Short hand-checkable certificates for bounds on the Ramsey number $R(5,5)$

Ali Asaria
ali@lab.cloud

Abstract

We prove bounds on the diagonal Ramsey number $R(5,5)$ by certificates short enough to check by hand, using a symmetry reduction for Paley graphs and classical counting arguments. Specific results that we prove include: the clique number of the Paley graph of order 37, from one displayed subgraph, giving $R(5,5) \geq 38$, and of order 17, giving $R(4,4) \geq 18$; a self-contained proof of the Shearer–Mathon doubling bound, which yields $R(5,5) \geq 37$ independently; $R(5,5) \leq 50$ from the classical recursion with the computer-verified value $R(4,5) = 25$, and $R(5,5) \leq 62$ with no computational input; and a proof that a subgraph-counting identity of McKay and Radziszowski cannot yield $R(5,5) \leq 49$ from the computed extremal edge counts alone.

1 Introduction

The *Ramsey number* $R(s,t)$ is the least number n of vertices at which every graph contains a clique of s pairwise-adjacent vertices or an independent set of t pairwise non-adjacent vertices. Equivalently, if the edges of the complete graph K_n are coloured red and blue, then for $n \geq R(s,t)$ a red K_s or a blue K_t must appear, no matter how the colouring is chosen. The existence of these numbers is Ramsey's theorem [Ram30], and the difficulty of computing them, even for single-digit s and t, is documented at length in the survey of record [Rad26].

The problem

Throughout this paper all graphs are finite, simple and undirected. For a graph G we write $\omega(G)$ for its clique number, $\alpha(G)$ for its independence number, $N(v)$ for the neighbourhood of a vertex v, and $G[X]$ for the subgraph induced on a set X of vertices. A graph G on n vertices satisfying

$$\omega(G) \leq s-1 \qquad \text{and} \qquad \alpha(G) \leq t-1 \tag{1}$$

will be called an (s,t)-*Ramsey graph*; the existence of such a graph is precisely the statement $R(s,t) > n$. The values $R(3,3) = 6$, $R(3,4) = 9$, $R(3,5) = 14$ and $R(4,4) = 18$ were determined by Greenwood and Gleason in 1955 by arguments a reader can check entirely by hand [GG55], and $R(4,5) = 25$ was determined by McKay and Radziszowski in 1995 by a large computation [MR95], since verified end to end in the HOL4 proof assistant [GB24]. For $R(5,5)$ the published record is

$$43 \;\leq\; R(5,5) \;\leq\; 46, \tag{2}$$

the lower bound resting on an explicit colouring of K_{42} found by Exoo [Exo89] and the upper bound on a computation by Angeltveit and McKay whose two independent implementations consumed roughly eighty processor-years [AM24]; the value $R(5,5) = 43$ is conjectured [Rad26]. Radziszowski's dynamic survey [Rad26] is the reference of record for all of these facts.

Certificates checkable by hand

This paper asks how much of the bracket (2) survives when every step of every proof must be checkable by a reader from the printed page: definitions stated, each step justified by a named earlier step or a cited theorem, each certificate displayed in closed form. The question is sharpened by the state of the record bounds, which sit firmly in the computational regime, and the experts' own assessment is that further progress by the same route would require an excessive amount of computer time [AM24]. A recent line of work applies machine search, including reinforcement learning in the programme initiated by Wagner, to the construction of Ramsey witnesses; the resulting graphs are certified by machine subgraph counting, so their correctness is again a computational fact [Wag21, GAYKS24]. In the other direction, Ge, Jayasooriya, Qiu, Sun and Yuan have given a fully hand-checkable proof that Exoo's colouring contains no monochromatic K_5, so the record lower bound $R(5,5) \geq 43$ does admit a proof on the page [GJQ+22]. Their argument runs to roughly twenty pages of case analysis, on a colouring that carries only a dihedral symmetry; Remark 9 returns to what that costs. Hand-checkability is therefore not a property this paper introduces, and priority for a hand-checkable certificate at the record bound belongs to [GJQ+22]. The present paper occupies the opposite corner of the trade-off: we accept weaker bounds in exchange for certificates that are short, and the brevity is bought by symmetry.

Paley graphs

For a prime $q \equiv 1 \pmod 4$, write $\mathbb{F}_q$ for the field of q elements, $\mathbb{F}_q^*$ for its nonzero elements, and

$$\mathrm{QR}(q) = \{\, x^2 : x \in \mathbb{F}_q^* \,\} \tag{3}$$

for its set of nonzero squares, the *quadratic residues*; the nonzero elements outside $\mathrm{QR}(q)$ are the non-residues. The *Paley graph* P_q has vertex set $\mathbb{F}_q$, with x and y adjacent exactly when $x - y \in \mathrm{QR}(q)$. The condition $q \equiv 1 \pmod 4$ makes -1 a square, by Euler's criterion, so the relation is symmetric and the definition is sound. Paley graphs are the classical algebraic witnesses for diagonal Ramsey lower bounds: Greenwood and Gleason's proof of $R(4,4) \geq 18$ exhibits P_{17} [GG55], and the survey records the general mechanism by which a P_p with no K_k certifies $R(k,k) \geq p+1$ [Rad26]. The clique number of P_{37} appears in Shearer's tables of computed values [She86], but we have found no written derivation of it in the literature, and the present paper supplies one. One reference we could not obtain, Broere, Doman and Ridley on the clique and chromatic numbers of certain Paley graphs [BDR88], treats small Paley graphs directly; we are unable to say whether a derivation for $q = 37$ is already to be found there.

