A Rank Lower Bound for Cutting Planes Proofs of Ramsey's Theorem

MASSIMO LAURIA, Universitat Politécnica de Catalunya, Barcelona, Spain

Ramsey's Theorem is a cornerstone of combinatorics and logic. In its simplest formulation it says that for every $k > 0$ and $s > 0$, there is a minimum number $r(k, s)$ such that any simple graph with at least $r(k, s)$ vertices contains either a clique of size k or an independent set of size s. We study the complexity of proving upper bounds for the number $r(k, k)$. In particular, we focus on the propositional proof system cutting planes; we show that any cutting plane proof of the upper bound "$r(k, k) \leq 4^k$" requires high rank. In order to do that we show a protection lemma which could be of independent interest.

CCS Concepts: • **Theory of computation** → **Proof complexity**; • **Mathematics of computing** → *Combinatoric problems;*

Additional Key Words and Phrases: Proof complexity, cutting planes, Ramsey theory, rank, integer programming

ACM Reference Format:
Massimo Lauria. 2016. A rank lower bound for cutting planes proofs of Ramsey's theorem. ACM Trans. Comput. Theory 8, 4, Article 17 (June 2016), 13 pages.
DOI: http://dx.doi.org/10.1145/2903266

1. INTRODUCTION

Ramsey's Theorem for simple graphs claims that if a graph is big enough, then it has either a clique or an independent set of moderate size. To be more specific, for any k and s there is a number $r(k, s)$ that is the smallest such that *any graph* with at least $r(k, s)$ vertices contains either a clique of size k or an independent set of size s.

Discovering the actual value of $r(k, s)$ is challenging, and so far only few cases have been computed exactly. For this reason, there is great interest in asymptotic estimates. Regarding upper bounds, Erdős and Szekeres [1987] show that

$$r(k, s) \leq \binom{k+s-2}{k-1}. \tag{1}$$

Furthermore, Erdős [1947] considers the case of diagonal Ramsey numbers (i.e., when $k = s$) and gets the lower bound

$$r(k, k) \geq (1 + o(1))\frac{k}{\sqrt{2}e}2^{k/2} \tag{2}$$

The author did most of this work at the Math Institute of the Czech Academy of Science, funded by the Eduard Čech Center. While finalizing the article, the author was supported by the European Research Council under the European Union's Seventh Framework Programme (FP7/2007–2013)/ERC Grant No. 279611.
This is a revised and expanded version of the paper [Lauria 2013], which appeared in *Proceedings of the 16th international conference on the Theory and Applications of Satisfiability Testing — SAT 2013*.
Author's address: M. Lauria Universitat Politècnica de Catalunya, Dept. Ciències de la Computació c/ Jordi Girona, 1–3 08034 Barcelona, Catalonia, Spain; email: lauria@cs.upc.edu.

DOI: http://dx.doi.org/10.1145/2903266

as one of the first applications of his probabilistic method. Of course there have been some improvements since. To the author's knowledge, the current state of the art regarding diagonal numbers $r(k,k)$ is represented by a lower bound of Spencer [1977] and an upper bound of Conlon [2009].

For the off-diagonal Ramsey numbers (i.e., $r(k,s)$ for $k \neq s$) the state of the art is the lower bound by Bohman and Keevash [2010] and the upper bound by Ajtai et al. [1980]. The maximally unbalanced numbers $r(3,t)$ got further attention in Kim [1995] and Ajtai et al. [1980].

The study of Ramsey's Theorem in proof theory is well established in literature. In bounded arithmetic there are articles attempting to classify the power of a theory in comparison with Ramsey Theorem. It is also considered a good candidate for separating low levels of bounded depth Frege proof systems [Pudlák 1991].

A propositional statement of the form "$r(k,k) \leq N$" become easier to prove as N increases. In particular, if $m = r(k,k)$ then the statement "$r(k,k) \leq m$" is the hardest possible and, indeed, Krishnamurthy and Moll [1981] proposed it as a candidate hard formula. They also proved a lower bound on the *width* of the clauses appearing in its resolution refutations. Later, Krajíček proved an exponential lowerbound on the length of bounded depth Frege proofs for the same statement [Krajíček 2011].

Proving a weaker bound should be easier. Indeed it is possible to give a short proof that "$r(k,k) \leq 4^k$" in a relatively weak fragment of sequent calculus (namely, where we just allow formulas of constant depth in the proof) [Pudlák 1991; Krajíček 2011]. It is not clear how strong the proof system must be in order to prove efficiently this statement. Recently, Pudlák has shown that the length of a resolution proof of "$r(k,k) \leq 4^k$" must be exponential in the length of the formula itself (see Pudlák [2012]). The propositional complexity of off-diagonal Ramsey upper bounds has received less attention, and the only known results are from Carlucci et al. [2011].

In the context of proof complexity research, cutting planes is one of the most studied proof systems after resolution, so it is natural to ask whether Ramsey's Theorem is hard for it. Cutting planes has been originally introduced as a technique to solve integer programs (see Gomory [1958] and Chvátal [1973]). The idea is use an efficient method to search for an optimum feasible point (e.g., the simplex method). If such point is not integer, then we can "round" (and therefore strengthen) some inequality that holds for the set of feasible solutions so that after the rounding the fractional point is not a feasible solution anymore.

