Electronic Colloquium on Computational Complexity, Report No. 124 (2012)

A rank lower bound for cutting planes proofs of Ramsey Theorem

Massimo Lauria

KTH Royal Institute of Technology
School of Computer Science and Communication
Stockholm, Sweden
lauria@kth.se

Abstract

Ramsey Theorem is a cornerstone of combinatorics and logic. In its simplest formulation it says that there is a function r such that any simple graph with $r(k,s)$ 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 prove that the upper bound "$r(k,k) \leq 4^k$" requires cutting planes proof of high rank. In order to do that we show a protection lemma which could be of independent interest.

1998 ACM Subject Classification F.2.2 Nonnumerical Algorithms and Problems

Keywords and phrases cutting planes, ramsey, proof complexity, rank

1 Introduction

The Ramsey Theorem for simple graphs claims that if a graph is big enough, 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 $r(k,s)$ which 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 is very challenging, and so far only few points have been computed exactly. For this reason there is great interest in asymptotic estimates. Erdős and Szekeres proved in [12] that

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

A lower bound for the diagonal numbers (i.e. $k=s$) was proved by Erdős [11]:

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

as one of the first applications of his probabilistic method. Of course there have been some improvements since: to the author knowledge the current state of the art regarding diagonal numbers $r(k,k)$ is represented by a lower bound of Spencer [23] and an upper bound of Conlon [9].

For the off-diagonal Ramsey numbers (i.e. $r(k,s)$ for $k \neq s$) the state of the art is by Bohman and Keevash (lower bound [3]) and Ajtai, Komlós and Szemerédi (upper bound [1]). Further attention has been devoted to the maximally unbalanced numbers $r(3,t)$ (see [17, 1]).

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

ISSN 1433-8092

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. Krishnamurthy and Moll [19] proposed this statement as a candidate of an hard formula to prove. They also proved a lower bound on the *width* of the clauses appearing in its resolution refutations. Krajíček later proved an exponential lower bound on the length of bounded depth Frege proofs [18], for the same statement.

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, any formula in the proof has bounded depth) [20, 18]. It is not clear how strong the proof system must be in order to prove efficiently this statement. Recently Pudlák has shown that resolution is not enough, proving 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 [22]). The propositional complexity of off-diagonal Ramsey upper bounds has received less attention, and the only known results are from [7].

Cutting plane is the second most popular proof system after resolution, so it is natural to ask whether Ramsey theorem is hard for it. Cutting plane has been originally introduced as a technique to solve integer programs (see [14, 8]). The original idea is to do a canonical linear programming optimization. If the optimum is achieved in a fractional point, it is possible to get an inequality which can be "rounded" in order to remove that point from the set of feasible solutions.

Cutting planes was later proposed as a proof system [10], indeed it is possible to view the previous process as a sequence of inferences: a new inequalities is either as positive combination or as 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 $\sum_i \frac{a_i}{c} x_i \leq \lfloor \frac{A}{c} \rfloor$, which is not valid for fractional solutions if A is fractional.

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 plane refutations is due to Pudlák [21], and it deals with a relatively artificial formula. Ramsey theorem is a natural (an important) statement which is probably difficult for cutting planes. Since length lower bound are so out of reach with the current techniques, we focus on the "rank" of a refutation: that is the depth (in term of rounding rule applications) of the refutation. For further information about cutting planes refutations and the notion of rank (also called Chvátal rank) we suggest the reader to refer to [16, Chapter 19].

In this paper we are going to prove that Ramsey theorem requires rank $\Omega(2^{k/2})$. The result does not follow from the classic protection lemma for cutting planes [6, Lemma 3.1], so we need to prove a different one which could be of independent interest.

