A SAT + Computer Algebra System Verification of the Ramsey Problem $R(3, 8)$ (Student Abstract)

Conor Duggan[1], **Zhengyu Li**[2], **Curtis Bright**[3], **and Vijay Ganesh**[2]

[1]University of Waterloo, Canada
[2]Georgia Institute of Technology, USA
[3]University of Windsor, Canada
c4duggan@uwaterloo.ca, {brian.li, vganesh45}@gatech.edu, cbright@uwindsor.ca

Abstract

The Ramsey problem $R(3, 8)$ asks for the smallest n such that every red/blue coloring of the complete graph on n vertices must contain either a blue triangle or a red 8-clique. We provide the first certifiable proof that $R(3, 8) = 28$, automatically generated by a combination of Boolean satisfiability (SAT) solver and a computer algebra system (CAS). This SAT+CAS combination is significantly faster than a SAT-only approach. While the $R(3, 8)$ problem was first computationally solved by McKay and Min in 1992, it was not a verifiable proof. The SAT+CAS method that we use for our proof is very general and can be applied to a wide variety of combinatorial problems.

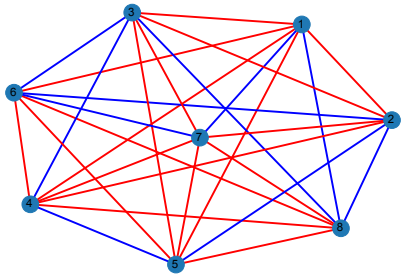

Figure 1: A red/blue edge coloring on 8 vertices without a blue 3-clique or red 4-clique, showing $R(3, 4) > 8$.

Introduction

Ramsey Theory was first introduced by Frank P. Ramsey in *On a problem of formal logic* (Ramsey 1930). Contemporary proof techniques to finding Ramsey numbers are often computer-assisted, making formal verification an essential step in such a proof method. Ramsey numbers are renowned and challenging problems; only 9 non-trivial Ramsey numbers are known, despite an extensive literature on the topic (Radziszowski 2011).

The Ramsey Theorem states that for every $p, q \in \mathbb{Z}$, there exists an $n \in \mathbb{Z}$ such that any red/blue coloring of the edges of the complete graph of order n, denoted K_n, contains a monochromatic blue p-clique or a red q-clique (an m-clique is a complete subgraph of order m). A Ramsey problem is defined as finding the smallest such integer n, denoted $R(p, q)$, for some given input (p, q).

A (p, q)-graph is a colored complete graph without a monochromatic blue p-clique and without a red q-clique. Figure 1 demonstrates that $R(3, 4) > 8$ by exhibiting a $(3, 4)$-graph on 8 vertices.

In 1992, McKay and Min computationally showed that no $(3, 8)$-graph exists on 28 vertices (McKay and Min 1992). Combined with a previous result that $R(3, 8) > 27$ (Grinstead and Roberts 1982), this showed $R(3, 8) = 28$. According to McKay and Min, their computation required approximately 10^{14} machine instructions on a network of SUN workstations.

A conflict-driven clause learning (CDCL) satisfiability (SAT) solver is a computer program that takes as input a Boolean formula in conjunctive normal form (CNF), and decides whether the input is satisfiable. CDCL SAT solvers can solve some instances with millions of variables efficiently (Ganesh and Vardi 2021). However, SAT solvers face challenges when solving combinatorial problems such as the Ramsey problem, in part due to the considerable amount of *symmetry* in the associated search space.

Computer Algebra Systems (CASs), such as Maple and Mathematica, are storehouses of mathematical knowledge and are widely used to solve a variety of scientific and engineering problems. We use a CAS to dynamically provide mathematical context to the SAT solver in order to break symmetries in the search space associated with an input formula. In particular, we use a CAS to generate blocking clauses that are given to the SAT solver dynamically via a programmatic interface (Ganesh et al. 2012). The clauses block the solver from exploring noncanonical matrix representations of a graph, since they are all isomorphic to one "canonical" representation. An adjacency matrix M of a graph is canonical if every permutation of the graph's vertices produces a matrix lexicographically greater than or equal to M, where lexicographical order is defined by concatenating the above-diagonal entries of the columns of the adjacency matrix starting from the left. Blocking noncanonical graphs is achieved using orderly generation (Li, Bright, and Ganesh 2022) and is implemented through the SAT+CAS paradigm (Bright, Kotsireas, and Ganesh 2022). This technique can dramatically prune a formula's search

space, since the CAS guides the SAT solver to not only block a noncanonical subgraph but also all its extensions. The SAT+CAS paradigm has been shown to be an effective approach to solving hard combinatorial math problems. Regarding the work presented here, we performed an ablation study demonstrating that SAT+CAS is orders of magnitude faster than a SAT-only solver. For example, for $R(3,7)$ on 23 vertices, SAT+CAS solved the problem in 2 minutes and the SAT solver alone could not solve it in 24 hours on an i7-9750 processor running at 2.60 GHz with 8GB of RAM.

