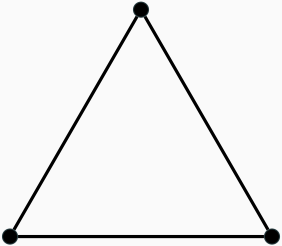
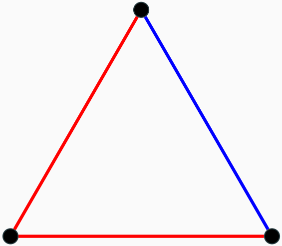
A Formal Proof of R(4,5)=25

Thibault Gauthier, Chad Brown

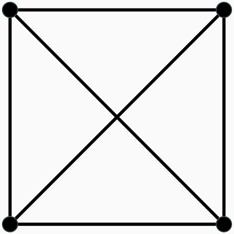
A complete graph of size 3



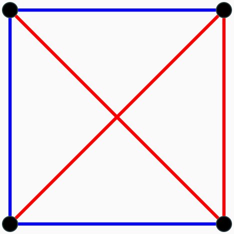
A blue-red coloring of a complete graph size 3 avoiding blue 3-cliques and red 3-cliques



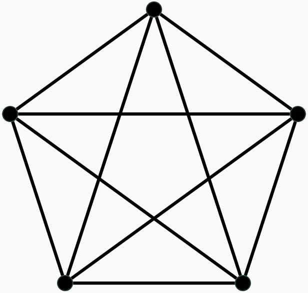
A complete graph of size 4



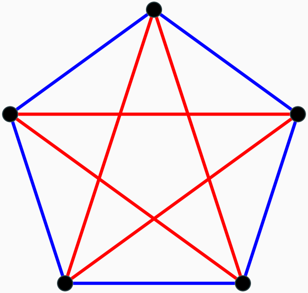
A blue-red coloring of a complete graph of size 4 avoiding blue 3-cliques and red 3-cliques



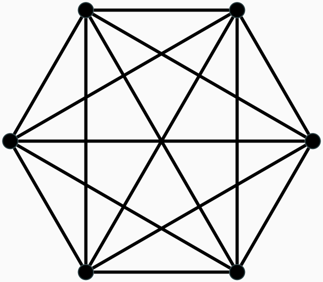
A complete graph of size 5



A blue-red coloring of a complete graph of size 5 avoiding blue 3-cliques and red 3-cliques



A complete graph of size 6



Definition of the Ramsey Number

The Ramsey number $R(n, m)$ is the smallest k such that:

- it is not possible to find a coloring of the complete graph of size k which avoids blue n-cliques and red m-cliques.

Example: $R(3, 3) = 6$

The set of graphs (modulo isomorphism) of size k which avoid blue n-cliques and red m-cliques is noted $\mathcal{R}(n, m, k)$.
A graph in $\mathcal{R}(n, m, k)$ will be called a $\mathcal{R}(n, m, k)$-graph.

Example: $\mathcal{R}(3, 3, 5) \neq \emptyset$ and $\mathcal{R}(3, 3, 6) = \emptyset$

We rely on the nauty algorithm to normalize graphs.

Why prove that R(4,5) = 25?

Is it simple, general, surprising, enlightening, beautiful?

Why prove that R(4,5) = 25?

Is it simple, general, surprising, enlightening, beautiful?

“Suppose aliens invade the earth and threaten to obliterate it in a year’s time unless human beings can find R(5,5). We could marshal the world’s best minds and fastest computers, and within a year we could probably calculate the value. If the aliens demanded R(6,6), however, we would have no choice but to launch a preemptive attack.” Paul Erdős

Why prove that R(4,5) = 25?

Is it simple, general, surprising, enlightening, beautiful?

“Suppose aliens invade the earth and threaten to obliterate it in a year’s time unless human beings can find R(5,5). We could marshal the world’s best minds and fastest computers, and within a year we could probably calculate the value. If the aliens demanded R(6,6), however, we would have no choice but to launch a preemptive attack.” Paul Erdős

How do we find the value of $R(5, 5)$ to avoid imminent death?
$R(4, 5) = 25$ is an important lemma.

Why formally prove that $R(4, 5) = 25$?

The proof relies on mathematical arguments and a very large computation.
(multiple CPU years at the time)

Both of these parts could have errors/bugs.