The rest of the paper is structured as follows. In Section 2 we give necessary preliminaries: we formally introduce the cutting plane proof system in Section 2.1 and we describe the integer inequalities encoding the Ramsey theorem in Section 2.2. We then define the rank of a cutting plane proof in Section 2.3. In Section 3 we give the proof of the main theorem (Theorem 7), and in Section 4 we discuss about 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 paper we consider an inference system for refuting unsatisfiable CNFs based on such technique. We encode propositional clauses as affine inequalities which have 0–1 solutions if and only if the corresponding assignments satisfy the original clauses. For example the clause

$$\neg x \vee y \vee \neg z$$

translates in

$$-x + y - z \geq -1.$$

After such encoding, any proof that there are no integer solutions for the linear program is a refutation of the corresponding CNF, so we can define a *proof system* for the UNSAT language by the means of cutting planes.

A proof system for UNSAT is a polynomial time machine P which has in input a CNF ϕ and a candidate refutation Π. If the formula ϕ is unsatisfiable 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.

Nowadays the study of proof systems focuses in large part on those systems which model actual SAT solvers, automatic theorem provers and algorithms for combinatorial optimization. This is because the study of complexity measures of the refutation process usually gives insight about 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 nondeterministic nature, so it models the best possible heuristic and any lower bound on (for example) proof length usually translates in a lower bound on the running time of all such algorithms.

A refutation in cutting planes is an inference process which starts with the inequalities encoding the CNF, and ends with a false inequality $1 \leq 0$. Two inference rules are available.

Positive linear combination:

$$\frac{a^T \cdot x \leq A \qquad b^T \cdot x \leq B}{(\alpha a + \beta b)^T \cdot x \leq (\alpha A + \beta B)}$$

for any non negative α, β.

Integer division with rounding:

$$\frac{(c \cdot a)^T \cdot x \leq A}{a^T \cdot x \leq \lfloor \frac{A}{c} \rfloor} .$$

Positive linear combination is sound in general. 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. Such proof system is complete, since it is possible to transform any resolution refutation of a CNF into a cutting plane refutation of the same CNF.

2.2 Ramsey statement

Informally, the classical "Ramsey Theorem" claims that any big enough structure, however complicated, contains an instance of a regular substrucure. A specific instance of Ramsey theorem on graphs claims that for any two numbers k and s there is an 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. In [12] it was proved 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 $\lceil \frac{\log n}{2} \rceil$.

▶ **Theorem 1** (Erdös, Szekeres 1935 [12]). *Any graph with 4^k vertices has either a clique of size k or an independent set of size k.*

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

$$\mathsf{NoCli}(U) := \bigvee_{\{i,j\}\in\binom{U}{2}} \neg x_{i,j} \tag{1}$$

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

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 $\binom{k}{2}$.

$$\textsc{Ram}_k := \left(\bigwedge_{U\in\binom{[4^k]}{k}} \mathsf{NoCli}(U) \right) \wedge \left(\bigwedge_{U\in\binom{[4^k]}{k}} \mathsf{NoInd}(U) \right). \tag{3}$$

In cutting planes refutations the clauses are represented as follows:

$$\mathsf{NoCli}(U): \sum_{\{i,j\}\in\binom{U}{2}} x_{i,j} \leq \binom{k}{2} - 1 \tag{4}$$

$$\mathsf{NoInd}(U): \sum_{\{i,j\}\in\binom{U}{2}} x_{i,j} \geq 1 \tag{5}$$

which can be succinctly represented as

$$1 \leq \sum_{\{i,j\}\in\binom{U}{2}} x_{i,j} \leq \binom{k}{2} - 1. \tag{6}$$

2.3 The rank of a cutting planes refutation

One complexity measure for cutting planes is the "rank" of an inference. Other geometric proof systems, with specific inference rules, have similar notions of rank. The rank of cutting planes proof system is also called Chvátal Rank.