Cutting planes was later proposed as a proof system [Cook et al. 1987]. Indeed, it is possible to view the previous process as a sequence of inferences: A new inequality is either a positive combination or a rounding of previously derived inequalities. Another way to describe the rounding rule is the following: If the inequality $\sum_i a_i x_i \leq A$ is valid and all a_i are integers divisible by c, then any integer solution would also satisfy $\sum_i \frac{a_i}{c} x_i \leq \left\lfloor \frac{A}{c} \right\rfloor$. By comparison, the latter inequality is not valid for fractional solutions unless $\frac{A}{c}$ is integer.

Studying the length of proofs in cutting planes is a way to study the running time for integer linear programming solvers based on the rounding rule. Unfortunately, this seems to be difficult. The only lower bound known for *unrestricted* cutting planes refutations is due to Pudlák [1997], and it deals with a relatively artificial formula. Lower bounds for cutting plane proofs of restricted forms existed before (e.g., when the numeric coefficients are small [Bonet et al. 1997] or when the proof is treelike [Impagliazzo et al. 1994]). In another restricted form of cutting planes every proof line has small "degree of falsity" (a complexity measure introduced in Goerdt [1992]). If the degree of falsity is sufficiently small, then the proof system has a sub-exponential simulation in resolution [Hirsch and Nikolenko 2005]. This implies that most strong

resolution lower bounds generalize to this limited version of cutting planes. In particular, this is true for Pudlák [2012].

Even if Ramsey's Theorem is likely to be a difficult formula for cutting planes, proof length lower bounds are out of reach for the current techniques. Hence, we focus on the "rank" of a refutation, that is, the depth (in terms of applications of the rounding rule) of the refutation. The focus on auxiliary complexity measures is not new in proof complexity, and it is not limited to cutting planes. Well-known examples are "width" in resolution, "degree" in polynomial calculus, and "rank" in geometric proof systems like Lovász-Schrijver and sums-of-squares. These measures relate with the actual proof length, in the sense that there are proof search algorithms that run in time $n^{O(r)}$ on formulas with n variables and measure r. Indeed, Chvátal et al. [1989] prove that under some technical conditions if there is a cutting planes proof of rank r then there is one of size $n^{O(r)}$. For further information about cutting planes refutations and the notion of rank (also called Chvátal rank), we refer to Jukna [2012, Chapter 19].

In this article we are going to prove that Ramsey's Theorem requires rank $\Omega(2^{k/2})$. The result does not follow from the classical protection lemma for cutting planes [Buresh-Oppenheim et al. 2006, Lemma 3.1], so we prove a different one that could be of independent interest.

The rest of the article has the following structure. In Section 2 we give necessary preliminaries: We formally introduce the cutting planes proof system in Section 2.1, we describe the integer inequalities encoding Ramsey's Theorem in Section 2.2, and we define the rank of a cutting planes proof in Section 2.3. In Section 3 we give the proof of the main theorem (Theorem 3.6), and in Section 4 we discuss improvements and related open problems.

2. PRELIMINARIES

2.1. Cutting Planes Proof System

Cutting planes is a technique to solve mixed integer linear programs. In this article we consider an inference system for refuting unsatisfiable CNFs that is based on cutting planes. We encode propositional clauses as affine inequalities that have 0–1 solutions if and only if the corresponding assignments satisfy the original clauses. A clause $\vee_i l_i$ translates to the inequality $\sum_i f_i \geq 1$ where

$$f_i = \begin{cases} x & \text{if } l_i = x \\ 1 - x & \text{if } l_i = \neg x. \end{cases} \tag{3}$$

For example, the clause

$$\neg x \vee y \vee \neg z \tag{4}$$

translates as

$$-x + y - z \geq -1 \tag{5}$$

after summing the constant terms.

A proof that there are no integer solutions for such a linear program is a refutation of the corresponding CNF. The linear program that we use to encode the CNF does not take into account the fact that we just care about integer solutions. Indeed, the initial polyhedron contains fractional solutions that we want to ignore. We do that by adding inequalities that preserve integer solutions but remove fractional ones. In this way, we get a *proof system* for the UNSAT language, defined using the means of cutting planes.

A proof system for UNSAT is a polynomial time machine P that has in input a CNF ϕ and a candidate refutation Π. If the formula ϕ is unsatisfiable, then there must be

some refutation Π for which $P(\phi, \Pi)$ accepts. If ϕ is satisfiable, then P does not accept any pair (ϕ, Π).

The study of proof systems was initially motivated by the fact that **NP** is the class of languages with short proof of membership. So in order to separate **NP** from **coNP**, we may show that all proof systems for UNSAT require super-polynomial length refutations for some formulas.

Proving lower bounds on the length of proofs, even if we restrict to interesting (and powerful) textbook proof systems like Frege and Extended Frege, seems extremely difficult. Nowadays, a lot of research focuses on the (much weaker) proof systems that model actual SAT solvers, automatic theorem provers and algorithms for combinatorial optimization. Here the study of the refutation complexity usually gives insight on the performance of such algorithms. In particular, most of these algorithms use heuristics to solve what computer science considers hard problems; a proof system has a nondeterministic nature, so it models the best-possible heuristic, and any lower bound on (for example) proof length usually translates to a lower bound on the running time of all algorithms that fit the model.

