Open Problems Column
Edited By William Gasarch
gasarch@umd.edu

1 This Issues Column!

Luca Trevisan passed away on June 19, 2024 at the age of 52, of cancer. He worked on randomness, approximation, and many other topics in theory. My last column consisted of open problems by Lance Fortnow, Oded Goldreich, Johan Håstad, Salil Vadhan, and David P. Williamson that Luca was interested in. This column is also about a problem that Luca was interested in.

The column is on **Constructive Lower Bounds on Ramsey numbers** and is by Rishi Cherukuri and William Gasarch. Extractors played a large part in that work, and one of Luca's biggest contributions was his papers on extractors.

Request for Columns! I invite any reader who has knowledge of some area to contact me and arrange to write a column about open problems in that area. That area can be (1) broad or narrow or anywhere inbetween, and (2) really important or really unimportant or anywhere inbetween.

Constructive Lower Bounds on Ramsey Numbers

Rishi Cherukuri[*]
University of Maryland at College Park
rcheruku@terpmail.umd

William Gasarch[†]
University of Maryland at College Park
gasarch@umd.edu

April 17, 2025

2 Introduction

Convention 2.1 Throughout this paper if $G = (V, E)$ is a graph then $n = |V|$ and $m = |E|$.

3 Ramsey Numbers

We review the basic concepts of Ramsey Theory.

Definition 3.1 Let $A \subseteq \mathsf{N}$. Let $a, n \in \mathsf{N}$.

1. $[n]$ is the set $\{1, \ldots, n\}$.
2. $\binom{A}{a}$ is the set of all a-sized subsets of A.
3. $\binom{[n]}{2}$ is the set of all pairs of elements of $\{1, \ldots, n\}$.
4. Let $\mathrm{COL}\colon \binom{[n]}{2} \rightarrow [2]$. Then H is a *homogenous set* if COL restricted to $\binom{H}{2}$ is constant.

The following is known as *Ramsey's Theorem (for graphs).*

Theorem 3.2 *For all k, there exists n, such that for all $\mathrm{COL}\colon \binom{[n]}{2} \rightarrow [2]$, there exists a homogenous set of size k.*

Definition 3.3 $R(k)$ is the least n such that, for all $\mathrm{COL}\colon \binom{[n]}{2} \rightarrow [2]$, there exists a monochromatic clique of size k. Note that such an $R(k)$ exists by Theorem 3.2

[*] Dept. of Comp. Sci., Univ.of Maryland, MD 20742

[†] Dept. of Comp Sci, Univ. of Maryland, MD, 20742

Upper Bounds

Result	Comment	Ref
$R(k) \le 2^{2k-1}$	Standard Proof	Folklore
$R(k) \le (1+o(1))4^{k-1}/\sqrt{\pi k}$	Elementary	[11]
$R(k) \le 4^s/s^{(c\log k)/(\log\log k)}$	Difficult	[10]
$R(k) \le (4-\epsilon)^k$	Difficult	[6]

Lower Bounds

Definition 3.4 A *constructive lower bound on* $R(k)$ is an algorithm that will, given k, produce a 2-coloring of $\binom{[n]}{2}$ in time $p(n)$ for some polynomial in n.

There were initially some rather poor lower bounds on $R(k)$ that were polynomial in k. These proofs were constructive. Then Erdős [12] used the probabilistic method to obtain exponential, though nonconstructive, lower bounds on $R(k)$. That last sentence is true but not quite right: the probabilistic method was invented by Erdős in that paper for the purpose of getting lower bounds on $R(k)$.

Since then there has been improvements to both the nonconstructive lower bound, and the constructive lower bounds. We give two charts of the progress: one for nonconstructive lower bounds, one for constructive lower bounds. The rest of the paper will elaborate on the chart, say what Luca Trevisan's contribution to this field is, and pose open questions.

The charts uses the following abbreviations.

- *Elt* means an elementary proof that could be taught to interested high school students.
- *LLL* means that the proof used the Lovasz Local Lemma.

