Proof Complexity of the Ramsey Theorem

Pavel Pudlák

Mathematical Institute, Academy of Sciences, Prague

Limits of Theorem Proving, Rome, 2012

Overview

- Ramsey Theorem
- Proof complexity of formalizations of RT in the propositional calculus
- Krajíček's τ-propositions
- How difficult is to prove that a graph is *non-Ramsey* (joint work with M. Lauria, V. Rödl and N. Thapen)
- How difficult is to construct a *non-Ramsey* graph

Ramsey Theorem

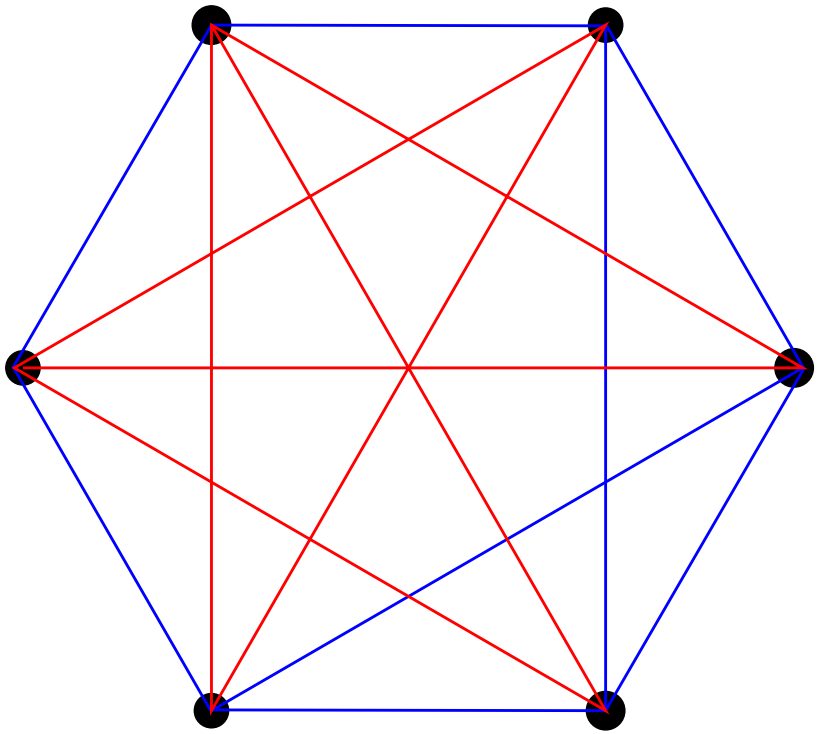
Theorem (Ramsey, Erdős-Szekeres)

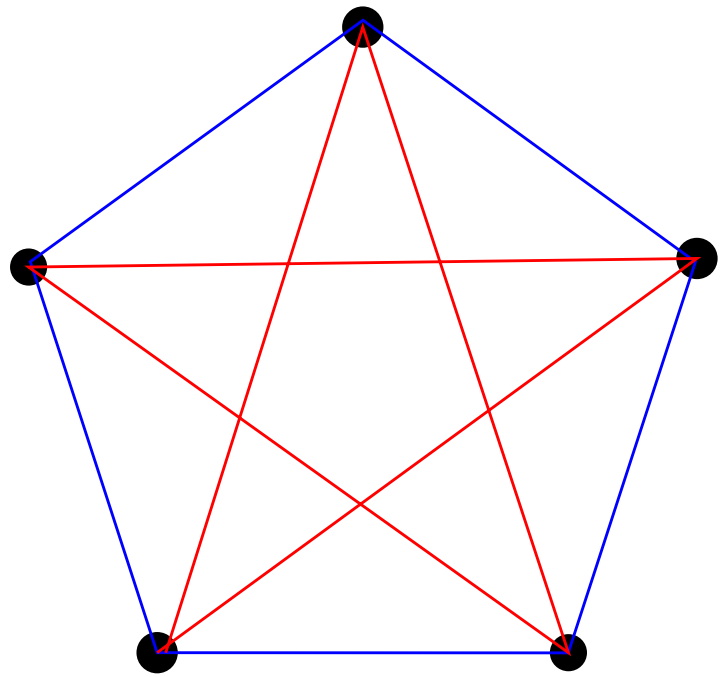
For every k, there exists n such that for all $f : [n]^2 \to [2]$, there exists a set $K \subseteq [n]$ such that $|K| = k$ and $f(x, y)$ is the same for all $x < y$, $x, y \in X$.