The linear program that we use to encode the CNF does not take in account the fact that we care about in integer solutions only. Indeed the initial polyhedron contains fractional solutions that we want to ignore. We do that by adding further inequalities which are valid on integer solutions but may remove fractional ones. The "integer division with rounding" inference rule is the way employed by cutting planes to add such inequalities. All initial inequalities (and their positive combinations) have rank 0. A line obtained by non negative combination of inequalities of rank r_1 and r_2 have rank $\max\{r_1, r_2\}$. A line obtained from an inequality of rank r using the division rule has rank $r + 1$.

Thus the rank represents the nesting of integer division applications in the refutation. The rank of a refutation is the largest rank among the refutation lines. The rank of an unsatisfiable CNF is the smallest rank among all possible refutations.

The notion of rank has also a geometric interpretation: a point p has rank r if there is an inequality of rank $r + 1$ which is not satisfied by p, and such that p satisfies all inequalities of rank r. More concretely we can think the inequalities to define 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 $r \geq 0$ such that $P_r = P_I$. If the CNF has no solution then $P_I = \emptyset$, and the rank of P_I corresponds to such r.

To show that the rank of a refutation is at least r, is sufficient to show that there is a point in P_r. To do that the only known technique is the use of protection lemmata, which roughly say that if some points in a structured set (called "protection set") have rank i, then another point has rank $i + 1$.

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 will use in this paper have a peculiar structure. We only use half integral points (i.e. each coordinate is either 0, $\frac{1}{2}$, or 1), which in turn is a natural encoding of partially specified graphs: 0 encodes non-edges, 1 encodes edges, $\frac{1}{2}$ encodes unspecified edges. The points we are interested in have additional structure, as described by the following definition.

▶ **Definition 2 (Fractional graph).** A "fractional graph" is a pair $G = (V, E)$ on the vertex set V when E is a function $E : \binom{V}{2} \to \{0, \frac{1}{2}, 1\}$. Consider $U \subseteq V$ such that for all $\{u, v\}$

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

then we say that G is integral on the vertex set U. U is called the integral part of G.

It is clear that a fractional graph is an half-integral point in the space $[0,1]^{\binom{V}{2}}$, thus the notion of rank applies to fractional graphs. The integral part of a fractional graph is unique.

Remark on notation: in the following we use $x_{i,j}$ to denote the variable referring to edges in the graph, and we denote an actual inequality as "$a \cdot x \leq b$" or "$ax \leq b$". We denote as G both the fractional graph and the corresponding point in the space. Indeed for a fractional graph $G = (V, E)$ the notation "$a \cdot G$" indicates the value

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

Fractional graphs are actually vectors with coordinates in $[0, 1]$, so we can make convex combination of them. For this paper we just need the average between two graphs.

▶ **Definition 3 (Graph average).** Given two fractional graph $G_1 = (V, E_1)$ 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 graph $H = (V, \frac{E_1+E_2}{2})$.

The average of two fractional graph is not necessarily a fractional graph according to our definition. It is in the particular conditions that we enforce in the definition of protection sets and in the rest of the paper.

▶ **Definition 4 (Protection set).** Consider a fractional graph G which is integral on vertices I. A protection set for G is a sequence of graph pairs $G'_{\{u,v\}}$ and $G''_{\{u,v\}}$ for any two u, v both outside I such that:

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

The protection set of a graph G has the following peculiar structure.

▶ **Lemma 5.** *Consider a graph G with integral part I and choose a pair $G'_{\{u,v\}}$, $G''_{\{u,v\}}$ from some protection set for G. Let p, p', p'' to be the points representing the $G, G'_{\{u,v\}}, G''_{\{u,v\}}$, respectively. The following hold:*

1. *$p_{a,b} = p'_{a,b} = p''_{a,b}$ for any $\{a, b\} \subseteq I$;*
2. *for any $\{a, b\} \subseteq I \cup \{u, v\}$ with $|\{a, b\} \cap \{u, v\}| > 1$, $p_{a,b} = \frac{1}{2}$ 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 $\{a, b\} \not\subseteq I$ 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 $\frac{1}{2}$. ◀

We show a protection lemma for fractional graphs which essentially states that the previous definition of protection set is meaningful, and thus will be useful to get rank lower bounds. This protection lemma is different from known ones for cutting planes: here the additional integer coordinates in the protection points overlaps, while they must be disjoint in [6]. This allows us to use fractional graphs to define protection sets.

