioms of $\mathsf{BT}^\bullet\mathsf{Rank}_n^r(I_r)$.

- **Multiplication Base Axioms:** Suppose $\mathsf{axiom} = u'_{i,j,0}$, where $i,j \in [m]$. Then

$$\mathsf{axiom} \circ R = \sum_{b\in[r]} A_{b,j} u_{i,b,0} = \sum_{b\in[r]} A_{b,j} \mathsf{MultBaseAx}_{i,b},$$

which is a linear combination of the axioms of $\mathsf{BT}^\bullet\mathsf{Rank}_n^r(I_r)$.

- **Multiplication Axioms:**

1. Suppose $\mathsf{axiom} = (1+x'_{i,k})u'_{i,j,k-1}(1+u'_{i,j,k})$, where $i,j \in [m]$, and $k \in [n]$. Then

$$\begin{aligned}\mathsf{axiom} \circ R &= (1+x_{i,k})\Big(\sum_{b_1\in[r]} A_{b_1,j} u_{i,b_1,k-1}\Big)\Big(1+\sum_{b_2\in[r]} A_{b_2,j} u_{i,b_2,k}\Big)\\ &= \sum_{b_1,b_2\in[r]} A_{b_1,j}A_{b_2,j} u_{i,b_1,k-1} \mathsf{MultAx}^7_{i,b_2,k},\end{aligned}$$

which is a degree-4 NS proof of $\mathsf{axiom} \circ R$ from $\mathsf{BT}^\bullet\mathsf{Rank}_n^r(I_r)$. This polynomial identity can be verified by induction on r.

2. Suppose $\mathsf{axiom} = (1+x'_{i,k})(1+u'_{i,j,k-1})u'_{i,j,k}$, where $i,j \in [m]$, and $k \in [n]$. Then $\mathsf{axiom}\circ R$ has a degree-4 NS-proof from $\mathsf{BT}^\bullet\mathsf{Rank}_n^r(I_r)$ due to symmetry: simply exchange $u_{a,b,k-1}$ and $u_{a,b,k}$ in Item 1.

3. Suppose $\mathsf{axiom} = (1+y'_{k,j})u'_{i,j,k-1}(1+u'_{i,j,k})$, where $i,j \in [m]$ and $k \in [n]$. Then

$$\begin{aligned}\mathsf{axiom} \circ R^2 &= (1+\sum_{b_3\in[r]} A_{b_3,j} y_{k,b_3})\Big(\sum_{b_1\in[r]} A_{b_1,j} u_{i,b_1,k-1}\Big)\Big(1+\sum_{b_2\in[r]} A_{b_2,j} e_{i,b_2,k}\Big)\\ &= \sum_{b_1,b_2\in[r]} A_{b_1,j}A_{b_2,j} u_{i,b_1,k-1} \mathsf{MultAx}^8_{i,b_2,k}\\ &\quad + \sum_{\substack{b_1,b_2,b_3\in[r]\\ b_2\neq b_3}} A_{b_1,j}A_{b_2,j}A_{b_3,j} y_{k,b_3} u_{i,b_1,k-1}(\mathsf{MultAx}^7_{i,b_2,k}\\ &\qquad + \mathsf{MultAx}^9_{i,b_2,k} + x_{i,k}\mathsf{MultAx}^8_{i,b_2,k}),\end{aligned}$$

which is a degree-6 NS proof of $\mathsf{axiom} \circ R$ from $\mathsf{BT}^\bullet\mathsf{Rank}_n^m(I)$.

4. Suppose $\mathsf{axiom} = (1+y'_{k,j})(1+u'_{i,j,k-1})u'_{i,j,k}$, where $i,j \in [m]$, and $k \in [n]$. Then $\mathsf{axiom}\circ R$ has a degree-6 NS-proof from $\mathsf{BT}^\bullet\mathsf{Rank}_n^r(I_r)$ due to symmetry: simply exchange $u_{a,b,k-1}$ and $u_{a,b,k}$ in Item 3.

5. Suppose $\mathsf{axiom} = x'_{i,k}y'_{k,j}u'_{i,j,k-1}u'_{i,j,k}$, where $i,j \in [m]$ and $k \in [n]$. Then

$$\begin{aligned}\mathsf{axiom} \circ R &= x_{i,k}\Big(\sum_{b_3\in[r]} A_{b_3,j} y_{k,b_3}\Big)\Big(\sum_{b_1\in[r]} A_{b_1,j} u_{i,b_1,k-1}\Big)\Big(\sum_{b_2\in[m]} A_{b_2,j} u_{i,b_2,k}\Big)\\ &= \sum_{b_1,b_2\in[r]} A_{b_1,j}A_{b_2,j} u_{i,b_1,k-1} \mathsf{MultAx}^9_{i,b_2,k}\\ &\quad + \sum_{\substack{b_1,b_2,b_3\in[r]\\ b_2\neq b_3}} A_{b_1,j}A_{b_2,j}A_{b_3,j} y_{k,b_3} u_{i,b_1,k-1}(\mathsf{MultAx}^9_{i,b_2,k}\\ &\qquad + x_{i,k}\mathsf{MultAx}^8_{i,b_2,k}),\end{aligned}$$

which is a degree-6 NS proof of $\mathsf{axiom} \circ R$ from $\mathsf{BT}^\bullet\mathsf{Rank}_n^r(I_r)$.

6. Suppose $\mathsf{axiom} = x'_{i,k}y'_{k,j}(1+u'_{i,j,k-1})(1+u'_{i,j,k})$, where $i,j \in [m]$ and $k \in [n]$. Then

$$\mathsf{axiom} \circ R = x_{i,k}\Big(\sum_{b_3\in[r]} A_{b_3,j} y_{k,b_3}\Big)\Big(\sum_{b_1\in[r]} A_{b_1,j} u_{i,b_1,k-1}\Big)\Big(\sum_{b_2\in[m]} A_{b_2,j} u_{i,b_2,k}\Big)$$

$$= \sum_{b_2 \in [r]} A_{b_2,j} \mathsf{MultAx}^9_{i,b_2,k}$$
$$+ \sum_{\substack{b_2,b_3 \in [r] \\ b_2 \neq b_3}} A_{b_2,j} A_{b_3,j} y_{k,b_3} (\mathsf{MultAx}^9_{i,b_2,k} + x_{i,k} \mathsf{MultAx}^8_{i,b_2,k})$$
$$+ (x'_{i,k} y'_{k,j} u'_{i,j,k-1} u'_{i,j,k}) \circ R,$$

which is a degree-6 NS proof of $\mathsf{axiom} \circ R$ from $\mathsf{BT}^{\bullet}\mathsf{Rank}^r_n(I_r)$. □

8 Hardness of Proving Circuit Lower Bounds

In this section, we show that there is a low-degree reduction from the weak rank principles to circuit lower bound statements. In other words, for every algebraic proof system $\mathcal{P}$ closed under low-degree reductions, if $\mathcal{P}$ cannot prove the weak rank principle, then $\mathcal{P}$ cannot prove circuit lower bounds for the truth table of any function. We also unconditionally show the hardness of such circuit lower bound statements for $\mathsf{PCR}_{\mathbb{F}_2}$. Although $\mathsf{PCR}_{\mathbb{F}_2}$, when measured by size, does not seem to be closed under low-degree reductions, we still manage to prove the hardness of circuit lower bound statements for $\mathsf{PCR}_{\mathbb{F}_2}$ by reducing them to an appropriate iterated variant of the weak rank principle.

Remark 8.1 (Comparison with [69, 72]). Razborov showed that low-degree polynomial calculus proofs [69] and short resolution proofs [72] cannot prove any circuit lower bounds. Both proofs proceed by first showing that (variants of) weak pigeonhole principles are hard for the underlying proof system and then reducing the weak pigeonhole principle to the circuit lower bound statements. Intuitively, these weak proof systems cannot prove circuit lower bounds because they cannot *count*.

Complementing Razborov's results above, in this section we show that there is a low-degree reduction from the rank principles to the circuit lower bound statements. Intuitively, weak proof systems that cannot reason about *linear algebra* cannot prove circuit lower bounds, either. Our result demonstrates yet another aspect in which the (weak) rank principles behave as an algebraic analogue of the (weak) pigeonhole principle.

Roughly speaking, our arguments uses *non-commutative algebraic branching programs* (ncABPs) as a proxy. Nisan [58] showed that the ncABP complexity of every non-commutative homogeneous polynomial f is *characterised* by the rank of certain matrix associated with f. Hence, if $\mathcal{P}$ cannot prove the weak rank principles, then $\mathcal{P}$ cannot prove any lower bound on the ncABP complexity of non-commutative homogeneous polynomials. In Section 8.1, we formalise the above intuition as a proof complexity reduction from the weak rank principles to polynomial equations expressing ncABP lower bound. Then, in Section 8.2, we show that the unprovability of ncABP lower bounds imply the unprovability of lower bounds for general Boolean circuits.

8.1 Lower Bounds for Non-commutative Algebraic Branching Programs

Fix an underlying field $\mathbb{F}$. We consider non-commutative polynomials over the variable set $X = \{x_1, x_2, \ldots, x_n\}$. Denote

$$X^k = \{x_{i_1} x_{i_2} \ldots x_{i_k} : i_1, i_2, \ldots, i_k \in [n]\}$$

as the set of degree-k non-commutative monomials.

Formalisation of ncABP lower bounds. Let f be a non-commutative homogeneous polynomial of degree d over the variable set $X = \{x_1, x_2, \ldots, x_n\}$. Let $\vec{r} = (r_0, r_1, \ldots, r_d)$ where $r_0 = r_d = 1$, we now define $\mathsf{lb}_{\mathrm{ncABP}}(f, \vec{r})$, which is a set of polynomial equations expressing that f cannot be computed by a non-commutative ABP where the i-th layer has r_i nodes.

(Variables) For every layer $1 \leq i \leq d$ and every variable x_j $(1 \leq j \leq n)$, there is a matrix $M_{i,x_j} \in \mathbb{F}^{r_{i-1} \times r_i}$ among the variables of $\mathsf{lb}_{\mathrm{ncABP}}(f, \vec{r})$. We will also denote M_i as the $r_{i-1} \times r_i$

matrix where the (u, v)-th entry is the (formal) linear form $\sum_{j\in[n]} M_{i,x_j}[u, v]x_j$. Note that here, $M_{i,x_j}[u, v]$ is a variable of the polynomial equation system $\mathsf{lb}_{\mathrm{ncABP}}(f, \vec{r})$ and x_j is a formal variable of f.

(Equations) For every degree-d non-commutative monomial $m \in X^d$, $\mathsf{lb}_{\mathrm{ncABP}}(f, \vec{r})$ contains a degree-d equation stating that the m-th coefficient of f is equal to the m-th coefficient of f', where f' is the non-commutative polynomial computed by the ABP. Suppose that $m = x_{j_1}x_{j_2}\dots x_{j_d}$, then this equation can be written as

$$\prod_{i=1}^{d} M_{i,x_{j_i}} - \mathsf{coeff}[f, m] = 0.$$

(Note that $\prod_{i=1}^{d} M_{i,x_{j_i}}$ is a 1×1 matrix over $\mathbb{F}$, i.e., a scalar in $\mathbb{F}$.)

Theorem 8.2. *Let f be any non-commutative homogeneous polynomial of degree d over the variable set $X = \{x_1, x_2, \dots, x_n\}$ and let $N = n^d$. Let $r \in \mathbb{N}$ and denote $\vec{r} = (1, \underbrace{r, r, \dots, r}_{(d-1)\ r\text{'s}}, 1)$.*

Then there is a degree-2 reduction from Rank_r^N to $\mathsf{lb}_{\mathrm{ncABP}}(f, \vec{r})$.

Proof. Identify $[N]$ with X^d, i.e., the set of non-commutative degree-d monomials over X. Consider what we call the *brute-force ncABP* computing f: this is a ncABP consisting of $d+1$ layers, with each internal layer of width N. The ncABP consists of N disjoint (with respect to nodes, except for the source and sink nodes) paths, where each such path from the root to the sink computes a single non-commutative monomial. More precisely, we can describe the brute-force ncABP in terms of matrices whose entries are linear forms over X as follows:

- For every $m \in X^d$, let $M_1^{\mathsf{bf}}[1, m] = \mathsf{coeff}[f, m]x_1$ where x_1 is the first variable in m.
- For every $2 \le i < d$ and every $m \in X^d$, let $M_i^{\mathsf{bf}}[m, m] = x_i$ where x_i is the i-th variable in m; for every $m, m' \in X^d$ with $m \neq m'$, let $M_i^{\mathsf{bf}}[m, m'] = 0$.
- For every $m \in X^d$, let $M_d^{\mathsf{bf}}[m, 1] = x_d$ where x_d is the d-th variable in m.

Let $X \in \mathbb{F}^{N\times r}$ and $Y \in \mathbb{F}^{r\times N}$ be the variables of Rank_r^N and $(M_1, M_2, \dots, M_d)$ be the variables of $\mathsf{lb}_{\mathrm{ncABP}}(f, \vec{r})$. Consider the following degree-2 mapping R that maps (X, Y) into:

- $M_1 = M_1^{\mathsf{bf}} \cdot X$, $M_d = Y \cdot M_d^{\mathsf{bf}}$;
  (What this actually means is that $M_{1,x_j} = M_{1,x_j}^{\mathsf{bf}} \cdot X$ and $M_{d,x_j} = Y \cdot M_{d,x_j}^{\mathsf{bf}}$ for every $x_j \in X$.)
- $M_i = Y \cdot M_i^{\mathsf{bf}} \cdot X$ for every $2 \le i < d$.
  (Similarly, what this actually means is that $M_{i,x_j} = Y \cdot M_{i,x_j}^{\mathsf{bf}} \cdot X$ for every $x_j \in X$.)