K is called *monochromatic*.

The least n is the Ramsey number $R(k)$.

Eg. $R(3) = 6$, $R(4) = 18$ (for $k > 4$ the values are not known).





Erdős asks us to imagine an alien force, vastly more powerful than us, landing on Earth and demanding the value of R(5) or they will destroy our planet. In that case, he claims, we should marshal all our computers and all our mathematicians and attempt to find the value. But suppose, instead, that they ask for R(6). In that case, he believes, we should attempt to destroy the aliens.[1]

–Joel Spencer

[1] Wikipedia, Ramsey's Theorem. Note that $102 \leq R(6) \leq 165$.

Asymptotic bounds

basically

$$2^{k/2} \leq R(k) \leq 4^k.$$

i.e.,

$$\frac{1}{2}\log_2 R(k) \leq k \leq 2\log_2 R(k)$$

Erdős 1947, Erdős-Szekeres 1935

$$(1+o(1))\frac{k}{\sqrt{2}e}2^{k/2} \leq R(k) \leq (1+o(1))\frac{4^{k-1}}{\sqrt{\pi k}}.$$

Spencer 1995, Conlon 2009

$$(1+o(1))\frac{\sqrt{2}k}{e}2^{k/2} \leq R(k) \leq k^{-c\log k/\log\log k}4^k$$

Lower bounds are non-constructive.

Formalization of RT in the propositional calculus

The variables are x_{ij}, for $1 \leq i < j \leq n$.

The clauses are $\bigvee_{i,j \in K} x_{ij}$ and $\bigvee_{i,j \in K} \neg x_{ij}$, for all sets $K \subseteq \{1, \ldots, n\}$, $|K| = k$.

The corresponding formula (a tautology if $n \geq R(k)$) will be denoted by $RAM(n, k)$.

The size of $RAM(n, k)$ is $n^{O(\log n)}$.

proof complexity of RT

Krishnamurthy proposed $RAM(R(k), k)$ as a hard tautology in 1981.

Theorem (Krajíček 2010)

$\forall d \exists \epsilon > 0 \forall n, k$ *if* $n = R(k)$, *then depth* d *Frege proofs of* $RAM(n, k)$ *have size* $2^{n^{\epsilon}}$.

Corollary

It is not possible to precisely determine Ramsey numbers only using Bounded Arithmetic.

proof complexity of RT

Krishnamurthy proposed $RAM(R(k), k)$ as a hard tautology in 1981.

Theorem (Krajíček 2010)

$\forall d \exists \epsilon > 0 \forall n, k$ *if* $n = R(k)$, *then depth* d *Frege proofs of* $RAM(n, k)$ *have size* 2^{n^ϵ}.

Corollary

It is not possible to precisely determine Ramsey numbers only using Bounded Arithmetic.

For $n = 4^k$ (i.e., $k = \frac{1}{2} \log_2 n$) the tautologies $RAM(n, k)$

- have quasipolynomial size proofs in bounded depth Frege systems,
- proofs in Resolution have size at least $2^{n^{\frac{1}{4} - o(1)}}$,
- open for $Res(\log)$ (Resolution with logarithmic size conjunctions).

τ propositions

Let $F : \{0,1\}^n \to \{0,1\}^m$ and $b \in \{0,1\}^m$ be such that

1. $n < m$,
2. F is computable by a polynomial size circuit C,
3. $b \notin Rng(F)$.

Then one can formalize condition 3. by a polynomial size tautology.