Non-Constructive Lower Bounds

Result	Comments	Paper
$R(k) \ge (1+o(1))k2^{k/2}/\sqrt{2}e$	Elt	[12]
$R(k) \ge (1+o(1))k2^{k/2}\sqrt{2}/e$	LLL	[23]

Constructive Lower Bounds

Result	Comments	Paper
$R(k) \geq (k-1)^2$	Elt	Folklore
$R(k) \geq \Omega(k^{2.3\ldots}$	Elt	[1]
$R(k) \geq \Omega(k^3)$	Elt	[20]
$R(k) \geq 2^{\Omega(\log^2(k)/\log\log k)}$	Set Systems	[13]
$R(k) \geq 2^{\Omega(\log^2(k)/\log\log k)}$	Info Theory and LA	[2]
$R(k) \geq 2^{\Omega(\log^2(k)/\log\log k)}$	Representing OR	[15]
$R(k) \geq 2^{\Omega(\log^2(k)/\log\log k)}$	Representing OR	[14]
$R(k) \geq$ Better than [13]	Extractors	[17]
$R(k) \geq$ Better than [13]	Extractors	[18]
$R(k) \geq 2^{\Omega(k^\delta)} (\delta < 1)$	Extractors	[19]

The results above motivates the following open questions.

1. Is there a constant $\alpha > \frac{1}{2}$ such that $R(k) \geq \Omega(2^{\alpha k})$. This has been open for a long time.

2. Narrow the gap between the highest lower bound and the lowest upper bound.

3. Obtain better constructive proofs of the lower bound on $R(k)$ with the hope that they one day match the nonconstructive proof.

The bulk of this paper will be to elaborate on the table of constructive lower bounds on $R(k)$.

4 A Mini Survey of Const. Lower Bounds on $R(k)$

4.1 Nagy's Construction: $R(k) \geq \Omega(k^3)$

Definition 4.1 A *set system* is a set of subsets of $\binom{[n]}{a}$ for some n, a.

Nagy [20] showed the following. The proof is elementary.

Theorem 4.2 *$R(k) \geq \Omega(k^3)$.*

Proof sketch: Let G be the complete graph on $\binom{k}{3}$ vertices. Represent G by having each vertex be an element of $\binom{[k]}{3}$. Let COL be the defined as follows

$$\mathrm{COL}(A,B) = \begin{cases} 1 & \text{if } |A \cap B| = 1 \\ 2 & \text{if } |A \cap B| \neq 1 \end{cases} \tag{1}$$

One can show that (a) G has $\Theta(k^3)$ vertices, and (b) the coloring does not have a homogenous set of size k. ▮

Open Problem 4.3 The proof that Nagy's Construction works is elementary. One could teach it to interested high school students. All of the later constructions are not elementary. Come up with an elementary proof that $R(k) \ge \Omega(n^4)$. Or even larger degree than that. This result would not be as strong as the later ones in this paper; however, they would be good for education.

4.2 The Frankl-Wilson Construction

Frankl & Wilson [13] showed the following. The proof is involved by elementary.

Theorem 4.4 *There is a constant c such that $R(k) \ge 2^{(\frac{c\log^2 k}{\log(\log(k))})}$.*

Proof sketch: Let q be a prime such that $k \sim \binom{q^3}{q-1}$. Let $n = \binom{q^3}{q^2-1}$. Let G be the complete graph on n vertices.

$$\mathrm{COL}(A,B) = \begin{cases} 1 & if |A \cap B| \equiv q-1 \pmod q \\ 2 & if |A \cap B| \not\equiv q-1 \pmod q \end{cases} \tag{2}$$

One can show that (a) there is a constant c such that G has $2^{(\frac{c\log^2 k}{\log(\log(k))})}$ vertices, and (b) the coloring does not have a homogenous set of size k.

$\blacksquare$

4.3 Alon's Construction

Alon [2] reproved Theorem 4.4. His proof used information theory and linear algebra. We need to present some background to even give a sketch of the proof.

Definition 4.5 Let G be the graph (V,E).