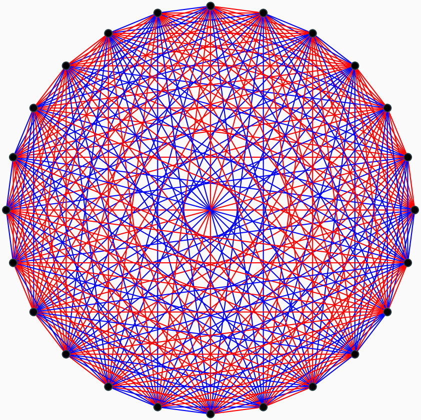
With a formal proof, we can be certain that $R(4, 5) = 25$.
(as long as the HOL4 kernel is sound)

How to prove that R(4,5) = 25?

We will prove that $\mathcal{R}(4,5,24) \neq \emptyset$ and that $\mathcal{R}(4,5,25) = \emptyset$.

$\mathcal{R}(4, 5, 24) \neq \emptyset$

The first person to find a $\mathcal{R}(4, 5, 24)$-graph is Kalbfleisch in 1965.
The picture shows the verified $\mathcal{R}(4, 5, 24)$-graph (from McKay's website).



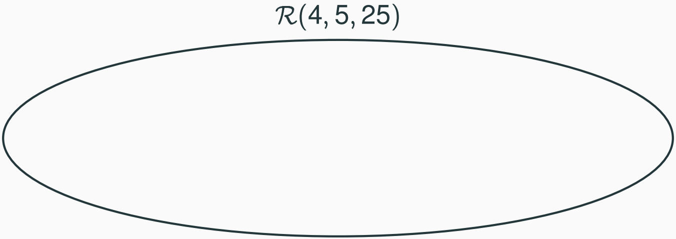
The verification took 10 minutes by a simple search algorithm.
(algorithms for the maximum clique problem can take less than a millisecond)

How to prove that $\mathcal{R}(4,5,25) = \emptyset$?

- Idea 1: enumerate all $\mathcal{R}(4,5,25)$-graphs
  ($2^{(25\times 24)/2} = 2^{300} \approx 10^{90}$)
- Idea 2: enumerate all $\mathcal{R}(4,5,25)$-graphs modulo isomorphism
  (about $2^{300}/25! \approx 10^{65}$)
- Idea 3: encode blue 4-cliques and red 5-cliques as SAT clauses
- Idea 4: add symmetry-breaking clauses (and parallelism)
- Plan: McKay and Radziszowski proved than $\mathcal{R}(4,5,25) = \emptyset$.
  Verify their arguments and replace their gluing algorithm by a SAT solver.