We prove this is a valid reduction from Rank_r^N to $\mathsf{lb}_{\mathrm{ncABP}}(f, \vec{r})$. Towards this end fix any monomial $m = x_{j_1}x_{j_2}\dots x_{j_d} \in X^d$ and consider the polynomial corresponding to m:

$$p_m = \prod_{i=1}^{d} M_{i,x_{j_i}} - \mathsf{coeff}[f, m].$$

Then, $p_m \circ R$ is the following polynomial over (X, Y):

$$p_m \circ R = M_{1,x_1}^{\mathsf{bf}}(XY)M_{2,x_2}^{\mathsf{bf}}(XY)M_{3,x_3}^{\mathsf{bf}}\dots M_{d-1,x_{d-1}}^{\mathsf{bf}}(XY)M_{d,x_d}^{\mathsf{bf}} - \mathsf{coeff}[f, m].$$

On the other hand, the following is immediate from the definitions of M_i^{bf}:

$$M_{1,x_1}^{\mathsf{bf}}M_{2,x_2}^{\mathsf{bf}}M_{3,x_3}^{\mathsf{bf}}\dots M_{d-1,x_{d-1}}^{\mathsf{bf}}M_{d,x_d}^{\mathsf{bf}} - \mathsf{coeff}[f, m] = 0.$$

Now we have the following telescoping sum:

$$\begin{aligned} p_m \circ R = {} & M^{\mathsf{bf}}_{1,x_1} M^{\mathsf{bf}}_{2,x_2} \dots M^{\mathsf{bf}}_{d,x_d} - \mathsf{coeff}[f,m] \\ & + M^{\mathsf{bf}}_{1,x_1}(XY-I) M^{\mathsf{bf}}_{2,x_2} \dots M^{\mathsf{bf}}_{d,x_d} \\ & + M^{\mathsf{bf}}_{1,x_1}(XY) M^{\mathsf{bf}}_{2,x_2}(XY-I) M^{\mathsf{bf}}_{3,x_3} \dots M^{\mathsf{bf}}_{d,x_d} \\ & + \dots \\ & + M^{\mathsf{bf}}_{1,x_1}(XY) M^{\mathsf{bf}}_{2,x_2}(XY) M^{\mathsf{bf}}_{3,x_3} \dots (XY-I) M^{\mathsf{bf}}_{d,x_d} \\ = {} & \sum_{i=1}^{d-1} \mathsf{Prefix}_i (XY-I) \mathsf{Suffix}_{i+1}, \end{aligned} \tag{33}$$

where $\mathsf{Prefix}_i = M^{\mathsf{bf}}_{1,x_1}(XY) M^{\mathsf{bf}}_{2,x_2}(XY) \dots (XY) M^{\mathsf{bf}}_{i,x_i}$ and $\mathsf{Suffix}_i = M^{\mathsf{bf}}_{i,x_i} M^{\mathsf{bf}}_{i+1,x_{i+1}} \dots M^{\mathsf{bf}}_{d,x_d}$. It is easy to see that (33) is of the form $\sum_{u,v\in[N]} \mathsf{axiom}_{u,v} p_{u,v}$, where $\mathsf{axiom}_{u,v}$ is the (u,v)-th entry of $(XY-I)$, and each $p_{u,v}$ is a polynomial over (X,Y) of degree at most $2d-2$. □

As a corollary, there is a degree-$O(\log(n^d/r))$ reduction from Rank^{2r}_r to $\mathsf{lb}_{\mathrm{ncABP}}(f,\vec{r})$.

8.2 Boolean Circuit Lower Bounds

We show that there is a degree-$O(n)$ algebraic reduction from polynomial equations expressing ncABP lower bounds to polynomial equations expressing Boolean circuit lower bounds. This implies that for every proof system $\mathcal{P}$ closed under low-degree algebraic reductions, if $\mathcal{P}$ cannot prove the weak rank principle, then it also cannot prove circuit lower bounds for any Boolean function. (Note that in our formalisation, the circuit lower bound statement has size $2^{O(n)}$, hence a reduction of degree $O(n)$ can be seen as *low degree*.)

Let $f : \{0,1\}^n \to \{0,1\}$ denote a Boolean function (represented by its length-2^n truth table), $s \in \mathbb{N}$, and $\mathsf{lb}(f,s)$ denote the polynomial equation system expressing that the circuit complexity of f is greater than s.

Theorem 8.3. *For every $f : \{0,1\}^n \to \{0,1\}$, there is a non-commutative polynomial $p_f : \mathbb{F}^2 \to \mathbb{F}$ of degree n such that for every parameter r, if we let $\vec{r} = (1, \underbrace{r, r, \dots, r}_{(n-1)\ r\text{'s}}, 1)$, then*

$$\mathsf{lb}_{\mathrm{ncABP}}(p_f, \vec{r}) \leq^{O(n)}_{\mathrm{alg}} \mathsf{lb}(f,s) \text{ where } s = O(nr^2).$$

Formalisation of $\mathsf{lb}(f,s)$. We now recall the precise definition of $\mathsf{lb}(f,s)$ from [69, 72, 73].

First, we list all variables of $\mathsf{lb}(f,s)$ along with their intended meaning. (In what follows, $a \in \{0,1\}^n$ represents the input of the circuit, $v, v' \in [s]$ represent gates of the circuit, $v' < v$, $b \in \{1,2\}$, and $i \in [n]$ represents a variable.)

Name	Intended Meaning
y_{av}	The Boolean value computed at the computational node v on the input a
y_{abv}	The value on a brought to v by the b-th input to v
$\mathrm{Fanin}(v)$	This is 0 if v is a NOT gate and 1 if v is an AND gate or an OR gate
$\mathrm{Type}(v)$	When $\mathrm{Fanin}(v) = 1$, this is 0 if v is an AND gate and 1 if v is an OR gate
$\mathrm{InputType}_b(v)$	This is 0 if the b-th input to v is a constant or a variable and 1 if it is one of the previous computational gates
$\mathrm{InputType}'_b(v)$	When $\mathrm{InputType}_b(v) = 0$, this is 0 if the b-th input to v is a constant, and is 1 if it is a variable
$\mathrm{InputType}''_b(v)$	When $\mathrm{InputType}_b(v) = \mathrm{InputType}'_b(v) = 0$, this equals the b-th input to v

$\text{InputVar}_b(v,i)$	When $\text{InputType}_b(v)=0$ and $\text{InputType}'_b(v)=1$, this is 1 if and only if the b-th input to v is the i-th variable
$\text{INPUTVAR}_b(v,i)$	Equals $\bigvee_{i'\le i}\text{InputVar}_b(v,i')$, introduced to keep bottom fan-in bounded
$\text{InputNode}_b(v,v')$	When $\text{InputType}_b(v)=1$, this is 1 if and only if the b-th input to v is the previous gate v'
$\text{INPUTNODE}_b(v,v')$	Analogous to $\text{INPUTVAR}_b(v,i)$ (i.e., equals $\bigvee_{v''<v'}\text{InputNode}_b(v,v'')$).

Table 1: Variables of $\mathsf{Ib}(f,s)$

Then, $\mathsf{Ib}(f,s)$ consists of the following clauses (we can translate them into low-degree polynomials in the standard way):

(Group 1) If the b-th input of v is a constant, then this constant is equal to y_{abv}:

- $\neg\text{InputType}_b(v)\wedge\neg\text{InputType}'_b(v)\to(y_{abv}=\text{InputType}''_b(v))$;

(Group 2) If the b-th input of v is a variable, then there is a unique i such that it is the i-th variable:

- $\neg\text{InputType}_b(v)\wedge\text{InputType}'_b(v)\to\neg(\text{InputVar}_b(v,i)\wedge\text{InputVar}_b(v,i'))$ where $i\neq i'$;
- $\neg\text{InputType}_b(v)\wedge\text{InputType}'_b(v)\to(\text{INPUTVAR}_b(v,i)=\text{INPUTVAR}_b(v,i-1)\vee\text{InputVar}_b(v,i))$ where we define $\text{INPUTVAR}_b(v,0)=0$;
- $\neg\text{InputType}_b(v)\wedge\text{InputType}'_b(v)\to\text{INPUTVAR}_b(v,n)$;
- $\neg\text{InputType}_b(v)\wedge\text{InputType}'_b(v)\wedge\text{InputVar}_b(v,i)\to y_{abv}=a_i$;

(Group 3) If the b-th input of v is a previous gate, then there is a unique $v'<v$ such that it is the v'-th gate:

- $\text{InputType}_b(v)\to\neg(\text{InputNode}_b(v,v')\wedge\text{InputNode}_b(v,v''))$ where $v'\neq v''$;
- $\text{InputType}_b(v)\to(\text{INPUTNODE}_b(v,v')=\text{INPUTNODE}_b(v,v'-1)\vee\text{InputNode}_b(v,v'))$ where we define $\text{INPUTNODE}_b(v,0)=0$;
- $\text{InputType}_b(v)\to\text{INPUTNODE}_b(v,v-1)$;
- $\text{InputType}_b(v)\wedge\text{InputNode}_b(v,v')\to y_{abv}=y_{av'}$;

(Group 4) Every gate operates as expected:

- $\neg\text{Fanin}(v)\to(y_{av}=\neg y_{a1v})$;
- $\text{Fanin}(v)\wedge\neg\text{Type}(v)\to(y_{av}=y_{a1v}\wedge y_{a2v})$;
- $\text{Fanin}(v)\wedge\text{Type}(v)\to(y_{av}=y_{a1v}\vee y_{a2v})$;

(Group 5) The circuit computes f:

- $y_{as}=f(a)$.

The reduction. We first provide an outline of the reduction. Given any Boolean function $f:\{0,1\}^n\to\{0,1\}$, let $p_f:\mathbb{F}^2\to\mathbb{F}$ be the degree-n non-commutative polynomial over the variables z_0,z_1 such that:

- For every $x\in\{0,1\}^n$, the coefficient of the monomial $z_{x_1}z_{x_2}\dots z_{x_n}$ is equal to $f(x)$. (Here we treat $f(x)\in\{0,1\}$ as an element in $\mathbb{F}$.)

Suppose that p_f can be computed by a small ncABP P. For every degree-n non-commutative monomial m, let $\mathsf{Coeff}(P, m)$ denote the coefficient of m in the non-commutative polynomial computed by P (this non-commutative polynomial should be equal to p_f). Then Coeff can be computed by a small Boolean circuit. Plugging P into Coeff gives us a small circuit for f.

In more details, let $\vec{r} = (r_0, r_1, \ldots, r_n)$ where $r_0 = r_d = 1$ and $r_i = r$ for every $1 \leq i < d$. Let $M_1, \ldots, M_n$ denote the matrices representing the ncABP P, where each M_i is of dimension $r_{i-1} \times r_i$. Note that each entry of each M_i is a linear form over (the non-commutative variables) z_0 and z_1, hence we can write $M_i = M_{i,z_0} z_0 + M_{i,z_1} z_1$ where each $M_{i,z_b} \in \mathbb{F}^{r_{i-1} \times r_i}$. Every $x \in \{0,1\}^n$ corresponds to the non-commutative monomial $m_x = z_{x_1} z_{x_2} \ldots z_{x_n}$, and the coefficient of m_x is

$$\prod_{i=1}^{n} M_{i,z_{x_i}}. \tag{34}$$

Let $\mathsf{Coeff}(\{M_{i,z_b}\}, x)$ denote the circuit that given $\{M_{i,z_b}\}$ and x as inputs, outputs the value of (34). The size of Coeff is at most $s = O(nr^2)$. Moreover, it is possible to design a circuit implementation of Coeff such that for every internal gate g and every $x \in \{0,1\}^n$, there is an $\mathbb{F}$-polynomial $q_{g,x}$ of degree $O(n)$ over the inputs $\{M_{i,z_b}\}$ that computes the value of g.

Now we are ready to specify the reduction from $\mathsf{lb}_{\mathrm{ncABP}}(p_f, \vec{r})$ to $\mathsf{lb}(f, s)$, where $s = O(nr^2)$. Let $\{M_{i,z_b}\}$ be the inputs of $\mathsf{lb}_{\mathrm{ncABP}}(p_f, \vec{r})$. Consider the circuit $C(x) = \mathsf{Coeff}(\{M_{i,z_b}\}, x)$ that takes $x \in \{0,1\}^n$ as an input. The variables

$$\begin{aligned} &\mathrm{Fanin}(v), \mathrm{Type}(v), \mathrm{InputType}_b(v), \mathrm{InputType}'_b(v), \\ &\mathrm{InputVar}_b(v,i), \mathrm{INPUTVAR}_b(v,i), \mathrm{InputNode}_b(v,v'), \mathrm{INPUTNODE}_b(v,v') \end{aligned} \tag{35}$$

are fixed constants that reflect the wiring of C. Note that the circuit Coeff takes $\{M_{i,z_b}\}$ as inputs, but the circuit C treats $\{M_{i,z_b}\}$ as hardwired constants. Therefore, some variables of the form $\mathrm{InputType}''_b(v)$ are projections over $\{M_{i,z_b}\}$. Finally, the variables y_{av} and y_{abv} are internal values on the computation $C(a)$; all of them can be computed by a degree-$O(n)$ polynomial over $\{M_{i,z_b}\}$ (i.e., $q_{g,a}$ for the corresponding gate g).

Next we verify that every clause in $\mathsf{lb}(f, s)$ (composed with our reduction) admits a degree-$O(n)$ NS-proof from $\mathsf{lb}_{\mathrm{ncABP}}(p_f, \vec{r})$. In fact this essentially follows from definition:

- (Group 1) is true since we assign both y_{abv} and $\mathrm{InputType}''_b(v)$ the same projection over $\{M_{i,z_b}\}$.
- (Group 2) and (Group 3) only contains variables in (35) (which are constants under our reduction). They assert that the circuit has a valid structure; since our circuit C indeed has a valid structure, they are trivially true.

  The only two exceptions are

  $$\begin{aligned} \neg\mathrm{InputType}_b(v) \wedge \mathrm{InputType}'_b(v) \wedge \mathrm{InputVar}_b(v,i) &\to y_{abv} = a_i; \text{ and} \\ \mathrm{InputType}_b(v) \wedge \mathrm{InputNode}_b(v,v') &\to y_{abv} = y_{av'}. \end{aligned}$$

  as they contain not only variables in (35) but also variables of the form y_{abv} and $y_{av'}$. But they are also trivially true by our definitions of y_{abv} and $y_{av'}$.
- (Group 4) is true because the polynomials $q_{g,x}$ correctly captures the values being computed at the gate g on input x.
- (Group 5) asserts that $y_{as} = f(a)$. This is exactly the a-th axiom in $\mathsf{lb}_{\mathrm{ncABP}}(p_f, \vec{r})$ and hence trivially admits a degree-$O(n)$ NS-proof from $\mathsf{lb}_{\mathrm{ncABP}}(p_f, \vec{r})$.

Corollary 8.4. *For every $f : \{0,1\}^n \to \{0,1\}$ and every parameter r, if the circuit complexity of f is greater than $s = O(nr^2)$, then there is a degree-$O(n^2)$ algebraic reduction from Rank_r^{2r} to $\mathsf{lb}(f, s)$.*

Proof. Let $\vec{r} = (1, \underbrace{r, r, \ldots, r}_{(n-1)\ r\text{'s}}, 1)$ and $p_f : \mathbb{F}^2 \to \mathbb{F}$ be the non-commutative polynomial guaranteed by Theorem 8.3, then there is a degree-$O(n)$ reduction from $\mathsf{lb}_{\mathrm{ncABP}}(p_f, \vec{r})$ to $\mathsf{lb}(f, s)$. By Theorem 8.2, there is a degree-2 reduction from $\mathsf{Rank}_r^{2^n}$ to $\mathsf{lb}_{\mathrm{ncABP}}(p_f, \vec{r})$. By Theorem 7.2, there is a degree-$O(n)$ reduction from Rank_r^{2r} to $\mathsf{Rank}_r^{2^n}$. Composing these three reductions (via Fact 4.7) gives us a degree-$O(n^2)$ reduction from Rank_r^{2r} to $\mathsf{lb}(f, s)$. □

Remark 8.5. The circuit for Coeff can be computed in NC^2 (since it computes an iterated matrix multiplication over $\mathbb{F}$). Hence, the above argument also gives a reduction from the weak rank principle to sentences expressing NC^2 circuit lower bounds. In particular, let $\mathsf{lb}_{\mathsf{NC}^2}(f, s)$ denote the collection of polynomial equations encoding that f cannot be computed by a circuit of size s and depth $\log^2 s$ (we do not attempt to formally define $\mathsf{lb}_{\mathsf{NC}^2}(f, s)$ here). The same argument above shows that for every Boolean function f and every parameter r, letting $s = \mathrm{poly}(n, r)$, there is a degree-$O(n^2)$ algebraic reduction from Rank_r^{2r} to $\mathsf{lb}_{\mathsf{NC}^2}(f, s)$. Hence, if the rank principle is hard for some proof system $\mathcal{P}$ (that is closed under low-degree reductions), then $\mathcal{P}$ cannot prove any lower bound against NC^2 circuits as well.