A refutation in cutting planes (as defined in Cook et al. [1987]) is an inference process that starts with the inequalities encoding the CNF and ends with a false inequality $1 \leq 0$. We have inference rules

$$\frac{a^T \cdot x \leq A \qquad b^T \cdot x \leq B}{(\alpha a + \beta b)^T \cdot x \leq (\alpha A + \beta B)} \quad \text{(Positive linear combination)} \tag{6}$$

for any non-negative integer α, β, and

$$\frac{(ca)^T \cdot x \leq A}{a^T \cdot x \leq \left\lfloor \frac{A}{c} \right\rfloor} \quad \text{(Integer division with rounding).} \tag{7}$$

Observe that all the coefficients of any derived inequality are integer. Positive linear combination is clearly sound. Integer division with rounding is only sound on integer solutions. The rule says that if the integer coefficients of the variables have a common factor c, then dividing everything by c keeps the left side of the inequality to be integer. Thus it is possible to strengthen the right side to the closest integer. Cutting planes is complete for propositional refutations, since it is easy to transform a resolution refutation of a CNF into a cutting planes refutation of the same CNF. It is a little bit more tricky to see that cutting planes can actually refute any incompatible system of integer inequalities [Chvátal 1973].

2.2. Ramsey Statement

Informally, the classical "Ramsey's Theorem" claims that any big-enough structure, however complicated, contains an instance of a regular substrucure. A specific instance of Ramsey's theorem for graphs claims that for any two numbers k and s there is an minimum integer number $r(k, s)$ such that any graph with $r(k, s)$ vertices has either a clique of size k or an independent set of size s. Erdős and Szekeres [1987] prove that $r(k, k) \leq 4^k$ or, equivalently, that any graph with n vertices has either a clique or an independent set of size $\left\lceil \frac{\log n}{2} \right\rceil$.

THEOREM 2.1 ([ERDŐS AND SZEKERES 1987]). *Any graph with* $\binom{k+s-2}{k-1}$ *vertices has either a clique of size k or an independent set of size s.*

COROLLARY 2.2. *Any graph with* 4^k *vertices has either a clique or an independent set of size k.*

We study cutting planes proofs of this latter corollary. Actually, we study refutations of its negation, encoded as a CNF. For any unordered pair of vertices $\{i, j\}$ we indifferently denote by either $x_{i,j}$ or $x_{j,i}$ the propositional variable whose intended meaning is that an edge connects vertices i and j. Let U be a set of vertices; we have two types of clauses,

$$\mathsf{NoCli}(U) := \bigvee_{\{i,j\}\in\binom{U}{2}} \neg x_{i,j}, \tag{8}$$

$$\mathsf{NoInd}(U) := \bigvee_{\{i,j\}\in\binom{U}{2}} x_{i,j}. \tag{9}$$

We encode "$r(k,k) > 4^k$" as the following CNF, which has $\binom{4^k}{2}$ variables and $2\binom{4^k}{k}$ clauses of width $\binom{k}{2}$,

$$\textsc{Ram}_k := \left(\bigwedge_{U\in\binom{[4^k]}{k}} \mathsf{NoCli}(U)\right) \wedge \left(\bigwedge_{U\in\binom{[4^k]}{k}} \mathsf{NoInd}(U)\right). \tag{10}$$

In cutting planes refutations the clauses are represented as

$$\mathsf{NoCli}(U): \sum_{\{i,j\}\in\binom{U}{2}} x_{i,j} \le \binom{k}{2} - 1, \tag{11}$$

$$\mathsf{NoInd}(U): \sum_{\{i,j\}\in\binom{U}{2}} x_{i,j} \ge 1, \tag{12}$$

which can be succinctly represented as

$$1 \le \sum_{\{i,j\}\in\binom{U}{2}} x_{i,j} \le \binom{k}{2} - 1. \tag{13}$$

In the rest of the article we express every quantity as a function of k. To get a picture on the proof complexity of this formula it is useful to state it at least once in term of the number n of vertices in the graph. This is customary for propositional formulas related to graph theory. Here $n = 4^k$: The formula has $\Theta(n^2)$ variables and $n^{\Theta(\log n)}$ clauses of width $\Theta(\log n)$, so it has quasi-polynomial length with respect to the number of variables. In Theorem 3.6 we will show that its rank is $\Omega(\sqrt[4]{n})$.

2.3. The Rank of a Cutting Planes Refutation

We shall now proceed to describe the Chvátal rank, which is a complexity measure for cutting planes. Other geometric proof systems, with their specific inference rules, have similar notions of rank. In this article we only discuss cutting planes proof, and, therefore, we will use the term generic term rank to refer to Chvátal rank.

Definition 2.3 (*Chvátal Rank*). Consider a cutting planes derivation. All initial inequalities have rank 0. The rank of a proof line obtained applying the "positive linear combination" rule to two lines of rank r_1 and r_2 is $\max\{r_1, r_2\}$. The rank of a proof line obtained from a line of rank r using the "integer division and rounding" rule is $r + 1$.

The rank of a derivation is the largest among the rank of its proof lines. The rank of an integer inequality is the smallest rank among all derivations of that inequality, from the initial system. The rank of an unsatisfiable system of inequalities is the minimum rank needed to derive the contradiction.

The notion of rank has a geometric interpretation: A point p has rank r if there is an inequality of rank $r+1$ that is not satisfied by p but p still satisfies all inequalities of rank r. More concretely, we can think of the inequalities as defining a chain of polyhedrons $P_0 \supseteq \ldots \supseteq P_i \supseteq \ldots \supseteq P_I$, where P_i contains all points of rank $\geq i$, and P_I is the convex hull of all integer solutions of the linear program. It is a well-known fact that there is some $r \geq 0$ such that $P_r = P_I$.

To show that the rank of a refutation is at least r is sufficient to show that there is a point in P_r. The basic tool is a *protection lemma*, a type of result that says that a point has rank $r+1$ when there is a set of points of rank r around it, positioned in a certain configuration (a *protection set*).