Overview of results

Our results rest on one tool: a reduction lemma for edge-transitive graphs, by which the clique number of P_q is read off from a single induced subgraph on $(q-5)/4$ vertices, displayed explicitly as a table of quadratic residues. The notion of a certificate displayed in closed form plays the

central role throughout. Each result below completes, shortens, or delimits a proof of a statement already on record, and the attribution is given where it is proved. The following specific results are among those we prove:

- The Paley graphs of orders 5, 17 and 37 have clique numbers 2, 3 and 4 respectively, each determined by the reduction lemma and a displayed case analysis. Consequently $R(3,3) \geq 6$, $R(4,4) \geq 18$ and $R(5,5) \geq 38$, all by one two-step argument. The third bound is weaker than the record (2), and Section 3 makes precise what the twenty-page analysis of [GJQ+22] buys that these two pages do not.
- A self-contained proof of the doubling bound of Shearer [She86] and Mathon [Mat87]: if P_p contains no K_k, then an explicit graph on $2p+2$ vertices built from two copies of P_p is a $(k+1,k+1)$-Ramsey graph, so $R(k+1,k+1) \geq 2p+3$. The retrievable literature states this bound and sketches its key step; we display the construction and prove every case. Applied to P_{17} it gives $R(5,5) \geq 37$, independently of the analysis of P_{37}.
- The upper bound $R(5,5) \leq 50$, from the classical recursion of Erdős and Szekeres [ES35] with the cited value $R(4,5) = 25$ [MR95, GB24], and the bound $R(5,5) \leq 62$ whose proof uses no computational input whatsoever. Along the way the four classical values of Greenwood and Gleason are re-derived in full, including the independence analysis of the cubic-residue colouring modulo 13 that the original paper asserted without proof.
- An account of why the hand routes catalogued in the survey [Rad26] stop at 50: the parity refinement of the recursion does not apply at $(5,5)$; Walker's inequality [Wal68] yields only 58; and the subgraph-counting identity that opened the computational route of McKay and Radziszowski [MR97] is exactly feasible on 49 vertices, in a sense that forces every vertex neighbourhood of a hypothetical $(5,5)$-Ramsey graph on 49 vertices to be an edge-maximal $(4,5)$-Ramsey graph on 24 vertices, yet provably cannot deliver a contradiction from extremal edge counts alone.

2 A reduction lemma for edge-transitive graphs

This section assembles the tool used by every lower bound in the paper. The facts about Paley graphs are classical; we prove them to keep the certificate chain self-contained, and because each proof is a few lines.

Automorphisms of Paley graphs

Proposition 1. *Let $q \equiv 1 \pmod 4$ be prime, let $a \in \mathrm{QR}(q)$ and let $b \in \mathbb{F}_q$. Then the map $\varphi_{a,b}(x) = ax + b$ is an automorphism of P_q. Moreover, for any two ordered pairs (x,y) and (x',y') of adjacent vertices there is an automorphism of this form carrying x to x' and y to y'; in particular P_q is vertex-transitive and edge-transitive.*

Proof. It will first be proved that $\varphi_{a,b}$ preserves adjacency. The map is a bijection of $\mathbb{F}_q$, and

$$\varphi_{a,b}(x) - \varphi_{a,b}(y) = a\,(x-y). \tag{4}$$

The set $\mathrm{QR}(q)$ is a subgroup of the multiplicative group $\mathbb{F}_q^*$, so for $a \in \mathrm{QR}(q)$ the product $a(x-y)$ lies in $\mathrm{QR}(q)$ exactly when $x-y$ does, and edges map to edges while non-edges map to non-edges. Now let (x,y) and (x',y') be ordered pairs of adjacent vertices. Since $q \equiv 1 \pmod 4$, the

element -1 is a square, so $y-x$ and $y'-x'$ both lie in $\mathrm{QR}(q)$, and

$$a = (y'-x')\,(y-x)^{-1} \tag{5}$$

is a ratio of two squares and hence a square. The automorphism $\varphi_{a,\,x'-ax}$ carries x to x' and y to $a(y-x)+x' = y'$, which completes the proof. □

Proposition 2. *Let $q \equiv 1 \pmod 4$ be prime and let $g \in \mathbb{F}_q^*$ be a non-residue. Then $\psi(x) = gx$ is an isomorphism from P_q to its complement, and consequently $\alpha(P_q) = \omega(P_q)$.*

Proof. It will be proved that ψ carries edges exactly onto non-edges. The map ψ is a bijection of $\mathbb{F}_q$ and $\psi(x)-\psi(y) = g(x-y)$. Multiplication by the non-residue g carries $\mathrm{QR}(q)$ onto the set of non-residues and the non-residues onto $\mathrm{QR}(q)$, so ψ carries edges of P_q exactly onto non-edges. Hence the complement of P_q is isomorphic to P_q itself, and $\alpha(P_q)$, which is the clique number of the complement, equals $\omega(P_q)$. □

The reduction lemma

For adjacent vertices u and v of a graph G we write

$$S(u,v) = N(u) \cap N(v) \tag{6}$$

for the common neighbourhood of the edge $\{u,v\}$. We adopt the convention that the clique number of a graph with no vertices is 0, while a graph with vertices and no edges has clique number 1.