1. Let $n \in \mathsf{N}$. Then G^n be the graph (V',E') where $V' = V^n$ and E' is as follows:

$$\{(v_1,\ldots,v_n),(u_1,\ldots,u_n)\colon (\forall i)[u_i = v_i \vee (u_i,v_i) \in E].$$

2. $\alpha(G)$ is the size of the largest independent set in G (often called *the ind. number of* G).

3. The *Shannon Capacity* $c(G)$ *of* G is $\lim_{n\to\infty} \alpha((G^n)^{\frac{1}{n}})$.

Definition 4.6 Let H be a field and $r \in \mathsf{N}$. View $H[x_1,\ldots,x_r]$ as a vector space. Let $\mathcal{H}_r$ be a subspace of $H[x_1,\ldots,x_r]$. Let $G=(V,E)$ be a graph.

A *representation of* G *over* $\mathcal{H}_r$ is a function from V to $(\mathcal{H}_r, H^r)$ (denote where v maps to by $(p_v(x_1,\ldots,x_r), a_v)$ (note that p_v is a polynomial in r variables, and a_v is a vector of r elements of H) such that

- For all $v \in V$, $p_v(a_v) \neq 0$.
- If $(u, v) \notin E$ then $p_v(a_u) = 0$.

Alon then proves the following:

Theorem 4.7 *For any graph $G = (V, E)$ with representation $\mathcal{H}_r$ over a field H, $c(G) \leq dim(\mathcal{H}_r)$.*

Using this theorem, Alon thus found:

BILL TO RISCH: IN THE DEF OF $K(p, r)$ YOU ALSO INCLUDE A COLORING OF $K(P, r)$. SO IS $K(p, r)$ A COLORED GRAPH? I TREAT IT AS SUCH IN THE FOLLOWING DEFINITION. CORRECT IT OR LEAVE A COMMENT ABOUT THIS.

Definition 4.8 Let $P = \{p_1, \ldots, p_g\}$ where each p_i is prime. Let $s = p_1 p_2 \cdots p_g - 1$. Consider an integer $r > s$. Define $K(P, r)$ to be a graph (V, E) together with a g-coloring of it, as follows:

- $V = \binom{[r]}{s}$.
- $E = \binom{V}{2}$. BILL TO RISCHI- YOU DID NOT SAY WHAT THE EDGES WERE SO I AM ASSUMING ITS THE COMPLETE GRAPH. EITHER AGREE AND TAKE THIS COMMENT OUT, OR DISAGREE AND EDIT.
- We color the edge (A, B) by the least j such that $|A \cap B| \not\equiv -1 \pmod{p_j}$.

Theorem 4.9 *Let $G = (V, E)$ be the 0-colored subgraph of a 2-colored $K(P, r)$. Then, $c(G)$ $\leq$*

$$\sum_{i=0}^{|K|-|G|} \binom{r}{i}$$

Thus, there exists COL: $\binom{[n]}{2} \rightarrow [2]$ *which has no homogenous set of size*

$$\sum_{i=0}^{n} \binom{r}{i}$$

Alon uses this theorem to give a bound on the Ramsey numbers $R(k)$ analogous to that of the Frankl-Wilson construction.

Theorem 4.10 *There is a constant c such that $R(k) \geq 2^{(\frac{c \log^2 k}{\log(\log(k)})}$.*

Proof sketch:

Let $n = 2^{(\frac{c \log^2 k}{\log(\log(k)})}$.

One can find a graph G on n vertices so that both G and $\overline{G}$ have a representation H_k. By Theorem 4.7, neither G nor $\overline{G}$ have a clique. One can easily use this to get a coloring of the edges such there is no homogenous set of size k.

▮

4.4 Grolmusz's Construction

Recall that the Frankl-Wilson construction as stated here needs that q is a prime. In their paper they need that q is a prime power. They asked if the construction could be extended to the case where q is not a prime power.

Grolmusz's construction achieves this. He needed to use the following concept.