In particular, it is possible to define a prover-delayer game as follows: Prover challenges the delayer to exhibit a protection set for a point p_0. Delayer either gives up or shows a set S_0. At the next round the prover picks a point $p_1 \in S_0$ and asks again for a protection set. If the Delayer has a strategy to play the game for r rounds, then the point p_0 has rank at least r.

3. A PROTECTION LEMMA FOR FRACTIONAL GRAPHS

The fractional points that we use in this article have a peculiar structure. We use half integral points (i.e., each coordinate is either 0, $\frac{1}{2}$, or 1) to encode partially specified graphs: 0 encodes non-edges, 1 encodes edges, and $\frac{1}{2}$ encodes unspecified edges. Furthermore, we enforce additional structure on the edges with integer values according to the following definition.

Definition 3.1 (*Fractional Graph*). A "fractional graph" on the vertex set V is a pair $G = (V, E)$, where E is a function from $\binom{V}{2}$ to $\{0, \frac{1}{2}, 1\}$. Furthermore, there must exist some $U \subseteq V$ such that for all $\{u, v\}$

$$E(\{u, v\}) = \frac{1}{2} \text{ if and only if } \{u, v\} \not\subseteq U.$$

We say that G is integral on the vertex set U, which is called the *integral part* of G.

Observe that the integral part of a fractional graph is unique. A fractional graph is a half-integral point in the space $[0, 1]^{\binom{V}{2}}$, and therefore the notion of rank applies.

Remark on notation: we use $x_{i,j}$ to denote the variables referring to edges, and we denote an inequality by "$a \cdot x \leq b$" or "$ax \leq b$." We denote by G both the fractional graph and the corresponding point in $[0, 1]^{\binom{V}{2}}$. Indeed, for a fractional graph $G = (V, E)$ the notation "$a \cdot G$" indicates the expression

$$\sum_{\{u,v\} \in \binom{V}{2}} a_{u,v} E(\{u, v\}).$$

We can make convex combinations of fractional graphs and still get a point in $[0, 1]^{\binom{V}{2}}$. For this article we just need the average between two graphs.

Definition 3.2 (*Graph Average*). Given two fractional graphs $G_1 = (V, E_1)$ and $G_2 = (V, E_2)$, we consider the average of them (denoted as $\frac{1}{2}G_1 + \frac{1}{2}G_2$) to be the point $H = \left(V, \frac{E_1+E_2}{2}\right)$.

The average of two fractional graphs is not necessarily a fractional graph according to our definition. It is under the conditions enforced by the definition of protection sets.

Definition 3.3 (*Protection Set*). Consider a fractional graph G which is integral on the vertices in I. A protection set for G is a set of graph pairs $(G'_{\{u,v\}}, G''_{\{u,v\}})$, one pair for each two distinct vertices $u \notin I$ and $v \notin I$, such that for any such pair

—both $G'_{\{u,v\}}$ and $G''_{\{u,v\}}$ are integral on $I \cup \{u, v\}$;
—$G = \frac{1}{2}G'_{\{u,v\}} + \frac{1}{2}G''_{\{u,v\}}$.

Notice that the protection set does not have a graph pair for vertices $\{u, v\}$, when $u \in I$ and $v \notin I$. A point p in $[0, 1]^{\binom{V}{2}}$ is an alternative representation of a fractional graph $G = (V, E)$ when each coordinate $p_{a,b}$ is equal to $E(\{a, b\})$.[1] The following simple lemma highlights the peculiar structure of a protection set for G.

Lemma 3.4. *Consider a graph G with integral part I and choose a pair $\left(G'_{\{u,v\}}, G''_{\{u,v\}}\right)$ from some protection set for G. Let p, p', p'' be the points representing $G, G'_{\{u,v\}}, G''_{\{u,v\}}$, respectively. The following holds:*

(1) for any $\{a, b\} \subseteq I$, $p_{a,b} = p'_{a,b} = p''_{a,b}$;
(2) for any $\{a, b\} \nsubseteq I$ and $\{a, b\} \subseteq I \cup \{u, v\}$, $p_{a,b} = \frac{1}{2}$ and $p'_{a,b} = 1 - p''_{a,b}$.

Proof. Point (1) holds because edge $\{a, b\}$ is in the integral part: $p_{a,b}$ must be integer and equal to $\frac{p'_{a,b}+p''_{a,b}}{2}$, so the values of $p'_{a,b}$ and $p''_{a,b}$ must be equal to $p_{a,b}$; to prove (2) notice that $\{a, b\} \nsubseteq I$ immediately implies that $p_{a,b} = \frac{1}{2}$. Both $G'_{\{u,v\}}$ and $G''_{\{u,v\}}$ have integral edge $\{a, b\}$, so the values $p'_{a,b}$, $p''_{a,b}$ must be opposite in order to average to $\frac{1}{2}$. □

The following protection lemma for fractional graphs shows that the definition of protection set is useful to get rank lower bounds. Our protection lemma differs from the ones in the literature. In those constructions the new integer coordinates must be disjoint and set independently (see Buresh-Oppenheim et al. [2006]). Here this is not needed, and, hence, we can use protection sets made by fractional graphs.

We now focus on the sequence of polytopes $[0, 1]^{\binom{V}{2}} \supseteq P_0 \supseteq P_1 \supseteq \cdots \supseteq P_i \supseteq \cdots$, where P_i is the set of points of rank at least i.