Lemma 3. *Let G be an edge-transitive graph containing at least one edge $\{u,v\}$. It holds that*

$$\omega(G) = 2 + \omega\big(G[S(u,v)]\big). \tag{7}$$

Proof. It will first be proved that the left side of (7) is at least the right side. If C is a clique of $G[S(u,v)]$, then every vertex of C is adjacent to both u and v, so $C \cup \{u,v\}$ is a clique of G, and $\omega(G) \geq |C|+2$. Now let K be a clique of G of maximum size. Since G has an edge, whose two endpoints form a clique of size 2, it holds that $|K| \geq 2$, so K contains an edge $\{x,y\}$. By edge-transitivity there is an automorphism of G carrying the edge $\{x,y\}$ to the edge $\{u,v\}$, in one orientation or the other; either way its image K' is a clique of the same size containing both u and v. Every vertex of $K' \setminus \{u,v\}$ is adjacent to both u and v, so $K' \setminus \{u,v\}$ is a clique of $G[S(u,v)]$ of size $|K|-2$, which completes the proof. □

The specialisation to Paley graphs

Let us now return to Paley graphs, and fix, here and for the rest of the paper, the edge $\{0,1\}$ of P_q as the representative edge, so that

$$S_q = S(0,1) = \{\, x \in \mathbb{F}_q : x \in \mathrm{QR}(q) \text{ and } x-1 \in \mathrm{QR}(q) \,\}. \tag{8}$$

The size of this set is determined by a classical character computation, which we include as a consistency check on the displayed tables; none of the theorems below depends on it, because in each instance the set S_q is listed exhaustively.

Proposition 4. *Let $q \equiv 1 \pmod 4$ be prime and let u, v be adjacent vertices of P_q. It holds that $|S(u,v)| = (q-5)/4$.*

Proof. By Proposition 1 it may be assumed that $u = 0$ and $v = 1$. Let χ denote the quadratic character of $\mathbb{F}_q$, so that $\chi(x) = 1$ for $x \in \mathrm{QR}(q)$, $\chi(x) = -1$ for x a non-residue, and $\chi(0) = 0$; χ is multiplicative, exactly half of $\mathbb{F}_q^*$ satisfies $\chi(x) = 1$, and $\chi(-1) = 1$ because $q \equiv 1 \pmod 4$. For $x \notin \{0,1\}$ the membership $x \in S_q$ is equivalent to $\chi(x) = \chi(x-1) = 1$, so

$$|S_q| = \frac{1}{4} \sum_{x \neq 0,1} \big(1 + \chi(x)\big)\big(1 + \chi(x-1)\big). \tag{9}$$

The four terms of the expansion are evaluated separately. The constant term contributes $q-2$. Since the character sums to zero over all of $\mathbb{F}_q$, it holds that

$$\sum_{x \neq 0,1} \chi(x) = -\chi(1) = -1, \qquad \sum_{x \neq 0,1} \chi(x-1) = -\chi(-1) = -1, \tag{10}$$

the second sum by the substitution $y = x - 1$, which omits the values $y = -1$ and $y = 0$. For the cross term, $\chi(x)\chi(x-1) = \chi(x^2)\,\chi(1 - x^{-1}) = \chi(1 - x^{-1})$ for $x \neq 0$, and as x ranges over $\mathbb{F}_q^*$ the quantity $1 - x^{-1}$ ranges over $\mathbb{F}_q \setminus \{1\}$, so

$$\sum_{x \neq 0,1} \chi(x)\chi(x-1) = \sum_{z \neq 1} \chi(z) = -\chi(1) = -1. \tag{11}$$

Combining the four terms gives $|S_q| = \frac{1}{4}\,(q - 2 - 1 - 1 - 1) = (q-5)/4$, which completes the proof. □

In order to prove $\omega(P_q) \leq k$, it therefore suffices to list the set S_q from the table of squares modulo q and to verify, on the page, that the graph induced on S_q contains no K_{k-2}; the bound $\alpha(P_q) \leq k$ then follows at no cost from Proposition 2.

3 Clique numbers of the Paley graphs on 5, 17, and 37 vertices

The three Paley graphs of this section certify lower bounds on the three diagonal Ramsey numbers $R(3,3)$, $R(4,4)$ and $R(5,5)$ by one and the same two-step argument, applied to sets S_q of sizes 0, 3 and 8. The graph P_{17} is in fact the unique $(4,4)$-Ramsey graph on 17 vertices, by a theorem of Kalbfleisch [Kal66]; see also Evans, Pulham and Sheehan [EPS81]. The corresponding question one level up, whether some other member of the family does better than P_{37} for $R(5,5)$, is settled in the negative in Remark 9. The smallest instance is immediate: $\mathrm{QR}(5) = \{1,4\}$, and no x satisfies both $x \in \mathrm{QR}(5)$ and $x - 1 \in \mathrm{QR}(5)$, so S_5 is empty, Lemma 3 gives $\omega(P_5) = 2$, Proposition 2 gives $\alpha(P_5) = 2$, and the pentagon P_5 is a $(3,3)$-Ramsey graph on 5 vertices, so that $R(3,3) \geq 6$.

Theorem 5. *It holds that $\omega(P_{17}) = \alpha(P_{17}) = 3$, and consequently $R(4,4) \geq 18$.*

Proof. The proof lists the set S_{17} from the residues modulo 17, finds that it induces no edge, and applies Lemma 3. The squares of $1, \ldots, 8$ modulo 17 give

$$\mathrm{QR}(17) = \{1,2,4,8,9,13,15,16\}. \tag{12}$$

Walking this list, the elements x with $x-1$ also in $\mathrm{QR}(17)$ are exactly

$$S_{17} = \{2, 9, 16\}. \tag{13}$$

The three pairwise differences of S_{17} are $9-2=7$, $16-9=7$ and $16-2=14$, and neither 7 nor 14 lies in $\mathrm{QR}(17)$, so the graph induced on S_{17} has no edge and its clique number is 1. Lemma 3 gives $\omega(P_{17}) = 2+1 = 3$, and Proposition 2 gives $\alpha(P_{17}) = 3$. Thus P_{17} is a $(4,4)$-Ramsey graph on 17 vertices, so that $R(4,4) \geq 18$, which completes the proof. □

Remark 6. The bound of Theorem 5 is attained: Proposition 19 below gives $R(4,4) = 18$, so P_{17} is an extremal witness, and by the theorem of Kalbfleisch quoted above it is the only one on 17 vertices.