Definition 4.11 Let $m, n \in \mathsf{N}$, $m, n \geq 2$.

1. Let $\vec{x}$ be $x_1, \ldots, x_n$.
2. Z_m is the integers $\{0, \ldots, m-1\}$ mod m.
3. $\mathsf{Z}_m[\vec{x}]$ is the set of polynomials in $x_1, \ldots, x_n$ with coefficients in Z_m. We will always evaluate such polynomials mod m.
4. Let $f(\vec{x})$ be a function with input $\{0,1\}^n$. A polynomial $p(\vec{x}) \in \mathsf{Z}_m[\vec{x}]$ *weakly represents f mod m* if, for all $\vec{x} \in \{0,1\}^n$, $\vec{y} \in \{0,1\}^n$, if $f(\vec{x}) \neq f(\vec{y})$ then $p(\vec{x}) \neq p(\vec{y}) \pmod{m}$.
5. OR_n is the function that maps $\vec{a} \in \{0,1\}^a$ to the OR of the bits.
6. Let p, q be primes. Let $P \in \mathsf{Z}_p[\vec{x}]$ and $Q \in \mathsf{Z}_q[\vec{x}]$. (P, Q) *represents* OR_n if the following occur.
   (a) $P(0, \ldots, 0) \equiv 1 \pmod{p}$.
   (b) $Q(0, \ldots, 0) \equiv 1 \pmod{q}$.
   (c) For all $\vec{a} \in \{0,1\}^n - (0, \ldots 0)$, $P(\vec{a}) \equiv 0 \pmod{p}$ or $Q(\vec{a}) \equiv 0 \pmod{q}$.

   (This is not a typo. We really do have $(0, \ldots, 0)$ map to 1.)

They use results from Barrington, Beigel, and Rudich [5] on representing the Boolean function OR with a low degree polynomial. Grolmusz's construction is interesting; however, it ends up obtaining the same lower bound that Frankl-Wilson did, and that Alon did.

4.5 Gopalan's Construction and Observation

Frankl-Wilson's proof and Alon's proof are wildly different, yet they both give the same constructive lower bound on $R(k)$. Grolmusz's construction generalizes Frankl-Wilson and it was hoped that it would give a better constructive lower bound, but alas, it also gave the same bound.

What is going on here?

Gopalan [14] gave a framework that encompassed the constructions of Frankl-Wilson, Alon, and Grolmusz. He then prove the following:

- Any construction in that framework is reducible to low-degree weak representations of the OR function.

- Any construction that is reducible to low-degree weak representations of the OR function cannot give a lower bound any better than $2^{\Omega(\log^2(k)/\log\log k)}$.

Hence any improvements would need to be outside of this framework.

Gopalan also gave his own construction which more explicitly showed the usage of low-degree weak representations of OR_n.

Open Problem 4.12 Come up with an easier proof of the constructive lower bound $R(k) \ge 2^{\Omega(\log^2(k)/\log\log k)}$. This will probably involve coming up with easier lower bounds of theorems about low-degree weak representations of the OR_n function.

4.6 Li's Construction

Recall that the nonconstructive lower bound on $R(k)$ uses the probabilistic method. Hence it might make sense to see if psuedo-random generators could be used to get constructive lower bounds. While this approach was certainty considered the main problem with is is that most (all?) psuedo-random generators depended on unproven assumptions.

Extractors are algorithms that convert a weak-random source to an almost uniform source. Luca Trevisan [24] showed a useful connection between extractors and psuedo-random generators. This paper was very important. Most (all?) later papers on extractors depend on it.

In a series of papers Li [17, 18, 19] Li obtained different kinds of extractors that were useful for obtaining constructive lower bounds on $R(k)$. We omit discussion of the extractors (except to say that the proofs are sophisticated and difficult) and state the constructive lower bound he obtained.

The first two papers had constructive lower bounds that beat the FW-bound; however, are hard to state. The third paper has a lower bound that is statable.

Theorem 4.13 *There exists δ such that, for all k, $R(k) \ge 2^{\Omega(k^\delta)}$.*

Li did not state it this way. We say what he did state and how to obtain the result.