8.3 Lower Bounds for $\mathsf{PCR}_{\mathbb{F}_2}$

We show how to apply iterability to obtain $\mathsf{PCR}_{\mathbb{F}_2}$ size lower bounds on $\mathsf{lb}_{\mathrm{ncABP}}(f, \vec{r})$ and $\mathsf{lb}^{\oplus}(f, s)$ (a variant of $\mathsf{lb}(f, s)$ that allows binary $\oplus$ gates).

8.3.1 Lower Bounds for Non-commutative ABPs

Definition 8.6. Let f be any non-commutative homogeneous polynomial of degree d over the variable set $Z = \{z_1, z_2, \ldots, z_n\}$. Let $\vec{r} = (r_0, r_1, \ldots, r_d)$ with $r_0 = r_d = 1$. For every $\Delta \in [d]$ and $j \in [n]$, let M_{Δ, z_j} be a variable matrix of dimension $r_{\Delta-1} \times r_\Delta$. Let $\mathcal{M}_\Delta$ be the set of all degree-Δ non-commutative monomial in $z_1, \ldots, z_n$. For every $\Delta \in [d]$ and $m \in \mathcal{M}_\Delta$, let $P_{\Delta, m}$ be an $r_{\Delta-1} \times r_\Delta$ variable matrix.

In this section, we assume that $\mathsf{lb}_{\mathrm{ncABP}}(f, \vec{r})$ is the following polynomial system:

$$\begin{aligned}
&P_{1,z_j} = M_{1,z_j} && j \in [n],\\
&P_{\Delta, mz_j} = P_{\Delta-1,m} M_{\Delta,z_j} && j \in [n], \Delta \in \{2, \ldots, d\}, m \in \mathcal{M}_{\Delta-1},\\
&P_{d,m} = \mathsf{coeff}(f, m) && m \in \mathcal{M}_d.
\end{aligned}$$

Assuming the formula $\mathsf{IRank}_n^m(\mathbf{A}, \kappa)$ is satisfiable, we will show how to construct a polynomial-size ncABP circuit for any non-commutative polynomial.

Theorem 8.7. *Let f be any non-commutative homogeneous polynomial of degree d over the variable set $Z = \{z_1, z_2, \ldots, z_n\}$. Let $r > 0$ and denote $\vec{r} = (1, \underbrace{r, r, \ldots, r}_{(d-1)\ r\text{'s}}, 1)$.*

Then any $\mathsf{PCR}_{\mathbb{F}_2}$ refutation of $\mathsf{lb}_{\mathrm{ncABP}}(f, \vec{r})$ requires size $2^{\Omega(\sqrt{r/d})}$.

Proof. We will reduce $\mathsf{lb}_{\mathrm{ncABP}}(f, \vec{r})$ to $\mathsf{IRank}_r^{nr}(\mathbf{A}, d, [n])$ for some particular $\mathbf{A}$. Let Π be a $\mathsf{PCR}_{\mathbb{F}_2}$ refutation of $\mathsf{lb}_{\mathrm{ncABP}}(f, \vec{r})$.

Let A_1 and A_0 be $nr \times nr$ matrices defined as:

$$A_1 = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix} \text{ and } A_0 = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}.$$

The main property of these matrices is that for every $b \in \{0, 1\}$, $(A_b)_{1,1} = b$.

For every $\pi \in [n]^d$, define $A^{(\pi)} = A_{\mathsf{coeff}(f, \prod_{j \in \pi} z_j)}$. For every $\pi \in [n]^{<d}$, define $A^{(\pi)}$ as an $nr \times nr$ block matrix

$$A^{(\pi)} = \begin{bmatrix} X^{(\pi*1)} & X^{(\pi*2)} & \cdots & X^{(\pi*n)} \end{bmatrix}.$$

Let $\mathbf{A} = \{A^{(\pi)} : \pi \in [n]^d\}$.

Also let Y be split into n consequent blocks of dimension $r \times r$:

$$Y = \begin{bmatrix} Y_1 & Y_2 & \cdots & Y_n \end{bmatrix}$$

Now define the reduction τ as follows.

$$\begin{aligned} \tau(P_{\Delta,m}) &= X^{(j_1,\ldots,j_\Delta)} && \Delta \in [d], m = z_{j_1} \cdots z_{j_\Delta} \in \mathcal{M}_\Delta, \\ \tau(M^{1,z_j}) &= X^{(j)} && j \in [n], \\ \tau(M^{\Delta,z_j}) &= Y_j && \Delta \in \{2,\ldots,d\}, j \in [n]. \end{aligned}$$

Every axiom of $\mathsf{lb}_{\mathrm{ncABP}}(f, \vec{r}) \upharpoonright \tau$ is either satisfied or becomes an axiom of $\mathsf{IRank}_r^{nr}(\mathbf{A}, d, [n])$, and $\Pi \upharpoonright \tau$ is a refutation of $\mathsf{IRank}_r^{nr}(\mathbf{A}, d, [n])$. By Theorem 5.43, it implies that the size of Π is $2^{\Omega(\sqrt{r/n})}$. □

Observe that the size of $\mathsf{lb}_{\mathrm{ncABP}}(f, \vec{r})$ is polynomial in $n^d dr^2$, thus the bound becomes non-trivial when $r = \omega(d \log^2 n)$.

8.3.2 Lower Bounds for Boolean Circuits

Similarly to [73], we consider Boolean circuits in the basis $\neg, \wedge, \vee, \oplus$, where the last three connectives are binary.

Definition 8.8 (Formula $\mathsf{lb}^{\oplus}(f,s)$)**.** Let $n, s > 0$ and $f\colon \{0,1\}^n \to \{0,1\}$. The formula $\mathsf{lb}^{\oplus}(f,s)$ is defined similarly to $\mathsf{lb}(f,s)$ except that it also allows binary $\oplus$ connectives.

We show that if, for a particular choice of parameters, the formula $\psi_{P(H(G))}(\mathbf{A}, \kappa)$ is satisfiable, we can construct a polynomial-size circuit for any Boolean function.

Theorem 8.9. *There exists $\delta > 0$ such that for every sufficiently large n and every function $f\colon \{0,1\}^n \to \{0,1\}$, if $s \geq n^5$, then any $\mathsf{PCR}_{\mathbb{F}_2}$ refutation of $\mathsf{lb}^{\oplus}(f,s)$ requires size $2^{\Omega((s^{\delta/5}/n)^{1/3})}$.*

Proof. Let $r = s^{1/5} \geq n$. Let $\delta, d > 0$ from Lemma 4.15 such that there exists an $(16r) \times ((r-10)/8)$ $(((r-10)/8)^{\delta}, d)$-lossless expander G with the appropriate degree bounds.

We will reduce $\mathsf{lb}^{\oplus}(f,s)$ to $\psi_{P(H(G))}(\mathbf{A}, n)$ for some particular $\mathbf{A}$. Let Π be a $\mathsf{PCR}_{\mathbb{F}_2}$ refutation of $\mathsf{lb}^{\oplus}(f,s)$.

Let A_1 and A_0 be $16r \times 16r$ matrices defined as:

$$A_1 = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix} \text{ and } A_0 = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}.$$

For every $\pi \in \{0,1\}^n$, define $A^{(\pi)} = A_{f(\pi)}$. For every $\pi \in \{0,1\}^{<n}$, define $A^{(\pi)}$ as a $16r \times 16r$ block matrix

$$A^{(\pi)} = \begin{bmatrix} X^{(\pi*0)} & X^{(\pi*1)} & Y^{(\pi*0)^T} & Y^{(\pi*1)^T} \end{bmatrix}.$$

We construct the circuit $\mathcal{C}(v_1, \ldots, v_n)$ that computes f, provided that $\psi_{P(H(G))}(\mathbf{A}, n)$ is satisfied. The circuit uses gates that correspond to the extension variables of $\psi_{P(H(G))}(\mathbf{A}, n)$.

1. For every $\mu \in [4]$, $i \in [16r]$, $k \in [r]$:
$$g_x[0, \mu, i, k] = x_{i,k}^{((),\mu)}.$$
2. For every $\ell \in [n]$, $\mu \in [4]$, $i \in [16r]$, $k \in [r]$:
$$g_x[\ell, \mu, i, k] = (v_\ell \wedge g_w[\ell - 1, i, (\mu - 1)r + k, 0]) \vee (\neg v_\ell \wedge g_w[\ell - 1, i, (\mu - 1)r + k + 4r, 0]).$$
3. For every $\mu \in [4]$, $j \in [16r]$, $k \in \mathcal{N}_H(j)$:
$$g_y[0, \mu, k, j] = y_{k,j}^{((),\mu)}.$$
4. For every $\ell \in [n]$, $\mu \in [4]$, $i \in [16r]$, $k \in \mathcal{N}_H(j)$:
$$g_y[\ell, \mu, k, i] = (v_\ell \wedge g_w[\ell - 1, i, (\mu - 1)r + k + 8r, 0]) \vee (\neg v_\ell \wedge g_w[\ell - 1, i, (\mu - 1)r + k + 12r, 0]).$$
5. For every $\ell \in \{0, \ldots, n\}$, $\mu \in [4]$, $i, j \in [16r]$, $k \in \mathcal{N}_H(j)$:
$$g_z[\ell, \mu, i, j, k] = g_x[\ell, \mu, i, k] \wedge g_y[\ell, \mu, k, j].$$
6. For every $\ell \in \{0, \ldots, n\}$, $\mu \in [4]$, $i, j \in [16r]$:
$$g_u[\ell, \mu, i, j, (1)] = g_z[\ell, \mu, i, j, 1].$$
7. For every $\ell \in \{0, \ldots, n\}$, $\mu \in [4]$, $i, j \in [16r]$ and every initial segment $\Sigma \cup (k)$ of $\mathcal{N}_H(j)$ with $\Sigma \neq \varnothing$:
$$g_u[\ell, \mu, i, j, \Sigma \cup (k)] = g_u[\ell, \mu, i, j, \Sigma] \oplus g_z[\ell, \mu, i, j, k].$$
8. For every $\ell \in \{0, \ldots, n\}$, $i, j \in [16r]$:
$$\begin{aligned} g_w[\ell, i, j, 1] &= g_u[\ell, 1, i, j, \mathcal{N}_H(j)] \oplus g_u[\ell, 2, i, j, \mathcal{N}_H(j)], \\ g_w[\ell, i, j, 2] &= g_u[\ell, 3, i, j, \mathcal{N}_H(j)] \oplus g_u[\ell, 4, i, j, \mathcal{N}_H(j)], \\ g_w[\ell, i, j, 0] &= g_w[\ell, i, j, 1] \oplus g_w[\ell, i, j, 2]. \end{aligned}$$

The output of the circuit is $g_w[n, 1, 1, 0]$. The size of the circuit is $O(nr^3)$, which is less than s for large enough n. It follows from the construction that for every $\pi \in \{0,1\}^n$, $C(\pi) = A^{(\pi)}{}_{1,1} = f(\pi)$.

We plug $\mathcal{C}(v_1, \ldots, v_n)$ into $\mathsf{Ib}^{\oplus}(f, s)$. It is not hard to verify that, as a result, we obtain a polynomial system that can be easily derived from $\psi_{P(H(G))}(\mathbf{A}, n)$. By Theorem 5.67, it implies that $\mathsf{Ib}^{\oplus}(f, s)$ requires a refutation of size $2^{\Omega((r/n)^{1/3})} = 2^{\Omega((s^{\delta/5}/n)^{1/3})}$. □

Observe that the size of $\mathsf{Ib}^{\oplus}(f, s)$ is polynomial in 2^n, thus the bound becomes non-trivial when $s = \omega(n^{20/\delta})$.

9 Proving Circuit Lower Bounds via the Weak Rank Principle

We show that the weak rank principle is capable of proving lower bounds against $\mathsf{AC}^0[p]$ circuits by formalising Smolensky's lower bound [75].

Roadmap of Section 9. Smolensky's proof consists of two parts: a correlation bound against low-degree polynomials (i.e., any low-degree polynomial over $\mathbb{F}_p$ has to make many errors when computing $\prod_{i=1}^n x_i$) and the "polynomial method" (i.e., every small $\mathsf{AC}^0[p]$ circuit is well-approximated by a low-degree polynomial over $\mathbb{F}_p$). Hence we arrange this section as follows:

- Section 9.1 provides an exposition of Smolensky's proof. The exposition is equivalent to the original proof, but it will be presented in a way that only involves simple manipulations computable in $\mathsf{AC}^0[p]$ and the weak rank principles.

  In Section 9.1.1 we prove the correlation bound against low-degree $\mathbb{F}_p$-polynomials. This is the main step where the weak rank principle is involved. In Section 9.1.2 we show that small $\mathsf{AC}^0[p]$ circuits can be approximated by low-degree $\mathbb{F}_p$ polynomials, and put everything together to finish the circuit lower bound.

- In Section 9.2 we formalise the lower bound in $\overline{\mathbf{V}^0(p)} + \mathrm{WRank}_p$.

  We start with a description of the relevant theories ($\overline{\mathbf{V}^0(p)}$ and $\overline{\mathbf{V}^0(p)} + \mathrm{WRank}_p$) in Section 9.2.1. The main formalisation will appear in Section 9.2.2. Finally, Section 9.2.3 contains a postponed proof of a technical theorem related to error-correcting codes.

It is recommended to read Section 9.1 before delving into Section 9.2 for the following reasons. First, to make the invocation of weak rank principles explicit, the proofs in Section 9.1 are presented in a somewhat different way than it is usually presented in textbooks (e.g., [8]); it would be beneficial to be familiarised with the proof before formalising it. Second, Section 9.1 contains important definitions (such as the matrices on which the weak rank principle is invoked) that the formalisation in Section 9.2 needs to reason about.

9.1 Smolensky's Lower Bound

9.1.1 Correlation Bound Against Low-Degree Polynomials

We need the following correlation bound against low-degree polynomials.

Theorem 9.1. *Let $P : \mathbb{F}_p^n \to \mathbb{F}_p$ be a polynomial of degree at most $0.1\sqrt{n}$. Let $S = \{x \in \{-1,1\}^n : P(x) = \prod_{i=1}^n x_i\}$, then $|S| \leq 0.99 \cdot 2^n$.*

Proof Ideas. The idea is that every function $f : S \to \mathbb{F}_p$ is equivalent to a polynomial of degree at most $d = n/2 + 0.1\sqrt{n}$ over S. In fact, let $T \subseteq [n]$ and $m = \prod_{i \in T} x_i$ be a multilinear monomial. If $|T| = \deg(m) \leq n/2$, then m is trivially equivalent to a polynomial of degree at most d (i.e., m itself). If $|T| = \deg(m) > n/2$, then the equality

$$m \equiv \left(\prod_{i \in [n] \setminus T} x_i \right) \cdot P(x) \tag{36}$$

still holds over S, and the RHS of (36) is a polynomial of degree at most d. Hence every multilinear monomial m is equivalent to a polynomial of degree at most d over S. Since $S \subseteq \{-1,1\}^n$, every function $f : S \to \mathbb{F}_p$ can be written as a linear combination of multilinear monomials, hence is also equivalent to a polynomial of degree at most d.