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 6 (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 contained in P_i, then $G \in P_{i+1}$.*

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 $G \notin P_{i+1}$, then it holds that $a \cdot G > b$ where $ax \leq b$ is an inequality of rank $i+1$. Said inequality can be derived by integer division from an inequality $a'x \leq b'$ of rank i, where

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

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

Fix I to be the integral vertices of G, and $J = V(G) \setminus I$. The value of $a \cdot G$ is strictly less than $b+1$ but it is strictly larger than b, so it must be $b + \frac{1}{2}$. The coefficient vector a is integral, thus if follows that

$$\sum_{\{u,v\} \in J} a_{u,v} + \sum_{u \in J, w \in I} a_{u,w} \equiv 1 \pmod 2 \tag{7}$$

because otherwise $a \cdot G$ would be integral.

We now show that equation (7) implies that we can find at least a pair $\{u, v\} \subseteq J$ for which it holds that:

$$a_{u,v} + \sum_{w \in I} a_{u,w} + \sum_{w \in I} a_{v,w} \equiv 1 \pmod 2. \tag{8}$$

To see this denote $b_u := \sum_{w \in I} a_{u,w}$ for all $u \in J$. Equations (7) and (8) can be rewritten as

$$\sum_{\{u,v\} \in J} a_{u,v} + \sum_{u \in J} b_u \equiv 1 \pmod 2 \tag{9}$$

and

$$a_{u,v} + b_u + b_v \equiv 1 \pmod 2. \tag{10}$$

We partition J in two classes $J_0 = \{u \in J : b_u \equiv_2 0\}$ and $J_1 = \{u \in J : b_u \equiv_2 1\}$. If there is a pair $\{u, v\}$ such that $b_u \equiv b_v \pmod 2$ and $a_{u,v} \equiv 1 \pmod 2$ we are done; if there is a pair $\{u, v\}$ such that $b_u \not\equiv b_v \pmod 2$ and $a_{u,v} \equiv 0 \pmod 2$ we are also done. If neither happens then we can manipulate equation (9) as follows

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

which is a contradiction: $|J|$ is even so the right hand side is always even.

Fix any pair $\{u, v\}$ such that equation (8) holds. We consider $a \cdot G$ as the sum of three contributions: the sum over the integral edges of G, the sum over the edges enumerated in equation (8) 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 (8) B is half integral, and in particular follows that $A + C$ is integer.

Consider the two graphs $G'_{\{u,v\}}$ and $G''_{\{u,v\}}$ in the protection set. By definition they must differ from G *only* on the edges which coefficients are in the summation (8), 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 integer numbers.

It follows that numbers $a \cdot G'_{\{u,v\}}$ and $a \cdot G''_{\{u,v\}}$ are integral and (being the two graphs in P_i) they are strictly smaller than $b+1$. Thus the two values are at most b. G is the average of the two graphs, so it follows that $a \cdot G \leq b$, which contradicts the assumption that $G \notin P_{i+1}$. ◀

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

▶ **Theorem 7.** *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 a 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}.

Prover choice (round $i > 0$): prover sets G_i to be an arbitrary element of the protection set of G_{i-1} shown by delayer.

For $k \geq 4$, fractional graph G_0 satisfies all equations (6), thus it is contained in the initial polytope P_0. Lemma 6 says that if delayer reaches round i, then G_0 has rank at least i. 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 6 add exactly two vertices. Furthermore at each step we keep a bijection σ_i between the integral part of G_i and $\{1 \dots 2i\}$.