Theorem 7. *It holds that $\omega(P_{37}) = \alpha(P_{37}) = 4$, and consequently $R(5,5) \geq 38$.*

Proof. The proof lists the set S_{37} from the residues modulo 37, shows by three cases that the graph it induces has an edge but no triangle, and applies Lemma 3. The squares of $1, \ldots, 18$ modulo 37 give

$$\mathrm{QR}(37) = \{1, 3, 4, 7, 9, 10, 11, 12, 16, 21, 25, 26, 27, 28, 30, 33, 34, 36\}. \tag{14}$$

Walking this list, the elements x with $x-1$ also in $\mathrm{QR}(37)$ are exactly

$$S_{37} = \{4, 10, 11, 12, 26, 27, 28, 34\}, \tag{15}$$

a set of $(37-5)/4 = 8$ elements, in agreement with Proposition 4. The 28 pairwise differences of S_{37}, with the members of $\mathrm{QR}(37)$ underlined, are

$$\begin{array}{llll} 11-4=\underline{7}, & 34-4=\underline{30}, & 11-10=\underline{1}, & 26-10=\underline{16}, \\ 12-11=\underline{1}, & 27-11=\underline{16}, & 28-12=\underline{16}, & 27-26=\underline{1}, \\ 28-27=\underline{1}, & 34-27=\underline{7}, & 10-4=6, & 12-4=8, \\ 26-4=22, & 27-4=23, & 28-4=24, & 12-10=2, \\ 27-10=17, & 28-10=18, & 34-10=24, & 26-11=15, \\ 28-11=17, & 34-11=23, & 26-12=14, & 27-12=15, \\ 34-12=22, & 28-26=2, & 34-26=8, & 34-28=6. \end{array} \tag{16}$$

The graph induced on S_{37} therefore has exactly the ten edges

$$\begin{array}{l} \{4,11\},\ \{4,34\},\ \{10,11\},\ \{10,26\},\ \{11,12\}, \\ \{11,27\},\ \{12,28\},\ \{26,27\},\ \{27,28\},\ \{27,34\}, \end{array} \tag{17}$$

and every one of these edges is incident to 11, incident to 27, or belongs to the perfect matching

$$M = \{\{4,34\},\ \{10,26\},\ \{12,28\}\} \tag{18}$$

on the remaining six vertices. It will now be proved that the graph induced on S_{37} contains no triangle, by three cases. If a triangle contains the vertex 11, its other two vertices form an edge inside $N(11) \cap S_{37} = \{4, 10, 12, 27\}$; the six differences $10-4=6$, $12-4=8$, $27-4=23$, $12-10=2$, $27-10=17$ and $27-12=15$ all lie outside $\mathrm{QR}(37)$ by (16), so no such edge exists. If a triangle contains 27 and avoids 11, its other two vertices form an edge inside $\{26, 28, 34\}$; the differences $28-26=2$, $34-26=8$ and $34-28=6$ lie outside $\mathrm{QR}(37)$, so no such edge

exists. If a triangle avoids both 11 and 27, all three of its edges lie in the matching M of (18), and two edges of a matching never share a vertex. Hence the graph induced on S_{37} is triangle-free, and its clique number is 2, an edge being present by (17). Lemma 3 gives $\omega(P_{37}) = 2+2 = 4$; explicitly, the four vertices $\{0,1,11,12\}$ form a clique, their six differences being $1, 11, 12, 10, 11, 1$, all in $\mathrm{QR}(37)$. Proposition 2 gives $\alpha(P_{37}) = 4$. Thus P_{37} is a $(5,5)$-Ramsey graph on 37 vertices, so that $R(5,5) \geq 38$, which completes the proof. □

Remark 8. The map $\sigma(x) = 1 - x$ is the automorphism $\varphi_{-1,1}$ of P_{37}; it swaps 0 and 1, so it maps S_{37} to itself, pairing it as $\{4,34\}$, $\{10,28\}$, $\{11,27\}$, $\{12,26\}$ with no fixed point, since $2x = 1$ has the solution $x = 19 \notin \mathrm{QR}(37)$. The edge list (17) is invariant under σ, and the second case of the triangle analysis is the σ-image of the first; a reader checking the tables may use this symmetry to halve the work.

The displayed tables (12) through (17) may also be confirmed by a direct symbolic computation; scripts that do so are among the artifacts described at the end of the paper.

Remark 9. The gap between 38 and the record lower bound 43 is structural for the methods of this section, and P_{37} is the last member of its family to which they apply. The next Paley graph, P_{41}, contains the clique $\{0,1,5,9,10\}$, whose ten differences take the six values $1 = 1^2$, $4 = 2^2$, $5 \equiv 13^2$, $8 \equiv 7^2$, $9 = 3^2$ and $10 \equiv 16^2$ modulo 41, all of them squares; so $\omega(P_{41}) \geq 5$ and P_{41} is not a $(5,5)$-Ramsey graph, while for the larger primes Shearer's tables report clique numbers of 5 and more [She86]. Beyond the family, the best $(5,5)$-Ramsey graph that is a circulant of any modulus has order 41, a computational result of Harborth and Krause re-certified by integer programming [HK03, CFL+26], and no cyclic construction on fewer than 102 vertices improves any lower bound in the survey's table [Rad26]. Exoo's graph on 42 vertices is not vertex-transitive, so the hand-checkable analysis of it in [GJQ+22] cannot use Lemma 3 and proceeds one family of potential cliques at a time; we take its twenty pages to be largely the price of that missing symmetry, though we have not tried to separate that cost from the exposition around it.