Given this, it follows that there are at most

$$p^{\sum_{i=0}^{d} \binom{n}{i}} \leq p^{0.99 \cdot 2^n}$$

different functions $f : S \to \mathbb{F}_p$, indicating that $|S| \leq 0.99 \cdot 2^n$. □

To aid our formalisations later, we need to explicitly construct the matrices over which the weak rank principle is used (instead of using concepts such as *dimensions of vector spaces*). We now rephrase the above proof so that the invocation of the weak rank principle becomes clear.

Theorem 9.2. *Let $S \subseteq \{-1,1\}^n$, $|S| \geq 0.999 \cdot 2^n$, $P : S \to \mathbb{F}_p$ be any polynomial of degree at most $0.1\sqrt{n}$. Then there exists some $z \in S$ such that $P(z) \neq \prod_{i=1}^n z_i$.*

Proof. Given $S \subseteq \{-1,1\}^n$, we construct the following matrices $A \in \mathbb{F}_p^{|S| \times r}$ and $B \in \mathbb{F}_p^{r \times |S|}$ where $r = 0.99 \cdot 2^n$. We identify $[r]$ (i.e., columns of A and rows of B) with monomials m of degree at most $d = n/2 + 0.1\sqrt{n}$. Now, for an input $x \in S$ and a monomial $m \in [r]$:

- Define $A[x, m] = m(x)$ to be the value of m on input x. Note that A can be seen as a linear mapping for *polynomial evaluation*: Let $\vec{e} \in \mathbb{F}_p^r$ and think of $\vec{e}$ as the coefficient list of a polynomial P with degree at most d. (That is, for every monomial m of degree at most d, $\vec{e}_m$ is the coefficient of m in P.) Then $A\vec{e} \in \mathbb{F}_p^S$ is exactly the list of values of P over S.
- Define $B[m, x]$ to be the sum of the following values:
  1. if $\deg(m) \le n/2$, we add $(\frac{p+1}{2})^n m(x)$ to $B[m, x]$;
  2. for every monomial m' that appears in P with coefficient $\alpha_{m'}$, if the degree of $\tilde{m} = m' \cdot m \cdot \prod_{i\in[n]} x_i$ is greater than $n/2$, we add $(\frac{p+1}{2})^n \cdot \alpha_{m'} \cdot \tilde{m}(x)$ to $B[m, x]$.

The intended meaning of B is the following. It was shown in Theorem 9.1 that every function $f : S \to \mathbb{F}_p$ is equivalent to a polynomial of degree at most $d = n/2 + 0.1\sqrt{n}$. Let $\vec{v}_f \in \mathbb{F}_p^S$ be the vector representing the value list of f, then $B\vec{v}_f \in \mathbb{F}_p^r$ is exactly the coefficient list of this polynomial.

To be more precise, we introduce the following notation. Let $\mathcal{M}$ denote the set of all multilinear monomials on variables $z_1, \ldots, z_n$, $\mathcal{M}_{\le n/2}$ and $\mathcal{M}_{>n/2}$ denote the subset of monomials with degree $\le n/2$ and $> n/2$ respectively. Let $f : S \to \mathbb{F}_p$ be a function, then it can be expressed as the polynomial

$$f(z) = \sum_{m\in\mathcal{M}} \lambda_{f,m} m(z)$$

where $\lambda_{f,m} = (\frac{p+1}{2})^n \sum_{x\in S} f(x)m(x)$.

To see this, notice that

$$\begin{aligned}
\sum_{m\in\mathcal{M}} \lambda_{f,m} m(z) &= \sum_{m\in\mathcal{M}} \left(\frac{p+1}{2}\right)^n \sum_{x\in S} f(x)m(x)m(z) \\
&= \left(\frac{p+1}{2}\right)^n \sum_{x\in S} f(x) \sum_{m\in\mathcal{M}} m(x)m(z) \\
&= \left(\frac{p+1}{2}\right)^n \sum_{x\in S} f(x) \cdot \delta_{x,z} \cdot 2^n \\
&= f(z). && \text{(over } \mathbb{F}_p\text{)}
\end{aligned}$$

Given any function $f : S \to \mathbb{F}_p$, denote

$$f_{\mathsf{low}}(z) = \sum_{m\in\mathcal{M}_{\le n/2}} \lambda_{f,m} m(z) \quad \text{and} \quad f_{\mathsf{high}}(z) = \sum_{m\in\mathcal{M}_{>n/2}} \lambda_{f,m} m(z).$$

The following claim expresses the "intended meaning of B" mentioned above:

Claim 9.3. *Let $f : S \to \mathbb{F}_p$ be any function, $\vec{v}_f \in \mathbb{F}_p^S$ be the list of values of f on S, and $\hat{f}$ denote the polynomial whose coefficient list is $B \cdot \vec{v}_f$. Then for every $z \in S$,*

$$\hat{f}(z) = f_{\mathsf{low}}(z) + f_{\mathsf{high}}(z) \cdot P(z) \cdot \prod_{i=1}^{n} z_i.$$

Proof. We have that

$$\begin{aligned}
& f_{\mathsf{low}}(z) + f_{\mathsf{high}}(z) \cdot P(z) \cdot \prod_{i=1}^{n} z_i \\
= & \sum_{m\in\mathcal{M}_{\le n/2}} \lambda_{f,m} m(z) + \sum_{\tilde{m}\in\mathcal{M}_{>n/2}} \lambda_{f,\tilde{m}} \tilde{m}(z) P(z) \prod_{i=1}^{n} z_i
\end{aligned}$$

$$= (\frac{p+1}{2})^n \sum_{x \in S} \left(\underbrace{\sum_{m \in \mathcal{M}_{\leq n/2}} f(x)m(x)m(z)}_{\text{(Part I)}} + \underbrace{\sum_{\tilde{m} \in \mathcal{M}_{>n/2}} f(x)\tilde{m}(x)\tilde{m}(z)P(z) \prod_{i=1}^{n} z_i}_{\text{(Part II)}} \right). \tag{37}$$

Let $x \in S$, $m \in \mathcal{M}$, consider the coefficient of $f(x)m(z)$ in (37). If $\deg(m) \leq n/2$ then the contribution of (Part I) is $(\frac{p+1}{2})^n m(x)$; otherwise it is 0. For every monomial m' of P with coefficient $\alpha_{m'}$, if $\tilde{m} = m \cdot m' \cdot \prod_{i=1}^{n} z_i$ has degree $> n/2$, then it contributes to (Part II) a coefficient of $(\frac{p+1}{2})^n \tilde{m}(x)\alpha_{m'}$; otherwise it contributes nothing. It follows from the definition of B that

$$(37) = \sum_{x \in S} \sum_{m \in \mathcal{M}} B[m, x] f(x) m(z),$$

which by definition is equal to $\hat{f}(z)$. ◇

We also claim that any witness that $A \cdot B$ is not the identity matrix gives rise to a bad input on which P and $\prod_{i=1}^{n} z_i$ differ:

Claim 9.4. *If $z, x \in S$ and $(AB)[z, x] \neq \delta_{z,x}$, then $P(z) \neq \prod_{i=1}^{n} z_i$.*

Proof. Let $f : \{-1, 1\}^n \to \mathbb{F}_p$ be the function that evaluates to 1 on input x and evaluates to 0 on every input in $\{-1, 1\}^n \setminus \{x\}$; note that $\vec{1}_x$ is exactly the "value list" vector of f. By Claim 9.3, $B \cdot \vec{1}_x \in \mathbb{F}_p^r$ is the coefficient list of the polynomial $f'(z) = f_{\mathsf{low}}(z) + f_{\mathsf{high}}(z) \cdot P(z) \cdot \prod_{i=1}^{n} z_i$. Note that $f(z) = f_{\mathsf{low}}(z) + f_{\mathsf{high}}(z) = \delta_{z,x}$. However, $(AB)[z, x] = f'(z) \neq \delta_{z,x}$. This means that $P(z) \neq \prod_{i=1}^{n} z_i$. ◇

Since $|S| \geq 0.999 \cdot 2^n \gg r$, it follows from the weak rank principle that there exists $z, x \in S$ such that $(AB)[z, x] \neq \delta_{z,x}$. This implies that $P(z) \neq \prod_{i=1}^{n} z_i$ as shown by Claim 9.4. □

The matrices A and B in the above proof will be crucial for our formalisation, hence we reiterate their definitions here. (Note that A does not depend on the polynomial P but B does.)

Definition 9.5. Let $N = 2^n$, $r = 0.99 \cdot 2^n$, and $P : \{-1, 1\}^n \to \mathbb{F}_p$ be a polynomial of degree at most $0.1\sqrt{n}$. Identify $[N]$ with $\{-1, 1\}^n$ and $[r]$ with the set of monomials of degree at most $d = n/2 + 0.1\sqrt{n}$. Define:

- A to be the $N \times r$ matrix such that $A[x, m] = m(x)$ for every $x \in \{-1, 1\}^n$ and $m \in \mathcal{M}_{\leq d}$.
- $B(P)$ to be the $r \times N$ matrix such that for every $x \in \{-1, 1\}^n$ and $m \in \mathcal{M}_{\leq d}$, $B[m, x]$ is the sum of the following values. (1) If $\deg(m) \leq n/2$, we add $(\frac{p+1}{2})^n m(x)$ to $B[m, x]$; (2) for every monomial m' that appears in P with coefficient $\alpha_{m'}$, if the degree of $\tilde{m} = m' \cdot m \cdot \prod_{i \in [n]} x_i$ is greater than $n/2$, then we add $(\frac{p+1}{2})^n \cdot \alpha_{m'} \cdot \tilde{m}(x)$ to $B[m, x]$.

9.1.2 Approximating $\mathsf{AC}^0[p]$ Circuits by Low-Degree Polynomials

The next ingredient in the proof is the *low-degree* approximation of $\mathsf{AC}^0[p]$ circuits [67]: For every parameter Δ and every $\mathsf{AC}^0[p]$ circuit C of depth d and size s, there is a polynomial $P : \mathbb{F}_p^n \to \mathbb{F}_p$ of degree at most $(p\Delta)^d$ that agrees with C on at least a $(1 - s \cdot 0.9^{\Delta})$ fraction of inputs. Here we treat $\{0, 1\}$ as a subset of $\mathbb{F}_p$ and we guarantee that for every $x \in \{0, 1\}^n$, $P(x) \in \{0, 1\}$. We also assume that C only consists of NOT gates, MOD_p gates, and OR gates (AND gates can be simulated by NOT and OR gates using De Morgan's law), and the definition of MOD_p gates is

$$\mathsf{MOD}_p(x_1, x_2, \ldots, x_n) = \begin{cases} 0 & \text{if } \sum_{i=1}^{n} x_i \equiv 0 \pmod{p}; \\ 1 & \text{otherwise.} \end{cases}$$

Defining the low-degree polynomials. In fact, the Razborov–Smolensky proof provides us a stronger guarantee: There is a *distribution $\mathcal{P}$ of low-degree polynomials* such that for every input $x \in \{0,1\}^n$, with high probability over $P \leftarrow \mathcal{P}$, we have $P(x) = C(x)$. Using error-correcting codes, we can make $\mathcal{P}$ the uniform distribution over a support of size $L = 2^{O(n)}$.[7] That is, there is a list of L polynomials $P_{C,1}, P_{C,2}, \ldots, P_{C,L}$ of degree at most $(p\Delta)^d$ such that for every $x \in \{0,1\}^n$,

$$\Pr_{j \leftarrow [L]}[P_{C,j}(x) \neq C(x)] \leq s \cdot 0.9^{\Delta}.$$

In particular, let $\ell \leq \text{poly}(t)$, $\mathsf{Enc} : \mathbb{F}_p^t \to \mathbb{F}_p^\ell$ be an $\mathbb{F}_p$-linear error-correcting code such that for every $\vec{x} \in \mathbb{F}_p^t \setminus \{0^t\}$, at least a 0.1 fraction of indices $i \in [\ell]$ satisfy that $\mathsf{Enc}(\vec{x})_i \neq 0$. Let $\vec{j} = (j_1, j_2, \ldots, j_\Delta)$ where each $j_i \in [\ell]$. We will have a polynomial $P_{C,\vec{j}}$ for each such $\vec{j}$, hence there are $L = \ell^\Delta$ polynomials in total. We define $P_{C,\vec{j}}$ inductively over the structure of C:

1. If the top gate of C is a NOT gate, then $C = \neg C'$ for some circuit C'. We define $P_{C,\vec{j}} = 1 - P_{C',\vec{j}}$.
2. If the top gate of C is a MOD_p gate, then $C = \mathsf{MOD}_p(C_1, C_2, \ldots, C_t)$ for some $t \in \mathbb{N}$ and sub-circuits $C_1, C_2, \ldots, C_t$. We define

   $$P_{C,\vec{j}} = (\sum_{i=1}^{t} P_{C_i,\vec{j}})^{p-1}.$$

   The correctness of $P_{C,\vec{j}}$ follows from Fermat's little theorem.
3. If the top gate of C is an OR gate, then $C = \mathsf{OR}(C_1, C_2, \ldots, C_t)$ for some $t \in \mathbb{N}$ and sub-circuits $C_1, C_2, \ldots, C_t$. The idea here is to approximate the OR function using the j_1-th, …, j_Δ-th outputs of Enc: let $H_C(x) = (C_1(x), \ldots, C_t(x))$, we "think" that $C(x)$ outputs 1 if there exists some $i \in [\Delta]$ such that $\mathsf{Enc}(H_C(x))_{j_i} \not\equiv 0 \pmod p$.

   In particular, let $\mathsf{OR} : \mathbb{F}_p^\Delta \to \mathbb{F}_p$ be any degree-Δ polynomial over $\mathbb{F}_p$ that computes the OR function over Δ Boolean inputs; for example, one could take $\mathsf{OR}(x_1, \ldots, x_\Delta) = 1 - \prod_{i=1}^{\Delta}(1 - x_i)$. We define

   $$P_{C,\vec{j}} = \mathsf{OR}\Big((\mathsf{Enc}(H_C(x))_{j_1})^{p-1}, (\mathsf{Enc}(H_C(x))_{j_2})^{p-1}, \ldots, (\mathsf{Enc}(H_C(x))_{j_\Delta})^{p-1}\Big).$$

It can be seen from the above inductive proof that the degree of $P_{C,\vec{j}}$ is at most $(p\Delta)^d$.

Correctness of $P_{C,\vec{j}}$. Next we show that for a random $\vec{j}$, there are only a fraction of $0.9^\Delta \cdot s$ inputs $x \in \{0,1\}^n$ such that $P_{C,\vec{j}}(x) \neq C(x)$. In fact, let Bad denote the set of $(x, \vec{j})$ such that $P_{C,\vec{j}}(x) \neq C(x)$, and let $K = 2^n L \cdot 0.9^\Delta \cdot s$, then $|\mathsf{Bad}| \leq K$. Moreover, this inequality can be "feasibly witnessed" by a pair of functions

$$\phi : \mathsf{Bad} \to [K] \quad \text{and} \quad \psi : [K] \to \mathsf{Bad}$$

such that for every $(x, \vec{j}) \in \mathsf{Bad}$, $\psi(\phi(x, \vec{j})) = (x, \vec{j})$. (Clearly, the existence of such functions (ϕ, ψ) implies that $|\mathsf{Bad}| \leq K$. The complexity of computing ϕ and ψ will be crucial our formalisation and will be discussed in Section 9.2.2.)