Lemma 3.5 (Protection Lemma). *Let G be a fractional graph with an even number of vertices and an integral part of even size. If G has a protection set where all graphs in all graph pairs are in P_i, then G is in P_{i+1}.*

Proof. The fractional graph G is the average of two points in P_i by construction, so $G \in P_i$ as well. Assume, by contradiction, that $G \notin P_{i+1}$; it then holds that $a \cdot G > b$ where $ax \leq b$ is an inequality of rank $i + 1$. We can derive such inequality by integer division from an inequality $a'x \leq b'$ of rank i, where

$$a'_{u,v} = qa_{u,v} \qquad b' = qb + r \qquad \text{for some } q, r \in \mathbb{Z} \text{ with } 0 < r < q. \tag{14}$$

Since $G \in P_i$ we have $a' \cdot G \leq b' < q(b + 1)$. Putting it all together we have that $b < a \cdot G < b + 1$.

Fix I to be the integral vertices of G and fix J to be $V(G)\backslash I$.

The value of $a \cdot G$ is strictly less than $b + 1$ but it is strictly larger than b, so it must be $b + \frac{1}{2}$ because G is half-integral and the coefficient vector a is integral. This means

[1]For every point p in $[0, 1]^{\binom{V}{2}}$ and pair $\{a, b\} \in \binom{V}{2}$, we denote the corresponding coordinate in p both as $p_{a,b}$ or $p_{b,a}$.

that the sum of the coefficients of the variables with value $\frac{1}{2}$ must be odd. Namely,

$$\sum_{\{u,v\}\in\binom{J}{2}} a_{u,v} + \sum_{u\in J, w\in I} a_{u,w} \equiv 1 \pmod 2, \tag{15}$$

because otherwise $a \cdot G$ would be integral. Equation (15) implies the following claim that we prove later.

Claim 1. *There is at least one pair $\{u, v\} \subseteq J$ for which*

$$a_{u,v} + \sum_{w\in I} a_{u,w} + \sum_{w\in I} a_{v,w} \equiv 1 \pmod 2. \tag{16}$$

We pick $\{u, v\}$ as in Claim 1. We write $a \cdot G$ as the sum of three contributions: the sum over the integral edges of G, the sum over the edges enumerated in Equation (16) for the chosen pair $\{u, v\}$, and the sum over the rest of the edges. Let us call these sums A, B, and C respectively: Clearly, $A + B + C = b + \frac{1}{2}$. All edges in G corresponding to the sum B have value $\frac{1}{2}$, so by Equation (16) B is half integral, and, furthermore, $A + C$ is an integer.

Consider the pair of graphs $\left(G'_{\{u,v\}}, G''_{\{u,v\}}\right)$ in the protection set. By definition, the two graphs must differ from G *only* on the edges which coefficients are in the summation (16), thus $a \cdot G'_{\{u,v\}} = A + B' + C$ and $a \cdot G''_{\{u,v\}} = A + B'' + C$ for some B' and B''. On these edges the two graphs have integral values, so B' and B'' are integers. Hence, numbers $a \cdot G'_{\{u,v\}}$ and $a \cdot G''_{\{u,v\}}$ are integral, too. Being the two graphs in P_i, these numbers are strictly smaller than $b + 1$. Hence,

$$a \cdot G = \frac{1}{2} a \cdot G'_{\{u,v\}} + \frac{1}{2} a \cdot G'_{\{u,v\}} \leq b, \tag{17}$$

which contradicts the hypothesis that $G \notin P_{i+1}$. □

Proof of Claim 1. We denote $b_u := \sum_{w\in I} a_{u,w}$ for all $u \in J$, so Equations (16) can be rewritten as

$$a_{u,v} + b_u + b_v \equiv 1 \pmod 2. \tag{18}$$

We partition J into two classes, $J_0 = \{u \in J : b_u \equiv 0 \pmod 2\}$ and $J_1 = \{u \in J : b_u \equiv 1 \pmod 2\}$. Notice that

$$\sum_{u\in J, w\in I} a_{u,w} \equiv \sum_{u\in J_0} b_u + \sum_{u\in J_1} b_u \equiv |J_1| \pmod 2. \tag{19}$$

Assume that Equation (18) does not hold for any pair of vertices in J. It follows that $a_{u,v} \equiv 1 \pmod 2$ if and only if $\{u, v\}$ intersects both J_0 and J_1, therefore

$$\sum_{\{u,v\}\in\binom{J}{2}} a_{u,v} \equiv |J_0||J_1| \pmod 2, \tag{20}$$

and we can rewrite Equation (15) using Equtions (19) and (20) to get

$$1 \equiv \sum_{\{u,v\}\in\binom{J}{2}} a_{u,v} + \sum_{u\in J} b_u \equiv |J_0||J_1| + |J_1| \pmod 2, \tag{21}$$

which leads to a contradiction: $|J|$ is even and, therefore, $|J_0||J_1| + |J_1|$ is even, too. □

We are now ready to prove the lower bound on rank of cutting planes proof of the Ramsey number upper bound.

THEOREM 3.6. *For all even $k \geq 4$, cutting planes rank of formula* RAM_k *is at least* $2^{k/2-1}$.

PROOF. Consider the following prover-delayer game:

—**Initial choice** (round 0): let P_0 be the polytope described by the linear system of RAM_k, and let G_0 be the fractional graph with empty integral part (i.e., all edges have value $\frac{1}{2}$).
—**Delayer choice** (round $i > 0$): Delayer shows a protection set for G_{i-1} contained in P_0.
—**Prover choice** (round $i > 0$): Prover sets G_i to be an arbitrary element of an arbitrary pair in the protection set of G_{i-1} shown by Delayer.