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

▶ Claim 1. There exists a graph H such that

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

$$h_{a,2m-1} = 1 - h_{a,2m}.$$

Delayer strategy: delayer uses such H to define its strategy against prover. The main idea is that at each round a new pair of vertices in G_0 are mapped to some diagonal pair of H. Each G_i in the trace of the game is almost a copy of the graph induced by the vertices $\{1 \dots 2i\}$ on H. We say "almost", because the value on the diagonal pair will be changed arbitrarily. 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, with integral part I. 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 $a \in I$

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

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'' keep the values of p. By construction the defined graphs make a protection set, because they satisfy the conditions of Definition 4.

After prover choice: prover can choose either $G'_{u,v}$ or $G''_{u,v}$ for some pair $\{u, v\}$. If prover chooses $G'_{u,v}$ then we extend σ_i to σ_{i+1} by adding the mapping $u \mapsto (2m-1)$ and $v \mapsto 2m$. Otherwise we add the mapping $u \mapsto 2m$ and $v \mapsto (2m-1)$.

Finally we show that the player can play for $e = 2^{k/2-1}$ rounds. In order to play that many round we need to argue that G_e is contained in P_0. Consider the equation (6) for an arbitrary set of vertices K of size $k \geq 4$: if there is a single vertex out of the integral part, then the sum contains at least two half-integral variables. None of the bounds can be violated.

If K is contained in the integral part of G_e, notice that the latter is isomorphic to some H' which is obtained from H by arbitrarily changing the edges on the diagonal pairs. By Claim 1 graph H' does not contain homogeneous vertices of size k. Thus Equation (6) on K is satisfied.

We have proved that $G_e \subseteq P_0$. That means (using Lemma 6) that $G_{e-1} \subseteq P_1$, $G_{e-2} \subseteq P_2$, . . . , and so on up to $G_0 \subseteq P_e$. This concludes the proof of the theorem ◀

Proof of Claim 1. Consider any $i \leq 2^{k/2-1}$. We determine independently at random the 0–1 values of $h_{v,(2i-1)}$ for all vertices $v < 2i-1$, and we set $h_{(v,2i)} := 1 - h_{v,(2i-1)}$. 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 which *are not on diagonal pairs*. The latter is true by construction for any set K containing a diagonal pair $\{2m-1, 2m\}$ plus some other vertex $v < 2m-1$. Let $\mathcal{K}_0$ 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

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

Families $\mathcal{K}_0$ and $\mathcal{K}_1$ are empty unless $k \geq 8$, and the 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

$$\Pr[H \text{ has an homogeneous set of size } k] \leq \sum_{K \in \mathcal{K}} \Pr[K \text{ is homogeneous}] \leq$$
$$\leq |\mathcal{K}_0| \frac{2}{2^{\binom{k}{2}}} + |\mathcal{K}_1| \frac{2}{2^{\binom{k}{2}-1}} \leq \frac{2}{2^{\binom{k}{2}}} \left[2^k \binom{n/2}{k} + 2^{k-1} \binom{n/2}{k-1} \right] < 1, \quad (11)$$

for $n = 2^{k/2}$. ◀

4 Conclusion

We have seen that Ramsey 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 $\binom{r(k,k)}{2}$ variables. Thus in order to improve the rank lower bound it is necesessary 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 [21]. This means that the formula for which the lower bound is proved has ad-hoc structure and is not interesting per se. Such lower bound has been proved by harnessing the connection between cutting planes inferences and monotone computation [21, 5]. It is an open problem how to prove length lower bounds for natural formulas, in particular using combinatorial techniques which allow 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 [2, 15]. It is interesting to notice that even if this implication is true then it has to be limited in some sense, since there are formulas with large rank (i.e. the square root of the number of variables) and small refutations [6]. Similar limitations hold for resolution and polynomial calculus as well (see [13, 4]), but still the study of auxiliary measures allowed many length lower bound there.