Li showed $\exists C$ such that, for all N, there is a coloring of K_N where there is no homogenous set of size $(\log N)^C$.

Set $k = (\log N)^C$.

$k^{1/C} = \log N$

$N = 2^{K^{1/C}}$.

Set $1/C = \delta$.

Open Problem 4.14

1. Improve Li's lower bound to $2^{\Omega(k)}$.

2. Li's paper did not state a value for δ. Find what value works for Li's proof and try to improve it.

3. Find an easier proof of Li's result.

4. Find an easier proof of a lower bound that is better than the FW lower bound, though perhaps not as good as Li's results.

5. Find an easier proof of a lower bound that is better than the FW lower bound, though perhaps uses a hardness assumption.

5 Other Constructive Ramsey Lower Bounds

In this paper we have focused on constructive lower bounds for $R(k)$. There has been work on constructive lower bounds for other types of Ramsey Numbers:

1. Chung, Cleve, & Dagum [8] found constructive lower bounds for the asymmetric Ramsey number $R(3, k)$ through a clever but elementary explicit graph construction.

2. Kostochka, Pudlak, & Rodl [16] found lower bounds for the asymmetric Ramsey numbers $R(4, k), R(5, k)$ and $R(6, k)$ through clever graph constructions and linear algebra.

3. Alon & Pudlak [3] found constructive lower bounds on the asymmetric Ramsey number $R(s, t)$ using algebraic methods over Galois fields.

4. The following papers are on constructive lower bounds for bipartite Ramsey numbers: Pudlak & Rodl [21], Barak, Rao, Shaltiel, Wigderson [4], Pudlak [22], Chattopadhyay & Zuckerman [7], Cohen [9]. Each of them used extractors and psuedo-randomness in their bounds for bipartite Ramsey numbers.

6 Open Problems

There are basically two open problems that apply to all of the types of Ramsey numbers we have discussed.

Open Problem 6.1

1. Improve the constructive lower bounds given in those papers.

2. Find easier proofs for the constructive lower bounds given in those papers.

3. Find easier proofs, suitable to teach to interested high school students, of smaller constructive lower bounds.

4. Find easier proofs, perhaps using hardness assumptions, of smaller constructive lower bounds (or even the same).

References

[1] H. Abbott. Lower bounds on some Ramsey numbers. *Discrete Mathematics*, 2:289–293, 1971.

[2] N. Alon. The Shannon capacity of a union. *Combinatorica*, 18(3):301–310, 1998. https://doi.org/10.1007/PL00009824.

[3] N. Alon and P. Pudlak. Constructive lower bounds for off-diagonal Ramsey numbers. *Israel Journal of Mathematics*, 2001. https://link.springer.com/content/pdf/10.1007/BF02809902.pdf.

[4] B. Barak, A. Rao, R. Shaltiel, and A. Wigderson. 2-source dispersers for sub-polynomial entropy and Ramsey graphs beating the Frankl-Wilson construction. In J. M. Kleinberg, editor, *Proceedings of the 38th Annual ACM Symposium on Theory of Computing, Seattle, WA, USA, May 21-23, 2006*, pages 671–680. ACM, 2006. https://doi.org/10.1145/1132516.1132611.

[5] D. A. M. Barrington, R. Beigel, and S. Rudich. Representing boolean functions as polynomials modulo composite numbers. *Comput. Complex.*, 4:367–382, 1994. https://doi.org/10.1007/BF01263424.

[6] M. Campos, S. Griffiths, R. Morris, and J. Sahasrabudhe. An exponential improvement for diagonal Ramsey, 2023. https://arxiv.org/abs/2303.09521.

[7] E. Chattopadhyay and D. Zuckerman. Explicit two-source extractors and resilient functions. In D. Wichs and Y. Mansour, editors, *Proceedings of the 48th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2016, Cambridge, MA, USA, June 18-21, 2016*, pages 670–683. ACM, 2016. https://doi.org/10.1145/2897518.2897528.