4 A doubled Paley graph on 36 vertices

Shearer [She86], and later but independently Mathon [Mat87], described a construction that doubles a Paley graph: if P_p contains no K_k, the construction produces a $(k+1,k+1)$-Ramsey graph on $2p+2$ vertices, so that $R(k+1,k+1) \geq 2p+3$. This bound underlies several of the best known diagonal lower bounds, including $R(7,7) \geq 205$ from P_{101} [Rad26, XXER04]. The sources available to us state the construction and its key computation in outline; Xu, Xie, Exoo and Radziszowski, who merge the same idea into a three-colour construction, invoke the final step with the words that the argument is the same as in the Paley doubling construction of Shearer [XXER04]. Since a displayed proof of the two-colour bound does not appear in any source we can retrieve, we give one here, self-contained; the construction is due to Shearer and Mathon, and the presentation and case analysis below are our own.

Definition 10. Let $p \equiv 1 \pmod 4$ be prime. The *doubled Paley graph* H_p has the $2p+2$ vertices

$$V(H_p) = \{u, u'\} \cup \{x_a : a \in \mathbb{F}_p\} \cup \{y_a : a \in \mathbb{F}_p\}, \tag{19}$$

and its edges are given by the following three rules.

1. u is adjacent to x_a for every a and to no other vertex, and u' is adjacent to y_a for every a and to no other vertex; in particular u and u' are not adjacent, u is adjacent to no y_b, and u' is adjacent to no x_a.
2. x_a and x_b are adjacent exactly when $a - b \in \mathrm{QR}(p)$, and likewise y_a and y_b; each copy induces P_p.
3. x_a and y_b are adjacent exactly when $a - b$ is a non-residue; in particular x_a and y_a are not adjacent.

The engine of the proof is the following observation, which is the step Shearer's argument turns on.

Lemma 11. *Let $p \equiv 1 \pmod 4$ be prime, and let $X \subseteq \mathrm{QR}(p)$ and $Y \subseteq \mathbb{F}_p^* \setminus \mathrm{QR}(p)$ be sets such that every difference of two distinct elements of X, and every difference of two distinct elements of Y, lies in $\mathrm{QR}(p)$, while every difference of an element of X and an element of Y lies outside $\mathrm{QR}(p) \cup \{0\}$. Then $T = \{\, t^{-1} : t \in X \cup Y \,\}$ is a clique of P_p, and consequently $|X| + |Y| \le \omega(P_p)$.*

Proof. The sets X and Y are disjoint, since a residue is not a non-residue, and $0 \notin X \cup Y$, so inversion is defined on $X \cup Y$ and $|T| = |X| + |Y|$. Let χ be the quadratic character, as in the proof of Proposition 4, and let $a, b \in X \cup Y$ be distinct. A calculation reveals that

$$a^{-1} - b^{-1} = (b - a)\,(ab)^{-1}, \tag{20}$$

and $\chi\big((ab)^{-1}\big) = \chi(ab)$ because $\chi(z)\chi(z^{-1}) = \chi(1) = 1$ for $z \neq 0$. If $a, b \in X$, then $\chi(b - a) = 1$ by hypothesis and $\chi(ab) = \chi(a)\chi(b) = 1$, so $\chi(a^{-1} - b^{-1}) = 1$. If $a, b \in Y$, then $\chi(b - a) = 1$ and $\chi(ab) = (-1)(-1) = 1$, so again $\chi(a^{-1} - b^{-1}) = 1$. If one of a, b lies in X and the other in Y, then $\chi(b - a) = -1$ and $\chi(ab) = -1$, so $\chi(a^{-1} - b^{-1}) = (-1)(-1) = 1$. In every case $a^{-1} - b^{-1} \in \mathrm{QR}(p)$, so T is a clique of P_p, which completes the proof. □

Theorem 12. *Let $p \equiv 1 \pmod 4$ be prime, let $k \ge 2$, and suppose $\omega(P_p) \le k - 1$. Then $\omega(H_p) \le k$ and $\alpha(H_p) \le k$, and consequently $R(k+1, k+1) \ge 2p + 3$.*

Proof. Throughout the proof, sets $A, B \subseteq \mathbb{F}_p$ denote the index sets of a vertex set's intersection with the two copies, so that the vertices in question are $\{x_a : a \in A\} \cup \{y_b : b \in B\}$.