Krajíček and Razborov conjectures that for suitable functions F, these tautologies are hard

- for all b such that $b \notin Rng(F)$, and
- for Frege systems, but, possibly, for all proof systems.

Note that these tautologies are obtained in non-constructive way.

How difficult is to prove that a graph is *non-Ramsey*

Definition

- A graph on n vertices is *k-Ramsey* if the largest independent sets and the largest cliques have size $\leq k$.
- A sequence of graphs is called *non-Ramsey*[2] if they are k-Ramsey for $k = O(\log n)$.

Problem (Erdős, $ 100)

Give an explicit construction of a sequence of non-Ramsey graphs.

[2] It would also be natural to call these graphs *Erdős graphs*.

Formalization of the condition k-Ramsey

Let G be graph on $[n]$ with the set of edges E. Then G is k-Ramsey iff

for every bijection $W : [k+1] \to [n]$

- *there exists* $1 \leq i < j \leq k+1$ *such that* $(W(i), W(j))$ *is a non-edge and (i.e.,* $Im(W)$ *is not a clique) and*
- *there exists* $1 \leq i' < j' \leq k+1$ *such that* $(W(i'), W(j'))$ *is an edge (i.e.,* $Im(W)$ *is not an independent set).*

Formalization of the condition k-Ramsey

Let G be graph on $[n]$ with the set of edges E. Then G is k-Ramsey iff

for every bijection $W : [k+1] \to [n]$

- *there exists* $1 \leq i < j \leq k+1$ *such that* $(W(i), W(j))$ *is a non-edge and (i.e.,* $Im(W)$ *is not a clique) and*
- *there exists* $1 \leq i' < j' \leq k+1$ *such that* $(W(i'), W(j'))$ *is an edge (i.e.,* $Im(W)$ *is not an independent set).*

We will need the bit graph of W. So

- replace $[n]$ by $\{0,1\}^r$, where $n = 2^r$,
- $W = (w_1, \ldots, w_r)$, where $w_i : [k+1] \to \{0,1\}$.

Formalization of the condition k-Ramsey

Let G be graph on $[n]$ with the set of edges E. Then G is k-Ramsey iff

for every bijection $W : [k+1] \to [n]$

- *there exists* $1 \leq i < j \leq k+1$ *such that* $(W(i), W(j))$ *is a non-edge and (i.e.,* $Im(W)$ *is not a clique) and*
- *there exists* $1 \leq i' < j' \leq k+1$ *such that* $(W(i'), W(j'))$ *is an edge (i.e.,* $Im(W)$ *is not an independent set).*

We will need the bit graph of W. So

- replace $[n]$ by $\{0,1\}^r$, where $n = 2^r$,
- $W = (w_1, \ldots, w_r)$, where $w_i : [k+1] \to \{0,1\}$.

We define a DNF$\wedge$DNF formula k-Ram(G) (tautology if G is k-Ramsey) using variables $x_{i,j}$ for $i \in [k+1]$ and $j \in [r]$.

The structure of the formula k-Ram(G) is:

$$\bigvee_{i\neq j\in[k+1]} \bigvee_{(u,v)\notin E} (F(i)=u \wedge F(j)=v)) \wedge \bigvee_{i\neq j\in[k+1]} \bigvee_{(u,v)\in E} (F(i)=u \wedge F(j)=v))$$

For a vertex $u=(u_1,\ldots,u_r)$, the clause $F(i)=u$ is expressed by

$$\neg^{(1-u_1)} x_{i1} \wedge \cdots \wedge \neg^{(1-u_r)} x_{ir}.$$

Thus k-Ram(G) has $(k+1)r$ variables and $\binom{k+1}{2}\binom{n}{2}$ clauses of size $2r$.