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 plane rank $\Omega(n)$?

As mentioned before there is a formula on n variables, polynomial length refutation and rank $\Omega(\sqrt{n})$ (see [6]). Thus any rank-length connection which holds in general would not be useful to prove a length lower bound for Ramsey Theorem, given the current knowledge. So even if a rank-length trade-off is proved, that would not solve the following problem:

▶ Open Problem 2. Does $\textsc{Ram}_k$ have a cutting planes refutation of polynomial length?

For further open problems about cutting planes refutations we suggest to refer to the book [16, CHapter 19].

Acknowledgment

Part of this work was done while the first author was at the Math Institute of the Czech Academy of Science, funded by the Eduard Čech Center.

References

1 Miklós Ajtai, János Komlós, and Endre Szemerédi. A note on Ramsey numbers. *Journal of Combinatorial Theory, Series A*, 29(3):354–360, 1980.

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

3 T. Bohman and P. Keevash. The early evolution of the h-free process. *Inventiones Mathematicae*, 181(2):291–336, 2010.

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

5 Maria Luisa Bonet, T. Pitassi, and Ran Raz. Lower bounds for cutting planes proofs with small coefficients. In *Proceedings of the twenty-seventh annual ACM symposium on Theory of computing*, pages 575–584. ACM, 1995.

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

7 Lorenzo Carlucci, Nicola Galesi, and Massimo Lauria. Paris-harrington tautologies. In *Proc. of IEEE 26th Conference on Computational Complexity*, pages 93–103, 2011.

8 Vasek Chvátal. Edmonds polytopes and a hierarchy of combinatorial problems. *Discrete Mathematics*, 4(4):305–337, 1973.

9 D. Conlon. A new upper bound for diagonal ramsey numbers. *Annals of Mathematics*, 170(2):941–960, 2009.

10 W. Cook, C.R. Coullard, and G. Turán. On the complexity of cutting-plane proofs. *Discrete Applied Mathematics*, 18(1):25–38, 1987.

11 P. Erdös. Some remarks on the theory of graphs. *Bull. Amer. Math. Soc*, 53:292–294, 1947.

12 Paul Erdős and G. Szekeres. A combinatorial problem in geometry. In Ira Gessel and Gian-Carlo Rota, editors, *Classic Papers in Combinatorics*, Modern Birkhäuser Classics, pages 49–56. Birkhäuser Boston, 1987.

13 Nicola Galesi and Massimo Lauria. Optimality of size-degree tradeoffs for polynomial calculus. *ACM Transaction on Computational Logic*, 12:4:1–4:22, October 2010.

14 R.E. Gomory. Outline of an algorithm for integer solutions to linear programs. *Bulletin of the American Mathematical Society*, 64(5):275–278, 1958.

15 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.

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

17 Jeong Han Kim. The Ramsey number $r(3,t)$ has order of magnitude $t^2/\log(t)$. *Random Structures and Algorithms*, 7(3):173–208, 1995.

18 Jan Krajíček. A note on propositional proof complexity of some Ramsey-type statements. *Archive for Mathematical Logic*, 50:245–255, 2011. 10.1007/s00153-010-0212-9.

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

20 Pavel Pudlák. Ramsey's theorem in Bounded Arithmetic. In *Proceedings of Computer Science Logic 1990*, pages 308–317, 1991.

21 Pavel Pudlák. Lower bounds for Resolution and Cutting Plane proofs and monotone computations. *Journal of Symbolic Logic*, 62(3):981–998, 1997.

22 Pavel Pudlák. A lower bound on the size of resolution proofs of the ramsey theorem. Technical Report TR11-162, 2011.

23 Joel Spencer. Asymptotic lower bounds for Ramsey functions. *Discrete Mathematics*, 20:69–76, 1977.

ECCC ISSN 1433-8092

http://eccc.hpi-web.de