It will first be proved that $\omega(H_p) \le k$. Let C be a clique of H_p. If $u \in C$, then $u' \notin C$ by rule 1, and no y_a lies in C, so $C \setminus \{u\}$ is a clique of the first copy of P_p and $|C| \le 1 + (k - 1) = k$; the case $u' \in C$ is symmetric. If C avoids u and u' and meets only one copy, then $|C| \le \omega(P_p) \le k - 1$. There remains the case that C avoids u and u' and meets both copies, with index sets $A \neq \emptyset$ and $B \neq \emptyset$. By rules 2 and 3, every difference of two distinct elements of A lies in $\mathrm{QR}(p)$, every difference of two distinct elements of B lies in $\mathrm{QR}(p)$, and every difference of an element of A and an element of B lies outside $\mathrm{QR}(p) \cup \{0\}$; the last condition forces $A \cap B = \emptyset$. Fix $a_0 \in A$ and translate, setting $A' = A - a_0$ and $B' = B - a_0$. Translation preserves every difference, so the same three conditions hold for A' and B', and now $0 \in A'$. Every $a \in A' \setminus \{0\}$ satisfies $a = a - 0 \in \mathrm{QR}(p)$, and every $b \in B'$ satisfies $b = b - 0 \notin \mathrm{QR}(p) \cup \{0\}$, so the pair $\big(A' \setminus \{0\},\ B'\big)$ satisfies the hypotheses of Lemma 11. The lemma gives $(|A| - 1) + |B| \le \omega(P_p) \le k - 1$, so $|C| = |A| + |B| \le k$.

It will now be proved that $\alpha(H_p) \le k$. Let I be an independent set of H_p. If $u \in I$, then no x_a lies in I; if moreover $u' \in I$, then no y_a lies in I and $I = \{u, u'\}$, of size $2 \le k$; and if $u' \notin I$,

then $I \setminus \{u\}$ is an independent set of the second copy of P_p, so $|I| \le 1 + \alpha(P_p) = 1 + \omega(P_p) \le k$ by Proposition 2. The case $u' \in I$ is symmetric. If I avoids u and u' and meets only one copy, then $|I| \le \alpha(P_p) \le k-1$. There remains the case that I avoids u and u' and meets both copies, with index sets $A \ne \emptyset$ and $B \ne \emptyset$. Non-adjacency inside the copies and across them reads: every difference of two distinct elements of A, and of two distinct elements of B, lies outside $\mathrm{QR}(p) \cup \{0\}$, while every difference of an element of A and an element of B lies in $\mathrm{QR}(p) \cup \{0\}$. Suppose first that some $c \in A \cap B$. Any further $a \in A$ with $a \ne c$ would have $a - c$ outside $\mathrm{QR}(p)$, as a difference within A, and simultaneously inside $\mathrm{QR}(p) \cup \{0\}$, as a difference between A and B, with $a - c \ne 0$; this is impossible, and the same argument empties $B \setminus \{c\}$, so $I = \{x_c, y_c\}$, of size $2 \le k$. Suppose instead that $A \cap B = \emptyset$, fix a non-residue g, and set $A^* = gA$ and $B^* = gB$. Multiplication by g is a bijection carrying differences within A^* and within B^* into $\mathrm{QR}(p)$, since a non-residue times a non-residue is a residue, and carrying the cross differences, which are nonzero because $A \cap B = \emptyset$, outside $\mathrm{QR}(p) \cup \{0\}$. The pair (A^*, B^*) therefore satisfies exactly the conditions of the clique case: fixing $a_0 \in A^*$ and translating by $-a_0$ puts 0 into the first set and leaves every difference unchanged, after which Lemma 11 applies to the translate of A^* with 0 removed and the translate of B^*, and gives $(|A| - 1) + |B| \le k - 1$. Hence $|I| = |A| + |B| \le k$.

In every case $|C| \le k$ and $|I| \le k$, so H_p is a $(k+1, k+1)$-Ramsey graph on $2p+2$ vertices, and $R(k+1, k+1) \ge 2p + 3$, which completes the proof. □

Remark 13. The hypothesis of Theorem 12 is vacuous at $k = 2$, since P_p always has an edge and so $\omega(P_p) \ge 2$; the first case carrying content is $k = 3$, where P_5 gives $R(4,4) \ge 13$.

Corollary 14. *It holds that $R(5,5) \ge 37$, by Theorem 12 applied with $p = 17$ and $k = 4$, the hypothesis $\omega(P_{17}) = 3$ being Theorem 5.*

Remark 15. The bound of Corollary 14 is one short of Theorem 7, and the two certificates are independent; both are included because the doubled graph is the general-purpose construction, while the direct analysis of P_{37} happens to beat it at this size. A third elementary route to a lower bound, the merge-of-colours theorem of Xu, Xie, Exoo and Radziszowski [XXER04], gives $R(5,5) \ge 4\,R(3,4) - 3 = 33$ from the value $R(3,4) = 9$ alone, and is dominated by both bounds above. The construction cannot be iterated: every vertex of H_p has degree p, one from rule 1 and $(p-1)/2$ from each of rules 2 and 3, so the complement of H_p is regular of the different degree $p+1$ and H_p is not self-complementary; and H_p lacks the cyclic structure of the graphs it is built from, as its describers note [XXER04].

5 The recursion and the classical values

Everything in this section is classical in substance; the recursion and its parity refinement are due to Erdős and Szekeres [ES35] and to Greenwood and Gleason [GG55], and the four small values are Greenwood and Gleason's. We prove all of it, first because the chain from these facts to $R(5,5) \le 50$ is then checkable end to end from this paper alone, and second because one step, the independence analysis of the cubic-residue colouring modulo 13, is asserted in [GG55] without a written proof.

