The proof complexity of the finite Ramsey theorem

Pavel Pudlák

Mathematical Institute, Academy of Sciences, Prague

(partially based on a joint work with Massimo Lauria, Vojtěch Rödl and Neil Thapen)

Erdős Centennial, Budapest, 2013

Ramsey Theorem

Theorem (Ramsey 1930, Erdős-Szekeres 1935)

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. $R(3) = 6$, $R(4) = 18$, $102 \leq R(6) \leq 165$; for $k > 4$ the values are not known.

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.

Two problems

Problem (1) (Erdős, $ 250)

Determine the value

$$\lim_{k\to\infty} R(k)^{\frac{1}{k}}$$

if it exists.

If it exists, it is between $\sqrt{2}$ and 4.

Problem (2) (Erdős, \$ 100)

Give a constructive proof of $R(k) \geq (1+\varepsilon)^k$ for some $\varepsilon > 0$, i.e., give an explicit construction of a sequence of graphs on n vertices without a monochromatic set of size $k > c \log n$ for some c.

Problem (2) (Erdős, \$ 100)

Give a constructive proof of $R(k) \geq (1+\varepsilon)^k$ for some $\varepsilon > 0$, i.e., give an explicit construction of a sequence of graphs on n vertices without a monochromatic set of size $k > c \log n$ for some c.

Let $n := R(k)$.

- $n^{O(\log n)}$-time deterministic algorithm to construct a graph with $k = 2\log_2 n$—the method of conditional probabilities
- very explicit construction for $k \leq \exp(c \cdot (\log n \log\log n)^{1/2})$, Frankl-Wilson 1981 (later, same bounds Alon, Grolmusz)
- very complicated polynomial time algorithm $k \leq \exp((\log n)^{o(1)})$, Barak, Rao, Shaltiel, Wigderson 2006 (improving Barak, Kindler, Shaltiel, Wigderson 2005)

Two problems in computational complexity

Problem (1')

How difficult is to compute $R(k)$, i.e., what it the computational complexity of this function?

Problem (2')

How difficult is to construct graphs from Problem 2, i.e., what is the computational complexity of sequences of graphs on n vertices without monochromatic sets of size $k > C \log n$ for some C?

Two problems in proof complexity

Problem (1”)

Roughly: *How difficult is it to prove that $R(k) \leq n$?*

More precisely: *How difficult is it to prove a formalization of the Ramsey theorem for particular parameters?*

Problem (2”)

Roughly: *How difficult is it to prove $R(k) \geq n$?*

More precisely: *How difficult is it to prove that a given graph G on n vertices does not have a monochromatic sets of size $> C \log n$ for some C?*

Propositional proof systems

- Resolution (a.k.a. depth 1 Frege)
- Bounded depth Frege
- Frege (no superpolynomial lower bounds are known)

Formalization of RT in the propositional calculus

Edges of a graph on n vertices are represented by variables x_{ij} for $1 \leq i < j \leq n$.

$$RAM(n,k) \;\equiv\; \bigvee_{K} \left(\bigwedge_{i,j \in K} x_{ij} \vee \bigwedge_{i,j \in K} \neg x_{ij} \right)$$

where K are all sets $K \subseteq \{1, \ldots, n\}$, $|K| = k$.

$RAM(n,k)$ is a tautology iff $n \geq R(k)$.

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

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 $2^{n^{\epsilon}}$.

Proof-idea: reduction to PHP_m^{m+1}.

This suggests that computing $R(k)$ precisely may be hard.

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.

Theorem (Pudlák 2011)

Resolution proofs of $RAM(4^k, k)$ have size at least $2^{n^{\frac{1}{4}-o(1)}}$.

Open for depth 2 Frege.

Proof-idea: Random restriction and a width lower bound.

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

Definition

Call a graph on n vertices *c-Ramsey* if all its independent sets and cliques have size $\leq c \log n$.

Problem (2'')

Given a graph G, how difficult is it to prove that G is c-Ramsey?

For c constant, there exists a proof of size $n^{O(\log n)}$ — *"proof by inspection"*.

Formalization Suppose c is constant (say $c = 2$). Given a graph on n vertices, there is a natural formula c-Ram(G) such that

- it has $O(\log^2 n)$ variables;
- it is a disjunction of $O(n^2 \log^2 n)$ conjunctions, each of size $2c \log n$;
- it is a tautology iff G is c-Ramsey.

Theorem (Lauria, Pudlák, Rödl and Thapen 2012)

For every graph G on n vertices,[1] *every resolution proof of c-Ram(G) has size at least $\Omega(n^{\log n})$.*

[1] of course, the theorem is nontrivial only for c-Ramsey graphs

Proof-idea: A width lower bound using properties of c-Ramsey graphs.

Proof-idea: A width lower bound using properties of c-Ramsey graphs.

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*-Ramsey, then its density of edges* α *satisfies* $\epsilon < \alpha < 1 - \epsilon$.

Proof-idea: A width lower bound using properties of c-Ramsey graphs.

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*-Ramsey, then its density of edges* α *satisfies* $\epsilon < \alpha < 1 - \epsilon$.

Lemma (Prömel-Rödl 1999)

$\forall c \exists \beta, \delta > 0$ *such that for every* c*-Ramsey graph* G
$\exists S \subseteq V(G),\ |S| \geq |V(G)|^{3/4}$ *such that* $\forall A, B \subseteq S$,

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

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 $i = 1, \ldots, r$.

Problems and Conjectures

Problem

In which proof system can one prove c-Ram(G) tautologies by polynomial size proofs at least for some G?

Problems and Conjectures

Problem

In which proof system can one prove c-Ram(G) tautologies by polynomial size proofs at least for some G?

Conjecture

There exists a c, an infinite family of c-Ramsey graphs $\mathcal{R}$ and a proof system $\mathcal{P}$ such that the tautologies c-Ram(G) have polynomial size proofs in $\mathcal{P}$ for $G \in \mathcal{R}$.

Specifically, the conjecture is believed true for $\mathcal{R}$ the Paley graphs.

Problems and Conjectures

Problem

In which proof system can one prove c-Ram(G) tautologies by polynomial size proofs at least for some G?

Conjecture

There exists a c, an infinite family of c-Ramsey graphs $\mathcal{R}$ and a proof system $\mathcal{P}$ such that the tautologies c-Ram(G) have polynomial size proofs in $\mathcal{P}$ for $G \in \mathcal{R}$.

Specifically, the conjecture is believed true for $\mathcal{R}$ the Paley graphs.

Problem

Prove superpolynomial lower bounds on c-Ram(G) tautologies for stronger proof systems.

What is the meaning of such results?

1. The proof systems are very weak, so it is only warming up before proving more essential results.

What is the meaning of such results?

1. The proof systems are very weak, so it is only warming up before proving more essential results.

2. Although weak, these system are able to capture proof methods that are actually used (provided that we use suitable formalizations).

What is the meaning of such results?

1. The proof systems are very weak, so it is only warming up before proving more essential results.

2. Although weak, these system are able to capture proof methods that are actually used (provided that we use suitable formalizations).

3. It is possible to exclude the existence of efficient algorithms of certain kind.

Thank You