For $k \geq 4$, fractional graph G_0 satisfies inequalities (13), and thus it is a point of the initial polytope P_0.

We now argue that if Delayer has a strategy for playing until round $2^{k/2-1}$ no matter how Prover chooses, then G_0 has rank at least $2^{k/2-1}$. Consider the tree of all possible games played by this Delayer against any possible Prover, so the branching from level $i-1$ to level $i \leq 2^{k/2-1}$ corresponds to the Prover's decision of which the graph in the protection set of G_{i-1} is picked to be G_i, and each node of the tree at level i corresponds to the specific value of G_i obtained so far.

Every path in this tree has length at least $2^{k/2-1}$, and all the children of the fractional graph corresponding to an internal node of the tree form a protection set for it. Lemma 3.5 immediately implies that the fractional graphs at level i are contained in $P_{2^{k/2-1}-i}$, and in particular that G_0 is in $P_{2^{k/2-1}}$. Therefore to prove the theorem it is sufficient to show a strategy for Delayer for playing up to round $2^{k/2-1}$.

At each step i in the prover-delayer game, G_i is a fractional graph with an integral part of $2i$ vertices, since each application of Lemma 3.5 adds exactly two vertices. Furthermore, at each step we keep a bijection σ_i between the integral part of G_i and $\{1, \ldots, 2i\}$.

We are going to build the protection sets using a model graph H on vertex set $\{1, \ldots, 2^{k/2}\}$. The indicator variable $h_{u,v}$ is either 1 if $\{u, v\} \in E(H)$ or 0 otherwise. We call "diagonal pair" any pair of the form $\{2i-1, 2i\}$ for some $i \in [2^{k/2-1}]$. We want H to have the properties stated in the following claim.

CLAIM 2. *There exists a graph H on vertex set $\{1, \ldots, 2^{k/2}\}$ such that*

—*H has neither a clique nor an independent set of size k;*
—*the previous property holds for every H' obtained from H by arbitrarily adding and removing diagonal edges;*
—*given any diagonal pair $\{2i-1, 2i\}$ and any vertex $a < 2i-1$, it holds that*

$$h_{a,(2i-1)} = 1 - h_{a,2i}. \tag{22}$$

This graph H must have $2^{k/2}$ vertices, so the fact that it has no clique and no independent set of size k does not necessarily violate Ramsey's Theorem. Indeed, we will show later that such graph H exists.

Delayer strategy: Delayer uses such H to define the strategy against Prover. The main idea is that at each round Delayer picks a new diagonal pair of vertices in H. The integral part of each G_i in the trace of the game is almost a copy of the graph induced by the vertices $\{1 \ldots 2i\}$ on H. We say "almost" because the edges on the diagonal pair will be arbitrarily added or removed, depending on the Prover choices. We call σ_i the mapping at round i, and we define σ_0 to be the empty mapping.

At round i we want to show a protection set for G_{i-1}, which has integral part I with $|I| = 2i - 2$. For each u and v not in I, we define the two graphs $G'_{\{u,v\}}$ and $G''_{\{u,v\}}$ by adding $\{u, v\}$ to the integral part in the following way: for every $a \in I$ we set

$$\begin{aligned} p'_{a,u} &:= h_{\sigma_{i-1}(a),(2i-1)} \\ p'_{a,v} &:= h_{\sigma_{i-1}(a),2i} \\ p''_{a,u} &:= h_{\sigma_{i-1}(a),2i} \\ p''_{a,v} &:= h_{\sigma_{i-1}(a),(2i-1)} \\ p'_{u,v} &:= 0 \\ p''_{u,v} &:= 1, \end{aligned}$$

where p, p', p'' are the point representing fractional graphs G_i, $G'_{\{u,v\}}$, and $G''_{\{u,v\}}$, respectively. The other coordinates of p' and p'' are the same as in p. By construction, these graphs form a protection set of G_i, because they satisfy the conditions of Definition 3.3.

After prover choice: Prover can choose either $G'_{\{u,v\}}$ or $G''_{\{u,v\}}$ from the pair corresponding to some edge $\{u, v\}$. If Prover chooses $G'_{\{u,v\}}$, then we extend σ_{i-1} to σ_i by mapping $u \mapsto (2i - 1)$ and $v \mapsto 2i$. Otherwise, we do it by mapping $u \mapsto 2i$ and $v \mapsto (2i - 1)$.

Finally, we show that Delayer can play for $e = 2^{k/2-1}$ rounds. In order to play that many rounds, we need to argue that G_e is contained in P_0 or, equivalently, that it satisfies the bounds in (13). Take an arbitrary set of vertices $K \subseteq V(G_e)$ of size $k \geq 4$: If there is even a single vertex out of the integral part, then the sum in Equation (13) contains at least two half-integral variables and therefore the bounds are satisfied.

If K is contained in the integral part of G_e, then we use that the latter is isomorphic to some H' which is obtained from H by arbitrarily changing the edges on the diagonal pairs. By Claim 2 graph H' does not contain cliques of independent sets of size k, therefore the bounds in (13) are satisfied.