Proposition 16. *Let H be an induced subgraph of a graph G. It holds that $\omega(H) \le \omega(G)$ and $\alpha(H) \le \alpha(G)$. Consequently, if $n \ge R(s,t)$ then every graph on n vertices has a clique of size s or an independent set of size t.*

Proof. A clique of H is a set of pairwise-adjacent vertices of G, and an independent set of H is a set of pairwise non-adjacent vertices of G, since H is induced; the two inequalities follow. For the consequence, let G have $n \geq R(s,t)$ vertices and let H be the subgraph induced on any $R(s,t)$ of them. By the definition of $R(s,t)$, H has a clique of size s or an independent set of size t, and the inequalities carry it to G. □

Proposition 17. *It holds that $R(2,t) = t$ and $R(s,2) = s$ for all $s,t \geq 2$, and that*

$$R(s,t) \leq R(s-1,t) + R(s,t-1) \tag{21}$$

for all $s,t \geq 3$; consequently every $R(s,t)$ is finite.

Proof. It will first be proved that $R(2,t) = t$, and then the recursion. A graph on t vertices with no clique of size 2 has no edge, so its independence number is t; hence $R(2,t) \leq t$. The empty graph on $t-1$ vertices has clique number 1 and independence number $t-1$, so $R(2,t) > t-1$, and the two bounds give $R(2,t) = t$. Complementation exchanges cliques with independent sets and carries (s,t)-Ramsey graphs to (t,s)-Ramsey graphs, so $R(s,t) = R(t,s)$ for all s and t, and in particular $R(s,2) = s$. Now let $s,t \geq 3$, set $n = R(s-1,t) + R(s,t-1)$, let G be a graph on n vertices, and fix a vertex v, whose neighbourhood $N(v)$ and non-neighbourhood $M(v)$ partition the remaining $n-1$ vertices. Since $|N(v)| + |M(v)| = R(s-1,t) + R(s,t-1) - 1$, at least one of $|N(v)| \geq R(s-1,t)$ and $|M(v)| \geq R(s,t-1)$ holds. In the first case, Proposition 16 applied to $G[N(v)]$, whose order is at least $R(s-1,t)$, gives a K_{s-1} inside $N(v)$, which together with v is a K_s of G, or an independent set of size t. In the second case, the same proposition applied to $G[M(v)]$ gives a K_s, or an independent set of size $t-1$, which together with v is an independent set of size t in G, no vertex of $M(v)$ being adjacent to v. In every case $\omega(G) \geq s$ or $\alpha(G) \geq t$, so $R(s,t) \leq n$. Finiteness now follows by induction on $s+t$: the numbers $R(2,t)$ and $R(s,2)$ are finite, and (21) bounds $R(s,t)$ for $s,t \geq 3$ by two numbers whose indices sum to $s+t-1$, which completes the proof. □

Proposition 18. *Let $s,t \geq 3$ and suppose $R(s-1,t) = 2a$ and $R(s,t-1) = 2b$ are both even. It holds that $R(s,t) \leq 2a + 2b - 1$.*

Proof. Let G be a graph on $n = 2a + 2b - 1$ vertices. If some vertex v has $|N(v)| \geq 2a$ or $|M(v)| \geq 2b$, the two cases in the proof of Proposition 17 apply verbatim and finish the argument. Otherwise every vertex satisfies $|N(v)| \leq 2a - 1$ and $|M(v)| \leq 2b - 1$, and since these two quantities sum to $n - 1 = 2a + 2b - 2$ at every vertex, both bounds hold with equality everywhere; in particular G is regular of degree $2a - 1$. The degree sum $(2a + 2b - 1)(2a - 1)$ is then a product of two odd integers, hence odd, while the degree sum of any graph is twice its number of edges. This contradiction shows that the first alternative occurs, which completes the proof. □

The four classical values

Proposition 19. *It holds that $R(3,3) = 6$, $R(3,4) = 9$, $R(3,5) = 14$ and $R(4,4) = 18$.*

Proof. The proposition is proved value by value; all four lower-bound witnesses are displayed, two of them in Section 3.

For $R(3,3)$: the pentagon P_5 gives $R(3,3) \geq 6$, as shown at the head of Section 3, and Proposition 17 gives $R(3,3) \leq R(2,3) + R(3,2) = 6$.

For $R(3,4)$: Proposition 17 gives $R(3,4) \leq R(2,4) + R(3,3) = 4 + 6 = 10$, and both summands are even, so Proposition 18 sharpens this to $R(3,4) \leq 9$. For the lower bound, let W be the graph on $\mathbb{Z}_8$ in which x and y are adjacent exactly when $x - y \in \{1,4,7\} \pmod 8$. A triangle in W would give directed gaps $d_1, d_2, d_3 \in \{1,4,7\}$ with $d_1 + d_2 + d_3 \equiv 0 \pmod 8$, and the ten possible multisets have sums

$$3,\ 6,\ 1,\ 1,\ 4,\ 7,\ 4,\ 7,\ 2,\ 5 \pmod 8, \tag{22}$$

listed in the order $\{1,1,1\}, \{1,1,4\}, \{1,1,7\}, \{1,4,4\}, \{1,4,7\}, \{1,7,7\}, \{4,4,4\}, \{4,4,7\}, \{4,7,7\}, \{7,7,7\}$; none is 0, so W is triangle-free. An independent set of size 4 would have circular gaps $g_1, g_2, g_3, g_4 \geq 1$ summing to 8, and each gap, being the circular distance of two consecutive chosen vertices, avoids the adjacency distances 1 and 4. A gap of 5 or more would leave the other three gaps a total of at most 3, though each of them is at least 2; hence every gap lies in $\{2,3\}$. The only way to write 8 as an ordered sum of four parts from $\{2,3\}$ is $2+2+2+2$, and then two opposite chosen vertices lie at circular distance 4 and are adjacent. Hence $\alpha(W) \leq 3$, the set $\{0,2,5\}$ showing equality, and W is a $(3,4)$-Ramsey graph on 8 vertices, so that $R(3,4) \geq 9$.