[8] F. R. K. Chung, R. Cleve, and P. Dagum. A note on constructive lower bounds for the Ramsey numbers $R(3,t)$. *J. Combinatorial Theory B*, 57(1):150–155, 1993. https://doi.org/10.1006/jctb.1993.1013.

[9] G. Cohen. Two-source dispersers for polylogarithmic entropy and improved ramsey graphs. *SIAM J. Comput.*, 50(3), 2021. https://doi.org/10.1137/16M1096219.

[10] D. Conlon. A new upper bound for diagonal Ramsey numbers. *Annals of Mathematics*, 170(2):941–960, 2009. https://arxiv.org/abs/math/0607788.

[11] P. Erdős and G. Szekeres. A combinatorial problem in geometry. *Compositio Math*, 2(4):463–470, 1935. http://www.renyi.hu/~p_erodso/1935-01.pdf.

[12] P. Erdos. Some remarks on the theory of graphs. *Bulletin of the American Mathematical Society*, 53(4):292–294, 1946.

[13] P. Frankl and R. Wilson. Intersection theorems with geometric consequences. *Combinatorica*, 1:357–368, 1981. http://www.springer.com/new+%26+forthcoming+titles+%28default%29/journal/493.

[14] P. Gopalan. Constructing Ramsey graphs from boolean function representations. *Combinatorica*, 34(2):173–206, 2014.
https://doi.org/10.1007/s00493-014-2367-1.

[15] V. Grolmusz. Superpolynomial size set-systems with restricted intersections mod 6 and explicit Ramsey graphs. *Combinatorica*, 20(1):71–86, 2000.
https://doi.org/10.1007/s004930070032.

[16] A. V. Kostochka, P. Pudlák, and V. Rödl. Some constructive bounds on Ramsey numbers. *Journal of Combinatorial Theory B*, 100(5):439–445, 2010.
https://doi.org/10.1016/j.jctb.2010.01.003.

[17] X. Li. Improved non-malleable extractors, non-malleable codes and independent source extractors. In H. Hatami, P. McKenzie, and V. King, editors, *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2017, Montreal, QC, Canada, June 19-23, 2017*, pages 1144–1156. ACM, 2017.
https://doi.org/10.1145/3055399.3055486.

[18] X. Li. Non-malleable extractors and non-malleable codes: Partially optimal constructions. In A. Shpilka, editor, *34th Computational Complexity Conference, CCC 2019, July 18-20, 2019, New Brunswick, NJ, USA*, volume 137 of *LIPIcs*, pages 28:1–28:49. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2019.
https://doi.org/10.4230/LIPIcs.CCC.2019.28.

[19] X. Li. Two source extractors for asymptotically optimal entropy, and (many) more. In *64th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2023, Santa Cruz, CA, USA, November 6-9, 2023*, pages 1271–1281. IEEE, 2023.
https://doi.org/10.1109/FOCS57990.2023.00075.

[20] Z. Nagy. A constructive estimate of the Ramsey numbers. *Mat. Lapok*, pages 301–302, 1975.

[21] A. Podelski and A. Rybalchenko. A complete method for the synthesis of linear ranking functions. In *Verification, model checking, and abstract interpretation*, volume 2937 of *Lecture Notes in Computer science*, pages 239–251, New York, 2004. Springer. http://www7.in.tum.de/~rybal/papers/.

[22] P. Pudlák. *Topics in Discrete Mathematics Dedicated to Nesetril's 60th Birthday*, volume 26, chapter On explicit Ramsey graphs and estimates of the number of sums and products. Springer, 2006.
`https://www.cs.umd.edu/~gasarch/TOPICS/const_ramsey/sumprod.pdf`.

[23] J. Spencer. Ramsey's theorem–a new lower bound. *Journal of Combinatorial Theory, Series A*, 18:108–115, 1975.

[24] L. Trevisan. Extractors and pseudorandom generators. *J. ACM*, 48(4):860–879, 2001.
`https://doi.org/10.1145/502090.502099`.