We identify $[K]$ with $\{0,1\}^n \times [s] \times [0.9^\Delta \cdot L]$. That is, each element in $[K]$ is treated as a tuple (x, g, c) where $x \in \{0,1\}^n$ is an input, $g \in [s]$ is the index of some OR gate in C, and $c \in [0.9^\Delta \cdot L]$ is the "compressed" representation of some $\vec{j} \in [L] = [\ell]^\Delta$ that introduced an error on the g-th gate of C when computing $C(x)$.

[7] As our formalisation in Section 9.2 will use the weak rank principles over matrices of dimension $\text{poly}(L, 2^n)$, it is crucial that L is not too large.

Now, let $(x, \vec{j}) \in \mathsf{Bad}$. Let g be the bottommost gate of C that introduced an error; that is, if we denote by C^g the sub-circuit computed by g, then g is the bottommost gate such that $C^g(x) \neq P_{C^g,\vec{j}}(x)$. Suppose that C^g is the OR of sub-circuits $C_1, C_2, \ldots, C_t$. Then we have:

- $H_g(x) = (C_1(x), C_2(x), \ldots, C_t(x))$ is not the all-zero vector, but for every $k \in [\Delta]$ we have $\mathsf{Enc}(H_g(x))_{j_k} = 0$.

For every fixed x and g, the probability over a random $j \leftarrow [\ell]$ that $H_g(x) \neq \vec{0}$ but $\mathsf{Enc}(H_g(x))_j = 0$ is at most 0.9; hence the probability over a random $\vec{j}$ that the above bullet happens is at most 0.9^Δ. It follows that given x and g, every $\vec{j}$ that makes the above bullet happens can be encoded by a number $c \in [0.9^\Delta \cdot L]$. We then define $\phi(x, \vec{j}) = (x, g, c)$. It is easy to define the inverse function ψ such that $\psi(x, g, c) = (x, \vec{j})$ so that for every $(x, \vec{j}) \in \mathsf{Bad}$, we have that $\psi(\phi(x, \vec{j})) = (x, \vec{j})$.

Basis change. A minor but annoying issue is that Theorem 9.2 deals with low-degree polynomials $P : \{-1,1\}^n \to \{-1,1\}$ but our $P_{C,\vec{j}}$ are polynomials from $\{0,1\}^n$ to $\{0,1\}$. Observe that the linear map $\tau(x) = 1-2x$ maps 0 to 1 and maps 1 to -1, and its inverse map is $\tau^{-1}(x) = \frac{p-1}{2}(x-1)$. We define

$$Q_{C,\vec{j}}(x_1, \ldots, x_n) = \tau(P_{C,\vec{j}}(\tau^{-1}(x_1), \ldots, \tau^{-1}(x_n))).$$

Clearly, the degree of $Q_{C,\vec{j}}$ is the same as the degree of $P_{C,\vec{j}}$. Moreover, for every $x \in \{0,1\}^n$, we have that $P_{C,\vec{j}}(x) = \mathsf{MOD}_2(x)$ if and only if $Q_{C,\vec{j}}(\tau(x)) = \prod_{i=1}^n \tau(x_i)$. (Hereafter, for $x \in \mathbb{F}_p^n$, $\tau(x)$ is a vector in $\mathbb{F}_p^n$ obtained by applying τ to each coordinate of x individually.)

Proof of the main lower bound. Now we are ready to prove the main lower bound against $\mathsf{AC}^0[p]$ circuits. Let $C : \{0,1\}^n \to \{0,1\}$ be an $\mathsf{AC}^0[p]$ circuit that purportedly computes MOD_2. A naïve attempt is to find a good $\vec{j}$, construct the matrices $A \in \mathbb{F}_p^{2^n \times 0.99 \cdot 2^n}$ and $B = B(Q_{C,\vec{j}}) \in \mathbb{F}_p^{0.99 \cdot 2^n \times 2^n}$ (see Definition 9.5), use the weak rank principle to find inputs $z, x \in \{-1,1\}^n$ such that $(AB)[z,x] \neq \delta_{z,x}$, and conclude that $C(\tau^{-1}(z)) \neq \mathsf{MOD}_2(\tau^{-1}(z))$. However, it may be the case that $(\tau^{-1}(z), \vec{j}) \in \mathsf{Bad}$, which does not give us the desired conclusion.

To remedy this, we put the matrices A and $B(Q_{C,\vec{j}})$ together for every possible $\vec{j}$ (there are L many possibilities) in a block-diagonal manner. This results in a giant matrix multiplication of dimension $(2^n L) \times (0.99 \cdot 2^n L) \times (2^n L)$. We still need to handle the entries in Bad. However, since $|\mathsf{Bad}| \ll 0.01 \cdot 2^n L$, we can afford to increase the middle dimension (i.e., $0.99 \cdot 2^n L$) by $|\mathsf{Bad}|$ to "correct" all the values related to entries in Bad.

Theorem 9.6. *Let C be an $\mathsf{AC}^0[p]$ circuit of depth d and size $s < 2^{n^{1/2d}/(20p)}$, then there exists an input $x \in \{0,1\}^n$ such that $C(x) \neq \mathsf{MOD}_2(x)$.*

Proof. We set the following parameters:

Value	Intended meaning
$\Delta = \frac{n^{1/2d}}{10p}$	Number of "samples" taken in $\mathcal{S}$. Equiv. the degree of the "polynomial approximation" of OR
$\ell = \mathrm{poly}(s)$	Output length of Enc
$L = \ell^\Delta \leq \exp(n)$	Number of polynomials in $\mathcal{P}$
$N = 2^n L$	Dimension of the weak rank principle
$K = 2^n L \cdot 0.6^\Delta \cdot s \leq 0.001N$	$\lvert\mathsf{Bad}\rvert$
$R = 0.99 \cdot 2^n L + K \leq 0.991N$	Rank parameter of the weak rank principle

We construct the following two matrices $\hat{A}$ and $\hat{B}$ where $\hat{A} \in \mathbb{F}_p^{N \times R}$ and $\hat{B} \in \mathbb{F}_p^{R \times N}$. It would be convenient to identify $[N]$ with $\{-1,1\}^n \times [L]$, so every element in $[N]$ can be parsed as $(x, \vec{j})$ where $x \in \{-1,1\}^n$ and $\vec{j} \in [\ell]^\Delta$. Similarly, we identify $[R]$ with the disjoint union of $[0.99 \cdot 2^n] \times [\ell]^\Delta$ and $[K]$. Recall from the proof of Theorem 9.2 that we also identified $[0.99 \cdot 2^n]$ with monomials of degree at most $d = n/2 + 0.1\sqrt{n}$.

Let $(z, \vec{j}) \in [N]$ and $a \in [R]$, we define $\hat{A}[(z, \vec{j}), a]$ as follows:

- Suppose $a = (m, \vec{j}') \in [0.99 \cdot 2^n] \times [\ell]^{\Delta}$. If $\vec{j} \neq \vec{j}'$ then $\hat{A}[(z, \vec{j}), a] = 0$; otherwise $\hat{A}[(z, \vec{j}), a] = m(z)$.
- Suppose $a \in [K]$. If $(\tau^{-1}(z), \vec{j}) \in \mathsf{Bad}$ and $a = \phi(\tau^{-1}(z), \vec{j})$ then $\hat{A}[(z, \vec{j}), a] = 1$; otherwise $\hat{A}[(z, \vec{j}), a] = 0$.

Similarly, let $a \in [R]$ and $(x, \vec{j}) \in [N]$, we define $\hat{B}[a, (x, \vec{j})]$ as follows:

- Suppose $a = (m, \vec{j}') \in [0.99 \cdot 2^n] \times [\ell]^{\Delta}$. If $\vec{j} = \vec{j}'$ then $\hat{B}[a, (x, \vec{j})] = B(Q_{C,\vec{j}})[a, x]$ (recall the definition of $B(Q_{C,\vec{j}})$ in Definition 9.5); otherwise $\hat{B}[a, (x, \vec{j})] = 0$.
- Suppose $a \in [K]$. Let $(\tau^{-1}(z), \vec{j}') = \psi(a)$, we define

$$\hat{B}[a, (x, \vec{j})] = \delta_{(z,\vec{j}'),(x,\vec{j})} - \sum_{m \in [0.99 \cdot 2^n]} \hat{A}[(z, \vec{j}'), (m, \vec{j}')] \cdot \hat{B}[(m, \vec{j}'), (x, \vec{j})].$$

  (The intention is to set $\hat{B}[a, (x, \vec{j})]$ so that $(\hat{A} \cdot \hat{B})[(z, \vec{j}'), (x, \vec{j})] = \delta_{(z,\vec{j}'),(x,\vec{j})}$.)

From the above definition it is clear that for every $(\tau^{-1}(z), \vec{j}') \in \mathsf{Bad}$ and every $(x, \vec{j}) \in [N]$, we have $(\hat{A}\hat{B})[(z, \vec{j}'), (x, \vec{j})] = \delta_{(z,\vec{j}'),(x,\vec{j})}$. On the other hand, the weak rank principle implies that there exists $(z, \vec{j}'), (x, \vec{j}) \in [N]$ such that $(\hat{A}\hat{B})[(z, \vec{j}'), (x, \vec{j})] \neq \delta_{(z,\vec{j}'),(x,\vec{j})}$. It is easy to see that $\vec{j} = \vec{j}'$ as otherwise $(\hat{A}\hat{B})[(z, \vec{j}'), (x, \vec{j})] = 0 = \delta_{(z,\vec{j}'),(x,\vec{j})}$. Then we can see that $(A \cdot B(Q_{C,\vec{j}}))[z, x] \neq \delta_{z,x}$. It follows from Claim 9.4 that $Q_{C,\vec{j}}(z) \neq \prod_{i=1}^{n} z_i$, hence $P_{C,\vec{j}}(\tau^{-1}(z)) \neq \mathsf{MOD}_2(\tau^{-1}(z))$. However, since $(\tau^{-1}(z), \vec{j}') \notin \mathsf{Bad}$, we have that $P_{C,\vec{j}}(\tau^{-1}(z)) = C(\tau^{-1}(z))$. Hence $C(\tau^{-1}(z)) \neq \mathsf{MOD}_2(\tau^{-1}(z))$ and C fails to compute the MOD_2 function. □

9.2 Formalisation in $\overline{\mathbf{V}^0(p)} + \mathrm{WRank}_p$

9.2.1 The Theory $\overline{\mathbf{V}^0(p)} + \mathrm{WRank}_p$

We start with a brief introduction to the theories $\mathbf{V}^0(p)$, $\overline{\mathbf{V}^0(p)}$, and $\overline{\mathbf{V}^0(p)} + \mathrm{WRank}_p$. A more comprehensive treatment for the theories $\mathbf{V}^0(p)$ and $\overline{\mathbf{V}^0(p)}$ can be found in Cook and Nguyen's textbook [20]. The theory $\overline{\mathbf{V}^0(p)} + \mathrm{WRank}_p$ is introduced and studied for the first time in this work.

We consider *two-sorted* logic: the first sort are natural numbers (i.e., indices) and the second sort are bit strings (or more precisely, finite sets of natural numbers whose characteristic vectors are bit strings). In this context, we usually use capital letters (X, Y, Z) to denote strings and lower case letters (x, y, z) to denote numbers; however our notation does not strictly follow this convention and we list the exceptions in Remark 9.7.

The vocabulary for two-sorted logic is $\mathcal{L}_A^2$, which contains symbols

$$0, 1, +, \cdot, |\cdot|; =_1, =_2, \leq, \in.$$

Here, $=_1$ and $=_2$ denotes equality over numbers and strings respectively; it is usually clear in the context whether numbers or strings are being compared, so we often omit the subscripts 1 and 2 and simply write $=$ for convenience. We will also use $X(t)$ or X_t to denote "$t \in X$". These symbols are governed by a set of "basic axioms" called 2-**BASIC** (see [20, Figure 2]).

Let Φ be a set of formulas, then we can define the following *axiom schema*:

- Φ-**COMP** (comprehension): $\exists X \leq y \forall z < y\ (X(z) \leftrightarrow \varphi(z))$, where $\varphi(z)$ is any formula in Φ and X does not occur free in $\varphi(z)$.
- Φ-**IND** (number induction): $(\varphi(0) \wedge \forall x\ (\varphi(x) \rightarrow \varphi(x+1))) \rightarrow \forall z\ \varphi(z)$, where $\varphi(z)$ is any formula in Φ.

- Φ-**MIN** (number minimisation): $\varphi(y) \implies (\exists x \le y\ (\varphi(x) \wedge \neg\exists z < x\ \varphi(z)))$, where $\varphi(z)$ is any formula in Φ.

Let $\mathcal{L}$ be a two-sorted vocabulary that contains $\mathcal{L}_A^2$, then $\Sigma_0^B(\mathcal{L})$ is the set of $\mathcal{L}$-formulas whose only quantifiers are bounded number quantifiers (there can be free string variables).

Let m be a constant[8], the theory $\mathbf{V}^0(m)$ has vocabulary $\mathcal{L}_A^2$ and is axiomatised by 2-**BASIC**, $\Sigma_0^B(\mathcal{L}_A^2)$-**COMP**, and an axiom defining the function MOD_m; see [20, Section IX.4.6] for details.

We actually work with the theory $\overline{\mathbf{V}^0(m)}$ instead of $\mathbf{V}^0(m)$. This theory has vocabulary $\mathcal{L}_{\mathsf{FAC}^0(m)}$ that contains a symbol for every function in $\mathsf{FAC}^0(m)$ ($\mathsf{FAC}^0(m)$ is the class of (possibly non-Boolean) *functions* computable in $\mathsf{AC}^0(m)$). It proves $\Sigma_0^B(\mathcal{L}_{\mathsf{FAC}^0(m)})$-**COMP**, $\Sigma_0^B(\mathcal{L}_{\mathsf{FAC}^0(m)})$-**IND**, and $\Sigma_0^B(\mathcal{L}_{\mathsf{FAC}^0(m)})$-**MIN**: for example, for every $\mathsf{FAC}^0(m)$ function f that maps a string X to the string $f(X)$, we can use the number minimisation axiom inside $\overline{\mathbf{V}^0(m)}$ to conclude that if $f(X)$ is not the all-zero string, then there exists the smallest i such that $f(X)_i = 1$. Again, we refer to [20, Section IX.4.6] for more details.

Although $\overline{\mathbf{V}^0(m)}$ "contains much more features" than $\mathbf{V}^0(m)$, it is a conservative extension of $\mathbf{V}^0(m)$, i.e., every formula in the vocabulary $\mathcal{L}_A^2$ that can be proved in $\overline{\mathbf{V}^0(m)}$ can be proved in $\mathbf{V}^0(m)$ as well. Hence it is without loss of generality to work with $\overline{\mathbf{V}^0(m)}$ instead of $\mathbf{V}^0(m)$.