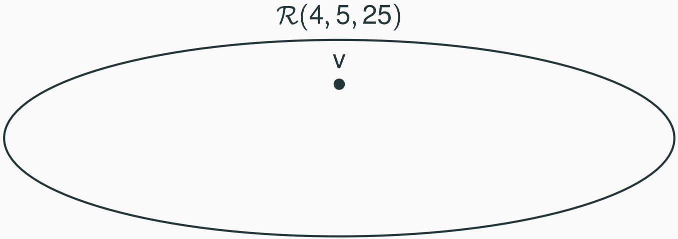
Plan

Suppose that there exists a $\mathcal{R}(4, 5, 25)$-graph



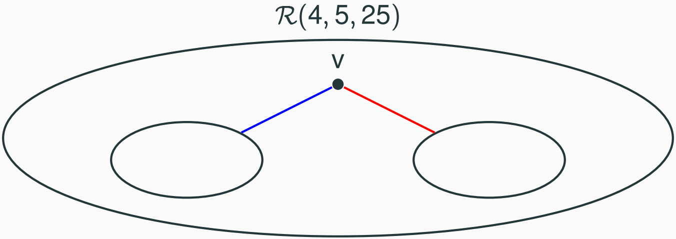
Plan

Pick a vertex v in that $\mathcal{R}(4, 5, 25)$-graph



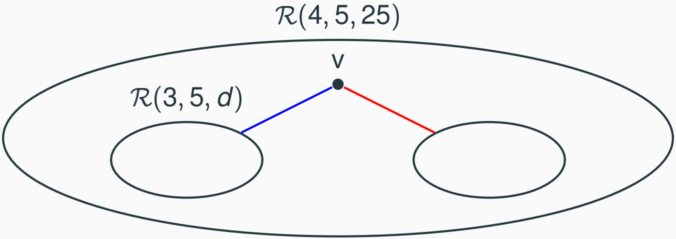
Plan

Consider the blue neighbors of v and the red neighbors of v



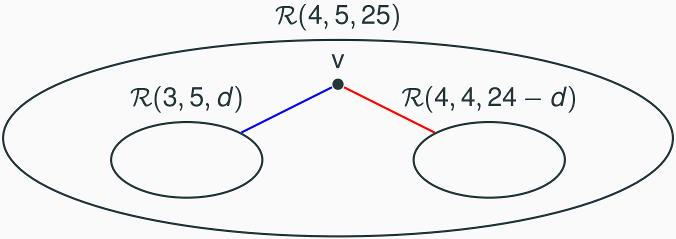
Plan

Prove that the blue neighbors form a $\mathcal{R}(3,5,d)$-graph



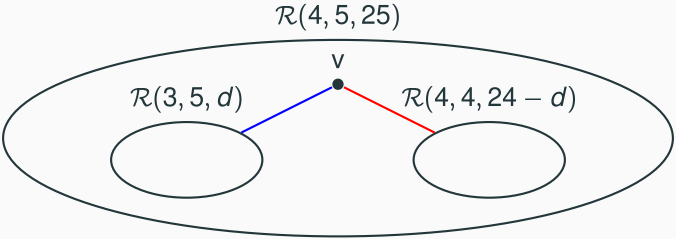
Plan

Prove that the red neighbors form a $\mathcal{R}(4, 4, 24 - d)$-graph



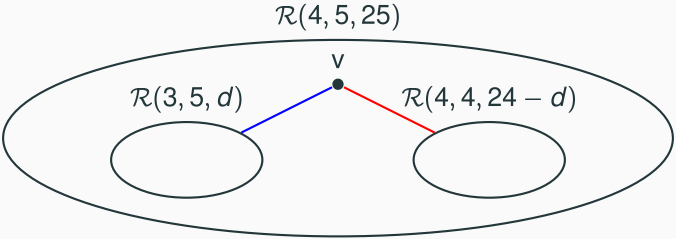
Plan

Prove that the vertex v, any $\mathcal{R}(3, 5, d)$-graph and any $\mathcal{R}(4, 4, 24 - d)$-graph can not occur together disjointly in a $\mathcal{R}(4, 5, 25)$-graph.
These problems are gluing problems.



$7 \leq d \leq 13$

From $\mathcal{R}(3, 5, 14) = \emptyset$, we get $d \leq 13$.
From $\mathcal{R}(4, 4, 18) = \emptyset$, we get $24 - d \leq 17$ and thus $7 \leq d$.



In a $\mathcal{R}(4, 5, 25)$-graph, there exists a vertex of even degree

The sum of the degree of the vertices of a graph is even.
(it is two times the number of edges)

In a graph with 25 vertices, if all vertices have odd degree then the sum of the degree of the vertices of that graph is odd.

Therefore, there exists a vertex with even degree.

Choose for v a vertex of even degree d.
Thus, we now have three cases $d = 8$, $d = 10$ or $d = 12$.

Estimated time for solving gluing problems

d	$\lvert\mathcal{R}(3,5,d)\rvert$	$\lvert\mathcal{R}(4,4,24-d)\rvert$	|problems|	CPU-days
8	179	2	358	0.055
10	313	130816	40945408	8373
12	12	1449166	17389992	7702

How do we estimate the expected gluing time for each d?

- Sample 200 random problems
- Measure average time taken by the HOL4 interface to MiniSat

Strategy for reducing the gluing time

Avoid duplicating work by regrouping similar problems

Regroup similar graphs into generalizations

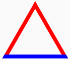
Lead to fewer problems but more difficult ones

Regrouping similar graphs into generalizations

$\mathcal{R}(3,5,3) = \{$  ,  ,  $\}$

Regrouping similar graphs into generalizations

$\mathcal{R}(3,5,3) = \{$  ,  ,  $\}$

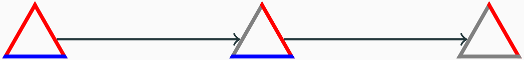


Regrouping similar graphs into generalizations

$\mathcal{R}(3, 5, 3) = \{$  ,  ,  $\}$

Regrouping similar graphs into generalizations

$\mathcal{R}(3,5,3) = \{$  ,  ,  $\}$



Regrouping similar graphs into generalizations

$\mathcal{R}(3,5,3) = \{$  ,  ,  $\}$

$\mathcal{R}^*(3,5,3) = \{$  $\}$

Regrouping similar graphs into generalizations

$\mathcal{R}(3,5,3) = \{$  $\}$

$\mathcal{R}^*(3,5,3) = \{$  $\}$

Heuristics:

- minimize overlap between generalizations
- preserves large monochromatic cliques (small clauses)

Regrouping similar graphs into generalizations

$\mathcal{R}(3,5,3) = \{$  ,  ,  $\}$

$\mathcal{R}^*(3,5,3) = \{$  $\}$

Heuristics:

- minimize overlap between generalizations
- preserves large monochromatic cliques (small clauses)

In the original proof:

- vertices were removed instead of edges.
- the heuristic was based on the number of blue(or red) edges.

Improvements in estimated time

	Graphs				Generalizations			
d	3,5,d	4,4,24-d	problems	days	3,5,d	4,4,24-d	problems	days
8	179	2	358	0.055	27	2	54	0.018
10	313	130816	40945408	8373	43	11752	505336	572
12	12	1449166	17389992	7702	12	26845	322140	374

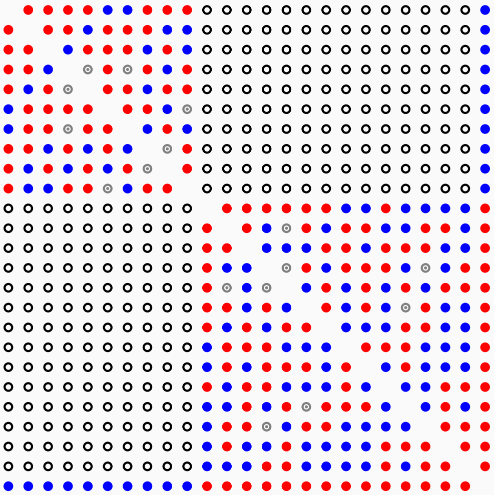
Improvements in estimated time

	Graphs				Generalizations			
d	3,5,d	4,4,24-d	problems	days	3,5,d	4,4,24-d	problems	days
8	179	2	358	0.055	27	2	54	0.018
10	313	130816	40945408	8373	43	11752	505336	572
12	12	1449166	17389992	7702	12	26845	322140	374

Formal proof that generalizations cover all graphs:

- an internal first-order solver for graphs
- isomorphism by renaming: vertices are represented by variables

Adjacency matrix of a gluing problem



A vertex, a $\mathcal{R}^*(3,5,10)$-generalization and a $\mathcal{R}^*(4,4,14)$-generalization.
Prove that it is not possible to color the black edges and the gray edges.

Encoding a gluing problem into SAT

Create one propositional variable $E_{a,b}$ for each edge in the graph.
$E_{a,b}$ is true if the edge (a, b) is blue.
$E_{a,b}$ is false if the edge (a, b) is red.

No blue 4-clique. For each subset S of size 4, create the clause:

$$\bigvee_{a,b \in S \wedge a < b} \neg E_{a,b}$$

No red 5-clique. For each subset T of size 5, create the clause:

$$\bigvee_{a,b \in T \wedge a < b} E_{a,b}$$

Add the unit clause $E_{a,b}$ if an edge (a, b) is blue in the matrix.
Add the unit clause $\neg E_{a,b}$ if an edge (a, b) is red in the matrix.

Unsatisfiable = cannot color the remaining edges (black and gray).

Formally proving the gluing problems

We call the HOL4 interface to MiniSat on each gluing problem.
I would like to thank Weber and Amjad for developing this interface.
The interface works by calling MiniSat which produces a proof trace that is replayed in HOL4.

This produced 827,530 gluing lemmas in approximately 1,440 CPU-days.
(higher than the estimated 946 CPU-days)

Conclusion

We have formally proven that $R(4,5) = 25$ in the HOL4 theorem prover.

In summary, $\mathcal{R}(4,5,25) = \emptyset$ can be deduced by contradiction from:

- the existence of a vertex of degree $d \in \{8,10,12\}$,
- Enumeration of $\mathcal{R}(3,5,d)$ and $\mathcal{R}()4,4,24-d)$ graphs.
- generalizations forming a cover,
- gluing lemmas.

Is there a simpler proof of $R(4,5) = 25$?
Could our approach help to prove that $R(5,5) = 43$?