We have proved that $G_e \in P_0$. That means (using Lemma 3.5) that $G_{e-1} \in P_1$, $G_{e-2} \in P_2, \ldots$, and so on until $G_0 \in P_e$. This shows that P_e is not the empty polytope, and that inequality $0 \leq -1$ has rank larger than e. This concludes the proof of the theorem. □

Proof of Claim 2. Consider any $i \leq 2^{k/2-1}$. We sample uniformly independently at random the 0–1 values of $h_{a,(2i-1)}$ for all vertices $a < 2i - 1$, and we set $h_{a,2i} := 1 - h_{a,(2i-1)}$. This definition immediately enforces the third condition of the claim. We get the first and the second condition by probabilistic method: We show that with positive probability any set of vertices of size k contains both an edge and a non-edge that *are not on diagonal pairs*. This is true by construction for any set K containing a diagonal pair $\{2i - 1, 2i\}$ plus some other vertex $a < 2i - 1$. Let $\mathcal{K}_0$ be the family of sets of size k with no diagonal pair and $\mathcal{K}_1$ the family of sets of size k such that the two smallest elements form a diagonal pair. The size of the families are

$$|\mathcal{K}_0| = 2^k \binom{n/2}{k} \qquad |\mathcal{K}_1| = 2^{k-2} \binom{n/2}{k-1}. \tag{23}$$

If $k < 8$, then families $\mathcal{K}_0$ and $\mathcal{K}_1$ are empty, and, hence, graph H has no homogeneous sets of size k by construction. Consider $k \geq 8$. There are $\binom{k}{2}$ independent random edges in sets from $\mathcal{K}_0$ and $\binom{k}{2} - 1$ in sets from $\mathcal{K}_1$. Fix $n = 2^{k/2}$, and notice that n is even. Then

$$\Pr[H \text{ has a homogeneous set of size } k] \leq \sum_{K \in \mathcal{K}} \Pr[K \text{ is homogeneous}] \leq$$
$$\leq |\mathcal{K}_0| \frac{2}{2^{\binom{k}{2}}} + |\mathcal{K}_1| \frac{2}{2^{\binom{k}{2}-1}} \leq \frac{2}{2^{\binom{k}{2}}} \left[2^k \binom{n/2}{k} + 2^{k-1} \binom{n/2}{k-1} \right] < 1, \quad (24)$$

for $n = 2^{k/2}$. □

4. CONCLUSION

We have seen that Ramsey's Theorem requires refutations of large rank. Of course, the actual rank depends on the value of $r(k, k)$ itself: The proof may focus on the first $r(k, k)$ vertices and the corresponding $\binom{r(k,k)}{2}$ edge variables. Thus, in order to improve the rank lower bound, it is necessary to understand better the Ramsey number itself, in particular its lower bounds.

Rank is just an auxiliary complexity measure: The interest of proof complexity revolves around the length of proofs. Unfortunately, there is very little understanding about the length of cutting planes refutations: The only lower bound known is based on the interpolation technique [Pudlák 1997] that only works on formulas with a very peculiar structure. Such a lower bound has been proved by harnessing the connection between cutting planes inferences and monotone computation [Pudlák 1997; Bonet et al. 1995]. It is an open problem how to prove length lower bounds for natural formulas, in particular using combinatorial techniques that allow us to study more general CNFs.

A natural question is whether the rank has a role here. In other proof systems (e.g., resolution and polynomial calculus), a good lower bound on an auxiliary complexity measure implies proof length lower bounds [Ben-Sasson and Wigderson 2001; Impagliazzo et al. 1999]. It is interesting to notice that even if this implication is true, then it must have some limitations, since there are formulas with large rank (i.e., the square root of the number of variables) and small refutations [Buresh-Oppenheim et al. 2006]. The latter also happens in resolution and polynomial calculus (with width and degree complexity measure, respectively. See Bonet and Galesi [2001] and Galesi and Lauria [2010]). Nevertheless, the study of such auxiliary measures led to size lower bounds.

In order to understand the relation between rank and length of cutting planes proof the following question is unavoidable:

OPEN PROBLEM 1. *Is there any k-CNF formula on n variables with polynomial length refutations and cutting planes rank* $\Omega(n)$*?*

As mentioned before, there is a formula on n variables, polynomial length refutation, and rank $\Omega(\sqrt{n})$ (see Buresh-Oppenheim et al. [2006]). Thus, any rank-length connection that holds in general would not be useful to prove a length lower bound for Ramsey's Theorem, given the current knowledge. So even if a useful rank-length relation is discovered, that would not solve the following problem.

OPEN PROBLEM 2. *Does* RAM_k *have a cutting planes refutation of polynomial length?*

For further open problems about cutting planes refutations, we suggest referring to the book by Jukna [2012, Chapter 19].

REFERENCES

Miklós Ajtai, János Komlós, and Endre Szemerédi. 1980. A note on Ramsey numbers. *J. Combin. Theory Ser. A* 29, 3 (1980), 354–360.

Eli Ben-Sasson and Avi Wigderson. 2001. Short proofs are narrow - resolution made simple. *J. ACM* 48, 2 (2001), 149–169.

T. Bohman and P. Keevash. 2010. The early evolution of the H-free process. *Invent. Math.* 181, 2 (2010), 291–336.

Maria Luisa Bonet and Nicola Galesi. 2001. Optimality of size-width tradeoffs for resolution. *Computat. Complex.* 10, 4 (2001), 261–276.

Maria Luisa Bonet, T. Pitassi, and Ran Raz. 1995. Lower bounds for cutting planes proofs with small coefficients. In *Proceedings of the Twenty-Seventh Annual ACM Symposium on Theory of Computing*. ACM, New York, NY, 575–584.