Finally, let $m = p$ be a prime. The *weak rank principle* over $\mathbb{F}_p$, denoted as WRank_p, is the following axiom. Let n be a number, $A \in \mathbb{F}_p^{2n\times n}$ and $B \in \mathbb{F}_p^{n\times 2n}$ be matrices coded as strings, then there exists $x, y \in [2n]$ such that

$$\sum_{z\in[n]} a_{x,z}b_{z,y} \neq \delta_{x,y} \pmod p.$$

(Note that $\sum_{z\in[n]} a_{x,z}b_{z,y} \bmod p$ can be expressed as a function in $\mathsf{FAC}^0[p]$, hence WRank_p is indeed a universal sentence in the language $\mathcal{L}_{\mathsf{FAC}^0(p)}$.) For every constant $\epsilon > 0$, one can use a similar argument as Theorem 7.3 to show that $\overline{\mathbf{V}^0(p)} + \mathrm{WRank}_p$ proves the following: Let n be a number, $A \in \mathbb{F}_p^{(1+\epsilon)n\times n}$ and $B \in \mathbb{F}_p^{n\times(1+\epsilon)n}$ be two matrices encoded as strings, then $AB \neq I_{(1+\epsilon)n}$. In other words, "$\mathrm{rank}(I_{2n}) > n$" and "$\mathrm{rank}(I_{(1+\epsilon)n}) > n$" are equivalent, and replacing the constant 2 in the definition of WRank_p with other constants greater than 1 does not affect the strength of the theory $\overline{\mathbf{V}^0(p)} + \mathrm{WRank}_p$. In fact, our formalisation will use "$\mathrm{rank}(I_{(1+\epsilon)n}) > n$" for some small constant $\epsilon > 0$.

9.2.2 Smolensky's Lower Bound in $\overline{\mathbf{V}^0(p)} + \mathrm{WRank}_p$

Fix a constant $d \in \mathbb{N}$ (in the meta-theory). Let $n \in \mathsf{Log}$ (that is, we assume 2^n is a "number"), $s = 2^{n^{1/2d}/(20p)}$, and C be a string that codes an $\mathsf{AC}^0[p]$ circuit of depth d and size s. Let $\mathsf{Eval}_d(C, x)$ denote the circuit evaluation function on depth-d $\mathsf{AC}^0[p]$ circuits, where $x \in [2^n]$ is a number that denotes the input of C. Since Eval_d is in $\mathsf{AC}^0[p]$, it is in the language of $\overline{\mathbf{V}^0(p)}$. Also, since x is a number, we can talk about $\mathsf{MOD}_2(x)$ in $\overline{\mathbf{V}^0(p)}$. Our goal is to prove that

$$\exists x\ \mathsf{Eval}_d(C, x) \neq \mathsf{MOD}_2(x).$$

Remark 9.7. It should be clear from the context whether a variable is of the number sort or the string sort. Most of the times we use capital letters (X, Y, Z) to denote strings and use lower-case letters (x, y, z) to denote numbers. However, one exception is that L, N, K, R (in the proof of Theorem 9.6) are numbers.

The matrix $B(P)$ (Definition 9.5). It is clear from the definition that there is an $\mathsf{FAC}^0[p]$ function that given (m, x) and the list of coefficients in P, outputs the value of $B(P)[m, x]$.

Claim 9.8 ($\overline{\mathbf{V}^0(p)} \vdash$:). *Let $z, x \in \{-1, 1\}^n$ such that $(A \cdot B(P))[z, x] \neq \delta_{z,x}$. Then $P(z) \neq \prod_{i=1}^n z_i$.*

[8] Here we mainly consider the case that $m = p$ is a prime, but it also makes perfect sense to consider the theory $\mathbf{V}^0(m)$ when m is a composite number.

Proof Sketch. The proofs of both Claim 9.3 and Claim 9.4 can be carried out in $\overline{\mathbf{V}^0(p)}$. □

The polynomials $P_{C,\vec{j}}$ and $Q_{C,\vec{j}}$. For each gate g, let C^g denote the sub-circuit computed by g, we represent the polynomials $P_{C^g,\vec{j}}$ and $Q_{C^g,\vec{j}}$ by their list of coefficients. There is an $\mathsf{FAC}^0[p]$ circuit that given the description of C, an index g, and a list of vectors $\vec{j}$, outputs the coefficient list of $P_{C^g,\vec{j}}$. (Note that since $\vec{j} \in [\ell]^\Delta$ and $\ell^\Delta = L$ is a number in the theory, $\vec{j}$ can be represented as a single number.) The coefficient list of $Q_{C,\vec{j}}(x) = P_{C,\vec{j}}(x - \vec{1}) + 1$ can be computed in $\mathsf{FAC}^0[p]$ as well, If C^g is an $\mathsf{AC}^0[p]$ circuit of depth d, then the degree of $P_{C^g,\vec{j}}$ is at most $(p\Delta)^d$ (and we only consider monomials up to this degree in our representation).

A good error-correcting code. Before formalising the low-degree approximations of $\mathsf{AC}^0[p]$ circuits, we need the following $\mathbb{F}_p$-linear error-correcting code whose correctness can be proved feasibly. In fact, we need to feasibly prove the following formalisation of "every nonzero codeword of Enc has constant relative Hamming weight":

Theorem 9.9. *Suppose that $\log^2 s \in \mathsf{Log}$. For some $\ell \le \mathrm{poly}(s)$, there is an $\mathbb{F}_p$-linear code $\mathsf{Enc} : \mathbb{F}_p^s \to \mathbb{F}_p^\ell$ and functions $\tilde{\phi}(X, i_1, i), \tilde{\psi}(X, i_1, c)$ computable in $\mathsf{FAC}^0[p]$ such that $\overline{\mathbf{V}^0(p)}$ proves the following. For every string $X \in \mathbb{F}_p^s$, every numbers $i_1 \in [s]$ and $i \in [\ell]$, if $X_{i_1} \neq 0$ but $\mathsf{Enc}(X)_i = 0$, then:*

- *$\tilde{\phi}(X, i_1, i)$ returns a number in $[0.9\ell]$, and*
- *$\tilde{\psi}(X, i_1, \tilde{\phi}(X, i_1, i)) = i$.*

Note that the above statement implies that the relative Hamming weight of $\mathsf{Enc}(X)$ is at least 0.1. Roughly speaking, the error-correcting code is the concatenation of Reed–Muller code and Hadamard code; the proof proceeds by formalising the local (unique-)decoding algorithm of the Reed–Muller code (see e.g., [8, Section 19.4.2]). We postpone the proof to Section 9.2.3.

The functions ϕ, ψ. We need to show that ϕ and ψ are computable in $\mathsf{FAC}^0[p]$. Given a string C representing our $\mathsf{AC}^0[p]$ circuit and two numbers x, $\vec{j}$, we can compute $\phi(x, \vec{j})$ as follows:

1. First, find the bottommost gate g for which $C^g(x) \neq P_{C^g,\vec{j}}(x)$.

   For every g, we can compute the indicator of whether $C^g(x) = P_{C^g,\vec{j}}(x)$ in $\mathsf{AC}^0[p]$. Then we use an FAC^0 circuit to compute the number g, which is the index of the bottommost gate on which the indicator is False. (If there is no such gate then we set $g = \bot$.)

2. Let $H_g(x) = (C_1(x), \ldots, C_t(x))$ where $C_1, \ldots, C_t$ are input gates of g. For each $k \in [\Delta]$, we have that $\mathsf{Enc}(H_g(x))_{j_k} = 0$. However, there exists an index $j' \in [t]$ such that $C_{j'}(x) = 1$, and the smallest such index can be computed in FAC^0 given $H_g(x)$. Hence we compute $c_k = \tilde{\phi}(H_g(x), j', j_k) \in [0.9\ell]$ using Theorem 9.9. This gives us a vector $\vec{c} = (c_1, \ldots, c_\Delta)$. (Note that $\ell^\Delta = L$ is a number in the theory, hence $\vec{c}$ can be represented as a single number.) We output $\phi(x, \vec{j}) = (x, g, \vec{c})$.

Similarly, one can compute ψ in $\mathsf{FAC}^0[p]$ by invoking the function $\tilde{\psi}$ in Theorem 9.9. Namely, given a string C representing our $\mathsf{AC}^0[p]$ circuit and three numbers $x, g, \vec{c}$, we can compute $\psi(x, g, \vec{c})$ as follows. First, let $C_1, \ldots, C_t$ be the input gates of g, we can compute $H_g(x) = (C_1(x), \ldots, C_t(x))$ in $\mathsf{FAC}^0[p]$. We can also compute the smallest index j' such that $C_{j'}(x) = 1$ in FAC^0 given $H_g(x)$. Then, for each $K \in [\Delta]$, we let $j_k = \tilde{\psi}(H_g(x), j', c_k)$. We return $\psi(x, g, \vec{c}) = (x, \vec{j})$.

Claim 9.10 ($\overline{\mathbf{V}^0(p)} \vdash$:)**.** *Suppose that $\log^2 s \in \mathsf{Log}$. For every $x \in \{0,1\}^n$ and $\vec{j} \in [\ell]^\Delta$, if $P_{C,\vec{j}}(x) \neq C(x)$, then $\psi(\phi(x, \vec{j})) = (x, \vec{j})$.*

Proof Sketch. Since $P_{C,\vec{j}}(x) \neq C(x)$, it follows from $\Sigma_0^B(\mathcal{L}_{\mathsf{FAC}^0(p)})$-**MIN** that there exists a bottommost gate g for which $C^g(x) \neq P_{C^g,\vec{j}}(x)$. It follows that $H_g(x)_{j'} \neq 0$ but $\mathsf{Enc}(H_g(x))_{j_k} = 0$ for every $k \in [\Delta]$. Let $c_k = \tilde{\phi}(H_g(x), j', j_k)$, then $\phi(x, \vec{j}) = (x, g, \vec{c})$. Let $\psi(x, g, \vec{c}) = (x, \vec{j}')$, then for every $k \in [\Delta]$,

$$j'_k = \tilde{\psi}(H_g(x), j', c_k) = \tilde{\psi}(H_g(x), j', \phi(H_g(x), j', j_k)) = j_k$$

where the last equality follows from Theorem 9.9. Hence $\psi(\phi(x, \vec{j})) = (x, \vec{j})$. □

The matrices $\hat{A}, \hat{B}$ as defined in the proof of Theorem 9.6. It is easy to see that these matrices can be computed in $\mathsf{FAC}^0[p]$. That is, there is an $\mathsf{FAC}^0[p]$ function that takes a string C and numbers $z, \vec{j}, a$ as inputs and outputs the value of $\hat{A}[(z, \vec{j}), a]$, and the analogous statement holds for $\hat{B}$.

Claim 9.11 ($\overline{\mathbf{V}^0(p)} \vdash$:). *Let $z, x \in \{-1, 1\}^n$, $\vec{j}, \vec{j}' \in [\ell]^\Delta$, then:*
(a) *If $\vec{j} \neq \vec{j}'$, then $(\hat{A}\hat{B})[(z, \vec{j}), (x, \vec{j}')] = 0$.*
(b) *If $\psi(\phi(z - \vec{1}, \vec{j})) = (z - \vec{1}, \vec{j})$, then $(\hat{A}\hat{B})[(z, \vec{j}), (x, \vec{j})] = \delta_{(z,\vec{j}),(x,\vec{j}))}$.*
(c) *If $\psi(\phi(z - \vec{1}, \vec{j})) \neq (z - \vec{1}, \vec{j})$, then $(\hat{A}\hat{B})[(z, \vec{j}), (x, \vec{j})] = (A \cdot B(Q))[z, x]$.*

Proof Sketch. These follow easily from the definitions. □

Putting it together. Fix a constant $d \in \mathbb{N}$ (in the meta-language), we have:

Theorem 9.12 ($\overline{\mathbf{V}^0(p)} + \mathrm{WRank}_p \vdash$:). *Let $n \in \mathsf{Log}$, $s = 2^{n^{1/2d}/(20p)}$, and C be a string that codes an $\mathsf{AC}^0[p]$ circuit of depth d and size s. Then there exists an input $x \in \{0, 1\}^n$ (coded as a number) such that $\mathsf{Eval}_d(C, x) \neq \mathsf{MOD}_2(x)$.*

Proof. Consider the matrices $\hat{A}$ and $\hat{B}$ as defined above. By WRank_p, there exists $(z, \vec{j}'), (x, \vec{j}) \in [N]$ such that $(\hat{A}\hat{B})[(z, \vec{j}'), (x, \vec{j})] \neq \delta_{(z,\vec{j}'),(x,\vec{j})}$. Then:

- By Claim 9.11 (item a), $\vec{j} = \vec{j}'$;
- By Claim 9.11 (item b), $\psi(\phi(z - \vec{1}, \vec{j})) \neq (z - \vec{1}, \vec{j})$;
- By Claim 9.11 (item c), $(AB)[(z, \vec{j}), (x, \vec{j})] = (A \cdot B(Q_{C,\vec{j}}))[z, x] \neq \delta_{z,x}$.
- By Claim 9.8, $Q_{C,\vec{j}}(z) \neq \prod_{i=1}^n z_i$, hence $P_{C,\vec{j}}(z - \vec{1}) \neq \mathsf{MOD}_2(z - \vec{1})$;
- By Claim 9.10 (and note that it is indeed the case that $\log^2 s \in \mathsf{Log}$), $P_{C,\vec{j}}(z - \vec{1}) = C(z - \vec{1})$. Hence $C(z - \vec{1}) \neq \mathsf{MOD}_2(z - \vec{1})$. □

Remark 9.13 (Comparison with [57]). We point out a few differences between our formalisation of Smolensky's lower bounds and the formalisation in [57].

1. Müller and Pich proved a lower bound against circuits of size $n^{\log n}$ in the (single-sorted) theory $\mathbf{APC}_1$ with the assumption that $n^{\log^{9d} n} \in \mathsf{Log}$. This allows randomised quasi-polynomial-time reasoning over the purported $\mathsf{AC}^0[p]$ circuit. We prove a lower bound against size $2^{\Omega(n^{1/2d})}$ in the (two-sorted) theory $\overline{\mathbf{V}^0(p)} + \mathrm{WRank}$ where the circuit is represented as an object of string sort. Except for the weak rank principle, this theory only allows (quasi-polynomial-size) $\mathsf{AC}^0[p]$-reasoning over the purported $\mathsf{AC}^0[p]$ circuit.

2. One drawback in the Müller–Pich proof is the requirement that $n^{\log^{9d} n} \in \mathsf{Log}$. In fact, this allows them to prove the required rank principle by *brute force*. Our formalisation explicitly separates the weak rank principles from other $\mathsf{AC}^0[p]$-manipulations.

9.2.3 Proof of Theorem 9.9

Theorem 9.9. *Suppose that $\log^2 s \in \mathsf{Log}$. For some $\ell \leq \mathrm{poly}(s)$, there is an $\mathbb{F}_p$-linear code $\mathsf{Enc} : \mathbb{F}_p^s \to \mathbb{F}_p^\ell$ and functions $\tilde{\phi}(X, i_1, i), \tilde{\psi}(X, i_1, c)$ computable in $\mathsf{FAC}^0[p]$ such that $\overline{\mathbf{V}^0(p)}$ proves the following. For every string $X \in \mathbb{F}_p^s$, every numbers $i_1 \in [s]$ and $i \in [\ell]$, if $X_{i_1} \neq 0$ but $\mathsf{Enc}(X)_i = 0$, then:*

- $\tilde{\phi}(X, i_1, i)$ *returns a number in* $[0.9\ell]$*, and*
- $\tilde{\psi}(X, i_1, \tilde{\phi}(X, i_1, i)) = i$.