The structure of the formula k-Ram(G) is:

$$\bigvee_{i\neq j\in[k+1]} \bigvee_{(u,v)\notin E} (F(i)=u \wedge F(j)=v)) \wedge \bigvee_{i\neq j\in[k+1]} \bigvee_{(u,v)\in E} (F(i)=u \wedge F(j)=v))$$

For a vertex $u=(u_1,\ldots,u_r)$, the clause $F(i)=u$ is expressed by

$$\neg^{(1-u_1)}x_{i1} \wedge \cdots \wedge \neg^{(1-u_r)}x_{ir}.$$

Thus k-Ram(G) has $(k+1)r$ variables and $\binom{k+1}{2}\binom{n}{2}$ clauses of size $2r$.

To transform this DNF$\wedge$DNF formula into a DNF formula of essentially the same size it suffices to use one extra variable.

The structure of the formula k-Ram(G) is:

$$\bigvee_{i\neq j\in[k+1]} \bigvee_{(u,v)\notin E} (F(i)=u \wedge F(j)=v)) \wedge \bigvee_{i\neq j\in[k+1]} \bigvee_{(u,v)\in E} (F(i)=u \wedge F(j)=v))$$

For a vertex $u=(u_1,\ldots,u_r)$, the clause $F(i)=u$ is expressed by

$$\neg^{(1-u_1)}x_{i1} \wedge \cdots \wedge \neg^{(1-u_r)}x_{ir}.$$

Thus k-Ram(G) has $(k+1)r$ variables and $\binom{k+1}{2}\binom{n}{2}$ clauses of size $2r$.

To transform this DNF$\wedge$DNF formula into a DNF formula of essentially the same size it suffices to use one extra variable.

Erdős's idea of the lower bound $2^{k/2} \leq R(k)$ can be used to construct a τ formula.

k-Ram(G) is a simplification which is suitable for Resolution.

Theorem

$\forall c\ \exists \epsilon > 0\ \forall G, n, k$ *if* $k \leq c \log n$ *and* G *is a* k*-Ramsey graph then every Resolution proof of* k*-Ram*(G) *has size at least* $n^{\epsilon \log n}$.

In plain words: *If* G *is any non-Ramsey graph, then there is no polynomial size Resolution proof of this fact.*

Theorem

$\forall c\ \exists \epsilon > 0\ \forall G, n, k$ *if* $k \leq c \log n$ *and* G *is a* k*-Ramsey graph then every Resolution proof of* k*-Ram*(G) *has size at least* $n^{\epsilon \log n}$.

In plain words: *If* G *is any non-Ramsey graph, then there is no polynomial size Resolution proof of this fact.*

Problem

Are there polynomial size proofs of these tautologies in stronger proof systems?

About the proof

Which properties of a non-Ramsey graph can we use?

- (-) The presence of a clique is not caused by having a large number of edges.

  Example. There exist a graphs with $\binom{n}{2} - o(n^2)$ edges without a clique of size $\epsilon \log n$ (e.g., Turán graphs).

- (-) The density of edges can be far from $1/2$.

  Example. Let G_0 be a random graph (density is $\approx 1/2$ and it is non-Ramsey). Let G be the disjoint union of two copies of G_0. G is still non-Ramsey and has density $\approx 1/4$.

- (+) A subgraph of a non-Ramsey graph of size n^ϵ, $\epsilon > 0$ is still a non-Ramsey graph.

Theorem (Erdős-Szemerédi 1972)

A non-Ramsey graph has positive density of both edges and non-edges.

More precisely: $\forall c\ \exists \epsilon > 0\ \forall G$ *if* G *is* $c \log n$*-Ramsey, then its density of edges* α *satisfies* $\epsilon < \alpha < 1 - \epsilon$.

Theorem (Erdős-Szemerédi 1972)

A non-Ramsey graph has positive density of both edges and non-edges.

More precisely: $\forall c\ \exists \epsilon > 0\ \forall G$ *if* G *is* $c \log n$*-Ramsey, then its density of edges* α *satisfies* $\epsilon < \alpha < 1 - \epsilon$.