Methodology

The Ramsey problem is encoded for a given n, p, q by generating a Boolean formula in CNF asserting the existence of a (p,q)-graph of order n. The encoding enforces every p-clique to have at least one edge in the opposite (red) color and every q-clique to have at least one edge in the opposite (blue) color, i.e.,

$$\bigwedge_{K_p \subseteq K_n} \bigvee_{e \in K_p} \neg e \wedge \bigwedge_{K_q \subseteq K_n} \bigvee_{e \in K_q} e,$$

where the variable e is assigned true when the corresponding edge is colored blue (and false otherwise). A SAT assignment corresponds to finding a (p,q)-graph of order n. Similarly, UNSAT means no such colorings exist for this particular n, i.e., all colorings contain a blue p-clique or a red q-clique. Partial static symmetry breaking clauses that enforce a lexicographic ordering on the rows of a graph's adjacency matrix are also used (Codish et al. 2019). Vertex degree constraints are appended to the encoding stating that for a (p,q)-graph on n vertices, each vertex v satisfies $n - R(p, q-1) \leq \deg(v) \leq R(p-1, q) - 1$ where $\deg(v)$ is the number of blue edges on vertex v (Conlon, Fox, and Sudakov 2015).

Verification of Our Result

The value of the Ramsey number $R(3,8) = 28$ is concluded by obtaining an UNSAT result on the encoding asserting the existence of a 28-vertex $(3,8)$-graph and a SAT result on the encoding asserting the existence of a 27-vertex $(3,8)$-graph. Thus, the correctness of the result is crucially dependent on the encodings and computational tools we use. Results given by the SAT+CAS paradigm can be verified, as the method generates certificates in the DRAT format (Wetzler, Heule, and Hunt Jr 2014), allowing an independent third party to certify the SAT solver's search is indeed exhaustive and also that the learned clauses provided by the CAS are correct. Thus, one only needs to trust the correctness of the proof verifier, rather than the SAT solver or the CAS.

$R(3,8)$ on 28 vertices was found to be UNSAT using MapleSAT (Liang et al. 2016) combined with a CAS, after 96 hours on an AMD EPYC 7763 2.45 GHz processor with 16 GiB of RAM. A 30 GiB DRAT file was generated and verified in 63 hours. Verification was performed on a virtual machine with an Intel Xeon CPU E5-2673 v3 processor running at 2.40 GHz and with 28 GiB of RAM.

Verification was performed using the DRAT-trim proof checker (Wetzler, Heule, and Hunt Jr 2014) slightly modified to support the addition of trusted clauses (Li, Bright, and Ganesh 2023). MapleSAT generates a DRAT proof consisting of the clauses learned by it during the solving process. The proof checker then verifies that each clause can be derived from the previous clauses via resolution. The CAS-derived blocking clauses are verified by evidencing that the clause blocks graphs whose adjacency matrices are not canonical. This is verified by checking a permutation applied to the blocked graph's corresponding adjacency matrix produces a matrix smaller in lexicographical order. The permutation is derived by the CAS during solving and recorded as a witness for the trusted clauses in the DRAT proof.

In summary, we present the first formally verified proof that the Ramsey number $R(3,8)$ is 28, via a SAT+CAS technique where the CAS implements orderly generation.

References

Bright, C.; Kotsireas, I.; and Ganesh, V. 2022. When satisfiability solving meets symbolic computation. *CACM*, 65(7): 64–72.

Codish, M.; Miller, A.; Prosser, P.; and Stuckey, P. J. 2019. Constraints for symmetry breaking in graph representation. *Constraints*, 24: 1–24.

Conlon, D.; Fox, J.; and Sudakov, B. 2015. Recent developments in graph Ramsey theory. *Surveys in combinatorics*, 424(2015): 49–118.

Ganesh, V.; O'Donnell, C. W.; Soos, M.; Devadas, S.; Rinard, M. C.; and Solar-Lezama, A. 2012. Lynx: A Programmatic SAT Solver for the RNA-Folding Problem. In *SAT 2012*, 143–156. Springer Berlin Heidelberg.

Ganesh, V.; and Vardi, M. Y. 2021. On the Unreasonable Effectiveness of SAT Solvers. *Beyond the Worst-Case Analysis of Algorithms*, 547–566.

Grinstead, C. M.; and Roberts, S. M. 1982. On the Ramsey numbers $R(3,8)$ and $R(3,9)$. *Journal of Combinatorial Theory, Series B*, 33(1): 27–51.

Li, Z.; Bright, C.; and Ganesh, V. 2022. An SC-Square Approach to the Minimum Kochen–Specker Problem. In *SC-Square@FLoC 2022*.

Li, Z.; Bright, C.; and Ganesh, V. 2023. A SAT Solver and Computer Algebra Attack on the Minimum Kochen–Specker Problem. *arXiv preprint arXiv:2306.13319*.

Liang, J. H.; Ganesh, V.; Poupart, P.; and Czarnecki, K. 2016. Learning Rate Based Branching Heuristic for SAT Solvers. In *SAT 2016*, 123–140.

McKay, B. D.; and Min, Z. K. 1992. The value of the Ramsey number $R(3,8)$. *Journal of Graph Theory*, 16(1): 99–105.

Radziszowski, S. 2011. Small Ramsey Numbers. *The electronic journal of combinatorics*, 1000: DS1–Aug.

Ramsey, F. P. 1930. On a Problem of Formal Logic. *Proceedings of the London Mathematical Society*, s2-30(1): 264–286.

Wetzler, N.; Heule, M. J. H.; and Hunt Jr, W. A. 2014. DRAT-trim: Efficient checking and trimming using expressive clausal proofs. In *SAT 2014*, 422–429. Springer.