Proof. Let $n = O(\log s / \log\log s)$, $h = \lceil s^{1/n} \rceil$, q be the smallest power of p that is greater than $10nh$. Note that $q \le \log^2 s \in \mathsf{Log}$, hence $\overline{\mathbf{V}^0(p)}$ can reason about $\mathbb{F}_q$ by brute force. (For example, $\overline{\mathbf{V}^0(p)}$ can prove the existence of an irreducible degree-$\log_p q$ polynomial over $\mathbb{F}_p$. See e.g., [43, Section 4.3].) Let H be the set of lexicographically first h elements in $\mathbb{F}_q$. We interpret $X \in \mathbb{F}_p^s \subseteq \mathbb{F}_q^s$ as a function $X : H^n \to \mathbb{F}_q$. Then there is a unique polynomial $\tilde{X} : \mathbb{F}_q^n \to \mathbb{F}_q$ of individual degree at most h that is consistent with X on H^n. Moreover, one can compute $\tilde{X}(\vec{v})$ using an $\mathsf{FAC}^0[p]$ circuit (in fact, an $\mathbb{F}_q$-linear transformation) over the string input X and the number input $\vec{v}$.

We now concatenate the above Reed–Muller code with the Hadamard code. Treat $\mathbb{F}_q$ as the $\log_p q$-dimensional vector space over $\mathbb{F}_p$, then each $\alpha \in \mathbb{F}_q$ is encoded as a vector $\mathrm{Had}(\alpha) \in \mathbb{F}_p^q$ defined as follows. For each $u \in \mathbb{F}_q$, we interpret both α and u as vectors in $\mathbb{F}_p^{\log_p q}$, and the u-th element of $\mathrm{Had}(\alpha)$ is equal to $\mathrm{IP}(\alpha, u) = \sum_{j=1}^{\log_p q} \alpha_j u_j$. Again, since $q \in \mathsf{Log}$, $\overline{\mathbf{V}^0(p)}$ can reason about the Hadamard code using brute force.

Define $\mathsf{Enc}(X)$ be the concatenation of $\mathrm{Had}(\tilde{X}(\vec{v}))$ for each $\vec{v} \in \mathbb{F}_q^n$. That is, the length of $\mathsf{Enc}(X)$ is $\ell = q^{n+1} \le \mathrm{poly}(s)$. Given an index $i \in [\ell]$, we interpret i as a pair of vectors $(\vec{v} \in \mathbb{F}_q^n, u \in \mathbb{F}_q = \mathbb{F}_p^{\log_p q})$, and define $\mathsf{Enc}(X)_i = \mathrm{IP}(\tilde{X}(v), u)$.

The local decoder of the Reed–Muller code requires the following equivalence class over "directions" in $\mathbb{F}_q^n$: two non-zero vectors $\vec{v}_1, \vec{v}_2 \in \mathbb{F}_q^n$ are equivalent if and only if there is a non-zero scalar $\alpha \in \mathbb{F}_q$ such that $\vec{v}_1 = \alpha \vec{v}_2$. Let $\vec{v}$ be a non-zero vector in $\mathbb{F}_q^n$ and define $[\vec{v}]$ as the following vector: let $i \in [n]$ be the first index such that $v_i \neq 0$, and for each $j \in [n]$, the j-th element of $[\vec{v}]$ is equal to $v_i^{-1} v_j$ (over $\mathbb{F}_q$). Again, $\overline{\mathbf{V}^0(p)}$ can prove (by brute force) that v_1 and v_2 are equivalent if and only if $[v_1] = [v_2]$, and that there are $q^{n-1} + q^{n-2} + \cdots + q + 1 \le 2q^{n-1}$ equivalence classes.

Let $X \in \mathbb{F}_p^s$ be a non-zero string, $i_1 \in [s]$ be an index such that $X_{i_1} = 1$, and $i \in [\ell]$ be an index such that $\mathsf{Enc}(X)_i = 0$. We interpret i as a pair of vectors $(\vec{v} \in \mathbb{F}_q^n, u \in \mathbb{F}_q)$. To compute $\hat{\phi}(X, i_1, i)$, we consider the following two cases:

- If $\tilde{X}(\vec{v}) \neq 0$, then we consider the Hadamard code. In particular, u is among the vectors in $\mathbb{F}_q$ for which $\mathrm{IP}(\tilde{X}(\vec{v}), u) = 0$. There are at most q/p such elements, hence we let $\tilde{\phi}(X, i_1, i) = (\mathsf{Hadamard}, \vec{v}, k)$ where u is the k-th smallest element in $\mathbb{F}_q$ such that $\mathrm{IP}(\tilde{X}(\vec{v}), u) = 0$.
- If $\tilde{X}(\vec{v}) = 0$, then we consider the Reed–Muller code. In particular, consider the directional vector $\vec{w} = \vec{v} - i_1$ (where we interpret $i_1 \in [s] \subseteq \mathbb{F}_q^n$ and the subtraction happens in $\mathbb{F}_q^n$). The unique line determined by $\vec{v}$ and i_1 is $\ell(t) = t \cdot [\vec{w}] + i_1$. Composing $\tilde{X}$ with ℓ gives us a univariate polynomial $f(t) = \tilde{X}(t \cdot [\vec{w}] + i_1)$ of degree at most nh. Since $f(0) \neq 0$, this polynomial has at most nh roots. We define $\tilde{\phi}(X, i_1, i) = (\mathsf{Reed\text{–}Muller}, [\vec{w}], k, u)$ where $\vec{v}$ corresponds to the k-th root of f. (Recall that k can be found by brute force.)

Now we can see that $\tilde{\phi}(X, i_1, i)$ either returns $(\mathsf{Hadamard}, \vec{v}, k)$ where $\vec{v} \in \mathbb{F}_q^n, k \in [q/p]$ or returns $(\mathsf{Reed\text{–}Muller}, [\vec{w}], k, u)$ where $[\vec{v}] \in [2q^{n-1}]$, $k \in [q/10]$, $u \in \mathbb{F}_q$. It follows that the size of $\mathrm{Range}(\tilde{\phi})$ is at most $q^{n+1}/p + q^{n+1}/5 \le 0.9\ell$.

We can similarly define the function $\tilde{\psi}(X, i_1, c)$:

- If c is of the form $(\mathsf{Hadamard}, \vec{v}, k)$, then we compute the k-th smallest $u \in \mathbb{F}_q$ such that $\mathrm{IP}(\tilde{X}(\vec{v}), u) = 0$ and output $(\vec{v}, u)$.
- If c is of the form $(\mathsf{Reed\text{–}Muller}, [\vec{w}], k, u)$, then we compute the k-th root $\vec{v}$ of the degree-nh polynomial $f(t) = \tilde{X}(t \cdot [\vec{w}] + i_1)$ and output $(\vec{v}, \vec{u})$.

It is easy to see that $\psi(X, i_1, \phi(X, i_1, i)) = i$ for every i such that $\mathsf{Enc}(X)_i = 0$. □

A Expander Properties

The proofs here mostly mimic the corresponding proofs from [73].

Lemma 4.15. *Let $C > 1$. There exist constants $\delta, d > 0$ such that for every large enough positive integers m, n with $n < m < Cn$, there is an $m \times n$ bipartite graph G satisfying the following:*

1. *the minimum left-degree of G is at least $\Delta_{min} = 50 \log n$,*
2. *the maximum left-degree of G is at most $\Delta_{max} = 150 \log n$,*
3. *G is an (n^δ, d)-lossless expander.*

In particular, G is an $(n^\delta, \Delta_{min} - d)$-boundary expander.

Proof. The proof essentially follows [73] but with a slightly different choice of parameters. We construct a bipartite graph G with parts $[m]$ and $[n]$. For every $i \in [m]$ and $k \in [n]$, we add an edge between i and k with probability $\frac{100 \log n}{n}$. Let $M_G = (a_{i,j})_{i \in [m], k \in [n]}$ be the adjacency matrix of such graph.

For each $i \in [m]$ and $k \in [n]$, $a_{i,k} = 1$ with probability $\frac{100 \log n}{n}$. Hence $\sum_{k \in [n]} a_{i,k}$ is the sum of n independent variables with expectation $100 \log n$. We apply the standard multiplicative Chernoff bound (see, e.g., [56, Corollary 4.6]), which states that for any $0 < \epsilon < 1$, $\Pr[|X - \mathbb{E}[X]| > \epsilon \mathbb{E}[X]] \leq 2 \exp(-\epsilon^2 \mathbb{E}[X]/3)$. Taking $X = \sum_{k \in [n]} a_{i,k}$, $\mathbb{E}[X] = 100 \log n$, and $\epsilon = 1/2$, we obtain

$$\Pr\left[\left|\sum_{k \in [n]} a_{i,k} - 100 \log n\right| > 50 \log n\right] \leq 2e^{100 \log n/12} = o(1/n).$$

By the union bound, these events happen simultaneously for all $i \in [m]$ and $k \in [n]$ with probability $o(1)$.

Now let $r = n^\delta$.

Claim A.1. *If property (7) is violated for some set $I \subseteq [m]$ of size $l \leq r$, then there exist a set $K \subseteq [n]$ of size $ld/2$ such that the rectangle $I \times K$ contains at least ld ones in A.*

Proof. Let $K = \bigcup_{i \in I} \mathcal{N}_G(i) \setminus \partial_G(I)$, i.e., it contains all non-unique neighbours of I. In particular, every column of the rectangle $I \times K$ contains at least two ones. Thus, if $|K| \geq ld/2$, we can take any $K' \subseteq K$ of size exactly $ld/2$. Now assume that $|K| < ld/2$. The number of ones in $I \times K$ is at least

$$\sum_{i \in I} |\mathcal{N}_G(i) \setminus \partial_G(I)| = \sum_{i \in I} |\mathcal{N}_G(i)| - |\partial_G(I)|,$$

since each $k \in \partial_G(I)$ is contained in exactly one $\mathcal{N}_G(i)$. Thus, since (7) is violated for I, this is further lower bounded by $d|I| = ld$. To conclude the proof, we can arbitrarily enlarge K to have size exactly $ld/2$. ◇

Now we will bound the probability of the existence of such $I \times K$. For every $\ell \in [r]$, there is at most $(Cn)^\ell$ choices of I, $n^{\ell d/2}$ choices of K, and $(\ell d)^{2\ell d}$ choices of the positions of ones in $I \times K$. Thus, the probability that there exists such a rectangle $I \times K$ with $|I| = \ell \leq r = n^\delta$ is at most

$$(Cn)^\ell n^{\ell d/2} (\ell d)^{2\ell d} \left(\frac{100 \log n}{n}\right)^{\ell d} \leq n^{2\ell} \left(\frac{n^{4\delta} d^4 (100 \log n)^2}{n}\right)^{\ell d/2} \leq n^{-2\ell}$$

for small enough δ and large enough n and d. Observing that $\sum_{\ell=1}^{r} n^{-2\ell} = o(1)$, the proof follows. □

Lemma 4.16. *Let G be an $m \times n$ (n^δ, d)-lossless expander with parts L and R, a minimum left-degree at least $\Delta_{min} = 50 \log n$ and a maximum left-degree at most $\Delta_{max} = 150 \log n$. Let K be a*

random subset of R such that every $j \in R$ is added to K independently with probability $2/3$. Then the graph $G \setminus K$ is an (n^δ, d)-lossless expander with a minimum left-degree $\Delta_{min}/6$ with probability $1 - o(1)$. In particular, $G \setminus K$ is an (n^δ, c)-boundary expander, where $c = \Delta_{min}/6 - d$.

Proof. Let $G' = G \setminus K$. For every $i \in L$, let $M_i \subseteq \mathcal{N}_G(i)$ be any fixed subset of size exactly Δ_{min}. ~~By the Chernoff bound, $\Pr[|M_i \setminus K| < \Delta_{min}/6] \leq o(1/n)$.~~

For each $i \in L$, every vertex $k \in M_i$ is included in K independently with probability $2/3$, and therefore survives with probability $1/3$. Hence $|M_i \setminus K|$ is the sum of Δ_{min} independent indicator variables with expectation $(1/3)\Delta_{min}$. We apply the standard multiplicative Chernoff bound (see, e.g., [56, Theorem 4.5]), which states that for any $0 < \epsilon < 1$, $\Pr[X < (1-\epsilon)\,\mathbb{E}[X]] \leq \exp(-\epsilon^2\,\mathbb{E}[X]/2)$. Taking $X = |M_i \setminus K|$, $\mathbb{E}[X] = (1/3)\Delta_{min}$, and $\epsilon = 1/2$, we obtain

$$\Pr[|M_i \setminus K| < \Delta_{min}/6] \leq e^{-\Delta_{min}/24} = o(1/n),$$

since $\Delta_{min} = 50 \log n$.

By the union bound, the left-degree of G' is at least $\Delta_{min}/6$ with probability $1 - o(1)$.

The remaining part of the proof repeats the argument from [73]. Let $I \subseteq L$ with $|I| \leq n^\delta$. For every $k \in R$, let $\gamma_k = |\{i \in I : k \in \mathcal{N}_G(i)\}|$. Using the bound from (7), it is easy to see that

$$\sum_{\substack{k \in R \\ \gamma_k \geq 2}} \gamma_k = \sum_{i \in I} |\mathcal{N}_G(i)| - |\partial_G(I)| \leq d|I|.$$

Now let $\gamma'_k = |\{i \in I : k \in \mathcal{N}_{G'}(i)\}|$. Clearly, $\gamma'_k \leq \gamma_k$ for all k, since $\gamma'_k = 0$ for all $k \in K$. This implies that

$$\sum_{i \in I} |\mathcal{N}_{G'}(i)| - |\partial_{G'}(I)| = \sum_{\substack{k \in R \\ \gamma'_k \geq 2}} \gamma'_k \leq \sum_{\substack{k \in R \\ \gamma_k \geq 2}} \gamma_k \leq d|I|. \qquad \square$$

References

[1] Miklós Ajtai. Parity and the pigeonhole principle. In Samuel R. Buss and Philip J. Scott, editors, *Feasible Mathematics: A Mathematical Sciences Institute Workshop, Ithaca, New York, June 1989*, pages 1–24. Birkhäuser Boston, Boston, MA, 1990. 19

[2] Miklós Ajtai. The complexity of the pigeonhole principle. *Comb.*, 14(4):417–433, 1994. 3

[3] Michael Alekhnovich, Eli Ben-Sasson, Alexander A. Razborov, and Avi Wigderson. Space complexity in propositional calculus. *SIAM J. Comput.*, 31(4):1184–1211, 2002. 17

[4] Michael Alekhnovich, Eli Ben-Sasson, Alexander A. Razborov, and Avi Wigderson. Pseudorandom generators in propositional proof complexity. *SIAM J. Comput.*, 34(1):67–88, 2004. 3, 6, 7, 8, 12, 15, 21, 30

[5] Michael Alekhnovich and Alexander A. Razborov. Lower bounds for polynomial calculus: Non-binomial case. In *IEEE Annual Symposium on Foundations of Computer Science 2001*, pages 190–199, 2001. 6

[6] Robert Andrews. On matrix multiplication and polynomial identity testing. *SIAM Journal on Computing*, pages FOCS22–1, 2024. 21

[7] Robert Andrews and Michael A. Forbes. Ideals, determinants, and straightening: Proving and using lower bounds for polynomial ideals. In *54th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2022*, pages 389–402. ACM, 2022. 4, 21

[8] Sanjeev Arora and Boaz Barak. *Computational Complexity: A Modern Approach*. Cambridge University Press, New York, NY, USA, 2009. 73, 80

[9] Albert Atserias and Tuomas Hakoniemi. Size-degree trade-offs for sums-of-squares and Positivstellensatz proofs. In *34th Computational Complexity Conference, CCC 2019, July 18-20, 2019, New Brunswick, NJ, USA*, pages 24:1–24:20, 2019. 8, 30