Lemma (Prömel-Rödl 1999)

Let G *be* $c \log n$*-Ramsey. Then*
$\exists \beta, \delta > 0\ \exists S \subseteq V(G),\ |S| \geq |V(G)|^{3/4}\ \forall A, B \subseteq S,$

$$|A|, |B| \geq |S|^{1-\beta} \quad \Rightarrow \quad \delta \leq \frac{|E(A,B)|}{|A| \cdot |B|} \leq 1 - \delta.$$

Theorem (Ben-Sasson—Wigderson)

Let ϕ be a DNF tautology. Let v_ϕ and w_ϕ be the number of variables and the width of ϕ; let $w_{\vdash\phi}$ be the minimal width of its resolution proof. Then the size of any resolution proof of ϕ is bounded from below by

$$\exp\left(\Omega\left(\frac{(w_{\vdash\phi} - w_\phi)^2}{v_\phi}\right)\right).$$

For $\phi = c \log n\text{-Ram}(G)$, we have:

- $v_\phi = O(\log^2 n)$,
- $w_\phi = O(\log n)$.

Hence to prove a lower bound $\exp(\Omega(\log^2 n))$, it suffices to prove

- $w_{\vdash\phi} = \Omega(\log^2 n)$.

A game

Adversary pretends that there is a mapping $W : [k+1] \to [n]$ that defines a clique in G.

Prover wants to disprove this claim by asking about the bits defining W. He can record and erase information.

The number of bits *Prover* needs to catch *Adversary* lying is the width.

We define a strategy that enables *Adversary* to go on as long as there is $i \in [k+1]$ for which *Prover* has less than $\epsilon \log n$ bits on his record.

The strategy (basic idea)

Fix an $S \subseteq V(G)$ from the Prömel-Rödl Lemma.

Let B_i^t, for $i \in [k+1]$ be the set of vertices consistent with the information *Prover* has about $W(i)$ in time t.

Choose answers so that $B_i^t \cap S$ is large. If it is not possible, pick $v \in B_i^t$ and stick to it. In such a case the number of recorded bits about v should be $\epsilon \log n$.

The strategy (basic idea)

Fix an $S \subseteq V(G)$ from the Prömel-Rödl Lemma.

Let B_i^t, for $i \in [k+1]$ be the set of vertices consistent with the information *Prover* has about $W(i)$ in time t.

Choose answers so that $B_i^t \cap S$ is large. If it is not possible, pick $v \in B_i^t$ and stick to it. In such a case the number of recorded bits about v should be $\epsilon \log n$.

Lemma

Let $X, Y_1, \ldots, Y_r \subseteq S$ such that $|X| \geq rm^{1-\beta}$, $Y_1, \ldots, Y_r \geq m^{1-\beta}$. Then there exists $v \in X$ such that $|E(\{v\}, Y_i)| \geq \delta |Y_i|$ for all $i = 1, \ldots, r$.

How difficult is to construct a *non-Ramsey* graph

Problem (Erdős, $ 100)

Give an explicit construction of a sequence of non-Ramsey graphs.

Explicit constructions Let $n := R(k)$.

- $n^{O(\log n)}$-time deterministic algorithm to construct a non-Ramsey graph—method of conditional probabilities.
- very explicit construction for $k \leq \exp(c \cdot (\log n \log\log n)^{1/2})$, Frankl-Wilson 1981
- very complicated polynomial time algorithm $k \leq \exp((\log n)^{o(1)})$, Barak, Rao, Shaltiel, Wigderson 2006 (improving Barak, Kindler, Shaltiel, Wigderson 2005)

(Non-Ramsey means $k = O(\exp(\log\log n))$.)

Suppose that $c \cdot \log n$-Ram(G) tautologies do not have polynomial proofs in any proof system.

Then there is no polynomial time algorithm to construct non-Ramsey grpahs.

In fact more: Every **NP** subset of non-Ramsey graphs is finite.

Problem

Are there polynomial size proofs of $c \cdot \log n$-Ram(G) tautologies in stronger proof systems?

Thank You