Maria Luisa Bonet, Toniann Pitassi, and Ran Raz. 1997. Lower bounds for cutting planes proofs with small coefficients. *J Symbol. Logic* 62, 3 (1997), pp. 708–728. http://www.jstor.org/stable/2275569.

J. Buresh-Oppenheim, Nicola Galesi, Shlomo Hoory, A. Magen, and Toniann Pitassi. 2006. Rank bounds and integrality gaps for cutting planes procedures. *Theor. Comput.* 2, 4 (2006), 65–90.

Lorenzo Carlucci, Nicola Galesi, and Massimo Lauria. 2011. Paris-Harrington tautologies. In *Proc. of IEEE 26th Conference on Computational Complexity (CCC 2011)*. 93–103.

Vašek Chvátal. 1973. Edmonds polytopes and a hierarchy of combinatorial problems. *Discr. Math.* 4, 4 (1973), 305–337.

Vašek Chvátal, William Cook, and M. Hartmann. 1989. On cutting-plane proofs in combinatorial optimization. *Linear Algeb. Appl.* 114 (1989), 455–499.

D. Conlon. 2009. A new upper bound for diagonal Ramsey numbers. *Ann. Math.* 170, 2 (2009), 941–960.

William Cook, Collette R. Coullard, and György Turán. 1987. On the complexity of cutting-plane proofs. *Discr. Appl. Math.* 18, 1 (1987), 25–38.

Paul Erdős. 1947. Some remarks on the theory of graphs. *Bull. Am. Math. Soc* 53 (1947), 292–294.

Paul Erdős and G. Szekeres. 1987. A combinatorial problem in geometry. In *Classic Papers in Combinatorics*, Ira Gessel and Gian-Carlo Rota (Eds.). Birkhäuser, Boston, 49–56. DOI:http://dx.doi.org/10.1007/978-0-8176-4842-8_3

Nicola Galesi and Massimo Lauria. 2010. Optimality of size-degree tradeoffs for polynomial calculus. *ACM Trans. Comput. Logic* 12, Article 4 (October 2010), 22 pages. Issue 1. DOI:http://dx.doi.org/10.1145/1838552.1838556

Andreas Goerdt. 1992. The cutting plane proof system with bounded degree of falsity. In *Computer Science Logic*, Egon Börger, Gerhard Jäger, Hans Kleine Büning, and MichaelM. Richter (Eds.). Lecture Notes in Computer Science, Vol. 626. Springer, Berlin, 119–133. DOI:http://dx.doi.org/10.1007/BFb0023762

Ralph E. Gomory. 1958. Outline of an algorithm for integer solutions to linear programs. *Bull. Am. Math. Soc.* 64, 5 (1958), 275–278.

Edward A. Hirsch and Sergey I. Nikolenko. 2005. Simulating cutting plane proofs with restricted degree of falsity by resolution. In *Theory and Applications of Satisfiability Testing*, Fahiem Bacchus and Toby Walsh (Eds.). Lecture Notes in Computer Science, Vol. 3569. Springer, Berlin, 135–142. DOI:http://dx.doi.org/10.1007/11499107_10

Russell Impagliazzo, Toniann Pitassi, and Alasdair Urquhart. 1994. Upper and lower bounds for tree-like cutting planes proofs. In *Proceedings of the Symposium on Logic in Computer Science, 1994. LICS'94.* IEEE, 220–228.

Russell Impagliazzo, Pavel Pudlák, and Jiří Sgall. 1999. Lower bounds for the polynomial calculus and the Gröbner basis algorithm. *Comput. Complex.* 8, 2 (1999), 127–144.

Stasys Jukna. 2012. *Boolean Function Complexity: Advances and Frontiers*. Springer-Verlag, Berlin.

Jeong Han Kim. 1995. The Ramsey number $R(3, t)$ has order of magnitude $t^2/\log(t)$. *Random Struct. Algor.* 7, 3 (1995), 173–208.

Jan Krajíček. 2011. A note on propositional proof complexity of some Ramsey-type statements. *Arch. Math. Logic* 50 (2011), 245–255. Issue 1. http://dx.doi.org/10.1007/s00153-010-0212-9.

Balakrishnan Krishnamurthy and Robert N. Moll. 1981. Examples of hard tautologies in the propositional calculus. In *13th ACM Symposium on Th. of Computing (STOC 1981)*. ACM, New York, NY 28–37.

Massimo Lauria. 2013. A rank lower bound for cutting planes proofs of Ramsey theorem. In *Theory and Applications of Satisfiability Testing - SAT 2013*, Matti Jarvisalo and Allen Van Gelder (Eds.). Lecture Notes in Computer Science, Vol. 7962. Springer, Berlin, 351–364. DOI:http://dx.doi.org/10.1007/978-3-642-39071-5_26

Pavel Pudlák. 1991. Ramsey's theorem in bounded arithmetic. In *Proceedings of Computer Science Logic 1990*. 308–317.

Pavel Pudlák. 1997. Lower bounds for resolution and cutting plane proofs and monotone computations. *J. Symbol. Logic* 62, 3 (1997), 981–998.

Pavel Pudlák. 2012. A lower bound on the size of resolution proofs of the Ramsey theorem. *Inf. Process. Lett.* 112, 14–15 (2012), 610–611.

Joel Spencer. 1977. Asymptotic lower bounds for Ramsey functions. *Discr. Math.* 20 (1977), 69–76.

Received July 2015; revised January 2016; accepted April 2016