[10] Per Austrin and Kilian Risse. Sum-of-squares lower bounds for the minimum circuit size problem. In Amnon Ta-Shma, editor, *38th Computational Complexity Conference, CCC 2023, July 17-20, 2023, Warwick, UK*, volume 264 of *LIPIcs*, pages 31:1–31:21. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2023. 13

[11] László Babai and Péter Frankl. *Linear algebra methods in combinatorics*. Department of Computer Science, Univ. of Chicago, 1992. 14

[12] Paul Beame, Stephen Cook, Jeff Edmonds, Russell Impagliazzo, and Toniann Pitassi. The relative complexity of NP search problems. *Journal of Computer and System Sciences*, 57(1):3–19, 1998. 9

[13] Paul Beame, Russell Impagliazzo, Jan Krajíček, Toniann Pitassi, and Pavel Pudlák. Lower bounds on Hilbert's Nullstellensatz and propositional proofs. *Proc. London Math. Soc. (3)*, 73(1):1–26, 1996. 16

[14] Eli Ben-Sasson and Russell Impagliazzo. Random CNF's are hard for the polynomial calculus. *Comput. Complex.*, 19(4):501–519, 2010. 12

[15] Maria Luisa Bonet, Samuel R. Buss, and Toniann Pitassi. Are there hard examples for Frege systems? In *Feasible mathematics, II (Ithaca, NY, 1992)*, volume 13 of *Progr. Comput. Sci. Appl. Logic*, pages 30–56. Birkhäuser Boston, Boston, MA, 1995. 4, 5, 6

[16] Samuel R. Buss. Polynomial size proofs of the propositional pigeonhole principle. *J. Symb. Log.*, 52(4):916–927, 1987. 3

[17] Samuel R. Buss, Dima Grigoriev, Russell Impagliazzo, and Toniann Pitassi. Linear gaps between degrees for the polynomial calculus modulo distinct primes. *J. Comput. Syst. Sci.*, 62(2):267–289, 2001. 8, 17, 30

[18] Lijie Chen, Jiatu Li, and Igor C. Oliveira. Reverse mathematics of complexity lower bounds. In *Proceedings of the 65th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 505–527. IEEE, 2024. 13

[19] Matthew Clegg, Jeff Edmonds, and Russell Impagliazzo. Using the Groebner basis algorithm to find proofs of unsatisfiability. In *Proceedings of the Annual ACM Symposium on the Theory of Computing 1996*, pages 174–183, 1996. 8, 16, 22, 30

[20] Stephen Cook and Phuong Nguyen. *Logical Foundations of Proof Complexity*. ASL Perspectives in Logic. Cambridge University Press, 2010. 3, 14, 78, 79

[21] Stephen A. Cook. A taxonomy of problems with fast parallel algorithms. *Information and Control*, 64(1-3):2–21, 1985. 14

[22] Stephen A. Cook and Robert A. Reckhow. Corrections for "On the lengths of proofs in the propositional calculus (preliminary version)". *SIGACT News*, 6(3):15–22, July 1974. 85

[23] Stephen A. Cook and Robert A. Reckhow. On the lengths of proofs in the propositional calculus (preliminary version). In *Proceedings of the Annual ACM Symposium on the Theory of Computing 1974*, pages 135–148, 1974. For corrections see Cook-Reckhow [22]. 16

[24] Ernie Croot, Vsevolod F Lev, and Péter Pál Pach. Progression-free sets in $\mathbb{Z}_4^n$ are exponentially small. *Annals of Mathematics*, pages 331–337, 2017. 14

[25] Stefan S. Dantchev and Barnaby Martin. Rank complexity gap for Lovász-Schrijver and Sherali-Adams proof systems. *Comput. Complex.*, 22(1):191–213, 2013. 12, 17

[26] Stefan S. Dantchev, Barnaby Martin, and Mark Nicholas Charles Rhodes. Tight rank lower bounds for the Sherali-Adams proof system. *Theor. Comput. Sci.*, 410(21-23):2054–2063, 2009. 12, 19

[27] Susanna F. de Rezende, Mika Göös, Jakob Nordström, Toniann Pitassi, Robert Robere, and Dmitry Sokolov. Automating algebraic proof systems is NP-hard. In *STOC*, pages 209–222. ACM, 2021. 17, 18

[28] Susanna F. de Rezende, Jakob Nordström, Kilian Risse, and Dmitry Sokolov. Exponential resolution lower bounds for weak pigeonhole principle and perfect matching formulas over sparse graphs. *TheoretiCS*, 4, 2025. 5

[29] Zeev Dvir. On the size of Kakeya sets in finite fields. *Journal of the American Mathematical Society*, 22(4):1093–1097, 2009. 14

[30] Jordan S Ellenberg and Dion Gijswijt. On large subsets of $\mathbb{F}_q^n$ with no three-term arithmetic progression. *Annals of Mathematics*, pages 339–343, 2017. 14

[31] Nicola Galesi, Joshua A. Grochow, Toniann Pitassi, and Adrian She. On the algebraic proof complexity of tensor isomorphism. In *38th Computational Complexity Conference (CCC 2023)*, volume 264 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 4:1–4:35. Schloss Dagstuhl–Leibniz-Zentrum für Informatik, 2023. 4, 5, 15

[32] Oded Goldreich, Shafi Goldwasser, and Silvio Micali. How to construct random functions. *J. ACM*, 33(4):792–807, 1986. 10, 11

[33] Dima Grigoriev. Linear lower bound on degrees of Positivstellensatz calculus proofs for the parity. *Theoret. Comput. Sci.*, 259(1-2):613–622, 2001. 8, 12, 30

[34] Joshua A. Grochow and Toniann Pitassi. Circuit complexity, proof complexity, and polynomial identity testing: The ideal proof system. *J. ACM*, 65(6):37:1–37:59, 2018. 4

[35] Armin Haken. The intractability of resolution. *Theoret. Comput. Sci.*, 39(2-3):297–308, 1985. 3

[36] Johan Håstad. On small-depth Frege proofs for Tseitin for grids. *J. ACM*, 68(1), November 2020. 9

[37] Pavel Hrubes and Iddo Tzameret. Short proofs for the determinant identities. *SIAM J. Comput.*, 44(2):340–383, 2015. 4, 5

[38] Hao Huang. Induced subgraphs of hypercubes and a proof of the sensitivity conjecture. *Annals of Mathematics*, 190(3):949–955, 2019. 14

[39] Russell Impagliazzo, Pavel Pudlák, and Jiří Sgall. Lower bounds for the polynomial calculus and the Gröbner basis algorithm. *Computational Complexity*, 8(2):127–144, 1999. 3, 8, 30

[40] Russell Impagliazzo and Nathan Segerlind. Counting axioms do not polynomially simulate counting gates. In *42nd Annual Symposium on Foundations of Computer Science, FOCS 2001, 14-17 October 2001, Las Vegas, Nevada, USA*, pages 200–209. IEEE Computer Society, 2001. 7, 24

[41] Dmitry Itsykson and Dmitry Sokolov. Resolution over linear equations modulo two. *Ann. Pure Appl. Log.*, 171(1), 2020. Extended abstract appeared initially in MFCS 2014. 9

[42] Emil Jeřábek. Dual weak pigeonhole principle, Boolean complexity, and derandomization. *Ann. Pure Appl. Log.*, 129(1-3):1–37, 2004. 3, 13, 15, 60

[43] Emil Jeřábek. *Weak pigeonhole principle, and randomized computation*. PhD thesis, Faculty of Mathematics and Physics, Charles University, Prague, 2005. 3, 13, 82

[44] Emil Jeřábek. Approximate counting in bounded arithmetic. *Journal of Symbolic Logic*, 72(3):959–993, 2007. 3, 13, 14, 15

[45] Eitetsu Ken. On some Σ_0^B-formulae generalizing counting principles over V^0. *Archive for Mathematical Logic*, 64(1-2):117–158, 2024. 7, 24

[46] Erfan Khaniki. Nisan-Wigderson generators in proof complexity: New lower bounds. In *37th Computational Complexity Conference (CCC 2022)*, volume 234 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 17:1–17:24, 2022. 7

[47] J. Krajíček. *Proof Complexity*. Encyclopedia of Mathematics and its Applications. Cambridge University Press, 2019. 9

[48] Jan Krajíček. *Bounded arithmetic, propositional logic, and complexity theory*, volume 60 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, 1995. 3, 8, 30

[49] Jan Krajíček. On the weak pigeonhole principle. *Fund. Math.*, 170(1-2):123–140, 2001. 3, 12, 15

[50] Jan Krajíček. Dual weak pigeonhole principle, pseudo-surjective functions, and provability of circuit lower bounds. *The Journal of Symbolic Logic*, 69(1):265–286, 2004. 3, 6, 12, 15, 21, 39, 40

[51] Jan Krajíček, Pavel Pudlák, and Alan Woods. An exponential lower bound to the size of bounded depth Frege proofs of the pigeonhole principle. *Random Structures and Algorithms*, 7(1):15–39, 1995. 3

[52] Jan Krajíček. A proof complexity generator. In *Proc. from the 13th International Congress of Logic, Methodology and Philosophy of Science (Beijing, August 2007)*, Studies in Logic and the Foundations of Mathematics. King's College Publications, London, 2009. 4, 6, 21

[53] Jan Krajíček. *Proof Complexity Generators*, volume 497 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, 2025. 3

[54] Alexis Maciel, Toniann Pitassi, and Alan R. Woods. A new proof of the weak pigeonhole principle. *J. Comput. System Sci.*, 64(4):843–872, 2002. 6, 15

[55] Mladen Mikša and Jakob Nordström. A generalized method for proving polynomial calculus degree lower bounds. *J. ACM*, 71(6):37:1–37:43, 2024. 5, 6, 45

[56] Michael Mitzenmacher and Eli Upfal. *Probability and Computing – Randomized Algorithms and Probabilistic Analysis*. Cambridge University Press, 2005. 83, 84

[57] Moritz Müller and Ján Pich. Feasibly constructive proofs of succinct weak circuit lower bounds. *Ann. Pure Appl. Log.*, 171(2), 2020. 13, 15, 81

[58] Noam Nisan. Lower bounds for non-commutative computation. In *Proceedings of the Annual ACM Symposium on the Theory of Computing*, pages 410–418, 1991. 14, 65

[59] Noam Nisan and Avi Wigderson. Hardness vs randomness. *J. Comput. Syst. Sci.*, 49(2):149–167, 1994. Preliminary version appeared in IEEE Annual Symposium on Foundations of Computer Science 1988. 6, 21

[60] J. Paris and A. Wilkie. Counting problems in bounded arithmetic. In *Methods in mathematical logic (Caracas, 1983)*, volume 1130 of *Lecture Notes in Math.*, pages 317–340. Springer, Berlin, 1985. 19

[61] J. Paris, A. J. Wilkie, and A. Woods. Provability of the pigeonhole principle and the existence of infinitely many primes. *Journal of Symbolic Logic*, 53(4):1235–1244, 1988. 3, 15, 60

[62] Fedor Part and Iddo Tzameret. Resolution with counting: Dag-like lower bounds and different moduli. *Comput. Complex.*, 30(1):2, 2021. 9

[63] Toniann Pitassi, Paul Beame, and Russell Impagliazzo. Exponential lower bounds for the pigeonhole principle. *Comput. Complexity*, 3(2):97–140, 1993. 3

[64] Toniann Pitassi, Benjamin Rossman, Rocco A. Servedio, and Li-Yang Tan. Poly-logarithmic Frege depth lower bounds via an expander switching lemma. In *Proceedings of the Forty-Eighth Annual ACM Symposium on Theory of Computing*, page 644–657, New York, NY, USA, 2016. Association for Computing Machinery. 9

[65] Ran Raz. Resolution lower bounds for the weak pigeonhole principle. *J. ACM*, 51(2):115–138, 2004. 3, 4, 5, 6, 13

[66] Ran Raz and Iddo Tzameret. Resolution over linear equations and multilinear proofs. *Ann. Pure Appl. Logic*, 155(3):194–224, 2008. 7

[67] Alexander A. Razborov. Lower bounds on the size of bounded depth circuits over a complete basis with logical addition. *Mathematical Notes of the Academy of Sciences of the USSR*, 41(4):333–338, 1987. 75

[68] Alexander A. Razborov. Bounded arithmetic and lower bounds in Boolean complexity. In *Feasible Mathematics II. Progress in Computer Science and Applied Logic*, volume 13, pages 344–86. Birkhäuser, 1995. 15

[69] Alexander A. Razborov. Lower bounds for the polynomial calculus. *Comput. Complexity*, 7(4):291–324, 1998. 3, 4, 10, 13, 19, 31, 38, 65, 67

[70] Alexander A. Razborov. Improved resolution lower bounds for the weak pigeonhole principle. *Electronic Colloquium on Computational Complexity (ECCC)*, 8(55), 2001. ECCC TR01-055. 5

[71] Alexander A. Razborov. Proof complexity of pigeonhole principles. In *Developments in language theory (Vienna, 2001)*, volume 2295 of *Lecture Notes in Comput. Sci.*, pages 110–116. Springer, Berlin, 2002. 3, 5

[72] Alexander A. Razborov. Resolution lower bounds for perfect matching principles. *J. Comput. Syst. Sci.*, 69(1):3–27, 2004. 5, 13, 65, 67

[73] Alexander A. Razborov. Pseudorandom generators hard for k-DNF resolution and polynomial calculus resolution. *Annals of Mathematics*, 181:415–472, 2015. 3, 6, 8, 10, 11, 12, 13, 14, 15, 21, 30, 39, 40, 67, 71, 83, 84

[74] Grant Schoenebeck. Linear level Lasserre lower bounds for certain k-CSPs. In *49th Annual IEEE Symposium on Foundations of Computer Science, FOCS 2008, October 25-28, 2008, Philadelphia, PA, USA*, pages 593–602. IEEE Computer Society, 2008. 12, 30

[75] Roman Smolensky. Algebraic methods in the theory of lower bounds for Boolean circuit complexity. In *Proceedings of the Annual ACM Symposium on the Theory of Computing*, pages 77–82, 1987. 14, 15, 72

[76] Dmitry Sokolov. Pseudorandom generators, resolution and heavy width. In Shachar Lovett, editor, *37th Computational Complexity Conference, CCC 2022, July 20-23, 2022, Philadelphia, PA, USA*, volume 234 of *LIPIcs*, pages 15:1–15:22. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2022. 3, 7

[77] Michael Soltys and Stephen Cook. The proof complexity of linear algebra. *Ann. Pure Appl. Logic*, 130(1-3):277–323, 2004. 4, 5, 14

[78] Michael Soltys and Alasdair Urquhart. Matrix identities and the pigeonhole principle. *Arch. Math. Log.*, 43(3):351–358, 2004. 4, 5, 8, 30

[79] Neil Thapen. A model-theoretic characterization of the weak pigeonhold principle. *Ann. Pure Appl. Log.*, 118(1-2):175–195, 2002. 3

[80] Neil Thapen. *The weak pigeonhole principle in models of bounded arithmetic*. PhD thesis, University of Oxford, 2002. 60

[81] Iddo Tzameret and Stephen A. Cook. Uniform, integral, and feasible proofs for the determinant identities. *J. ACM*, 68(2):12:1–12:80, 2021. 4, 14

[82] A. Woods. *Some problems in logic and number theory, and their connections*. PhD thesis, University of Manchester, 1981. 14. 3