For $R(3,5)$: Proposition 17 gives $R(3,5) \leq R(2,5) + R(3,4) = 5 + 9 = 14$. For the lower bound, the nonzero cubes modulo 13 are

$$C = \{1,5,8,12\}, \tag{23}$$

as one reads off from $1^3 = 1$, $2^3 = 8$, $4^3 = 12$ and $7^3 = 5$ together with the fact that cubing is three-to-one on $\mathbb{F}_{13}^*$, the multiplicative group being cyclic of order 12 and $\gcd(3,12) = 3$; the set satisfies $C = -C$, so the graph Y on $\mathbb{Z}_{13}$ joining x and y exactly when $x - y \in C$ is well defined. A triangle in Y would give $d_1, d_2, d_3 \in C$ with $d_1 + d_2 + d_3 \equiv 0 \pmod{13}$, and hence a pair sum $d_1 + d_2 \equiv -d_3 \in -C = C$; but the ten pair sums of C are

$$2,\ 6,\ 9,\ 0,\ 10,\ 0,\ 4,\ 3,\ 7,\ 11 \pmod{13}, \tag{24}$$

listed in the order 1+1, 1+5, 1+8, 1+12, 5+5, 5+8, 5+12, 8+8, 8+12, 12+12, and none lies in C, so Y is triangle-free. Now suppose I is an independent set of size 5, with circular gaps $g_1, \ldots, g_5 \geq 1$ summing to 13. Every pairwise difference of I avoids $C = \{\pm 1, \pm 5\}$, so every circular distance between chosen vertices lies in $\{2,3,4,6\}$; in particular each gap g_i, being itself the difference of two chosen vertices, avoids the values 1 and 5. A gap of 6 or more would leave the remaining four gaps a total of at most 7, though each of them is at least 2; hence all gaps lie in $\{2,3,4\}$, and the only multisets of five such parts summing to 13 are $\{2,2,2,3,4\}$ and $\{2,2,3,3,3\}$. The sum of two adjacent gaps is the circular distance of two chosen vertices one apart, and must therefore avoid 5 and 8, these being the two-digit sums whose circular distance lies in $\{1,5\}$; sums of three or four consecutive gaps repeat the same constraints, because a sum of consecutive gaps and the sum of the complementary gaps are the two directed distances of one and the same pair. In the multiset $\{2,2,2,3,4\}$ the forbidden adjacent sum $2+3=5$ forces both cyclic neighbours of the 3 to be the single 4, which is impossible. In the multiset $\{2,2,3,3,3\}$ the same constraint forces both cyclic neighbours of each 2 to be 2s, so the two 2s would form a 2-regular proper subgraph of a 5-cycle, which does not exist. Hence $\alpha(Y) \leq 4$, the set $\{0,2,4,6\}$ showing equality, and Y is a $(3,5)$-Ramsey graph on 13 vertices, so that $R(3,5) \geq 14$.

For $R(4,4)$: Theorem 5 gives $R(4,4) \geq 18$, and Proposition 17 gives $R(4,4) \leq R(3,4) + R(4,3) = 9 + 9 = 18$, which completes the proof. □

The upper bound for $R(5,5)$

Theorem 20. *It holds that $R(5,5) \le 50$.*

Proof. Proposition 17 gives $R(5,5) \le R(4,5) + R(5,4) = 2\,R(4,5)$, the symmetry $R(5,4) = R(4,5)$ having been noted in the proof of Proposition 17. The value $R(4,5) = 25$ is a theorem of McKay and Radziszowski, proved by a computer search in 1995 [MR95] and verified end to end, including all satisfiability refutations, in the HOL4 proof assistant by Gauthier and Brown [GB24]; it is the one computational input to this bound, and we cite it with that provenance. Hence $R(5,5) \le 50$, which completes the proof. □

Remark 21. A reader who declines every computational input still obtains a finite bound from this paper alone: Proposition 17 gives $R(4,5) \le R(3,5) + R(4,4) = 14 + 18 = 32$, both summands are even, so Proposition 18 gives $R(4,5) \le 31$, and then $R(5,5) \le 2 \cdot 31 = 62$. Together with Theorem 7 this yields $38 \le R(5,5) \le 62$ with every step on the pages of this paper.

The two standard sharpenings of (21) do not improve Theorem 20. The parity refinement of Proposition 18 requires both summands even, and both equal 25; Section 6 examines what remains of this route. Walker's inequality $R(k,k) \le 4\,R(k,k-2) + 2$ [Wal68], cited here from the survey [Rad26], gives $R(5,5) \le 4\,R(5,3) + 2 = 4 \cdot 14 + 2 = 58$ by Proposition 19, which is weaker than 50.

6 Counting identities at forty-nine vertices

The first improvement of the recursion bound in the literature was $R(5,5) \le 49$, obtained by McKay and Radziszowski from subgraph-counting identities combined with computed census data about $(4,5)$-Ramsey graphs [MR97]. This section proves the identity at the heart of that route, determines exactly how far it reaches on the page, and shows that its simplest form provably cannot reach $R(5,5) \le 49$. Everything up to the final proposition is free of computational input.

Proposition 22. *Every $(5,5)$-Ramsey graph on 49 vertices is regular of degree 24, and its degree sum, $49 \cdot 24 = 1176$, is even.*

Proof. Let F be a $(5,5)$-Ramsey graph on 49 vertices and let v be a vertex. The graph $F[N(v)]$ contains no K_4, since a K_4 there together with v, which is adjacent to every vertex of $N(v)$, is a K_5 of F; and it contains no independent set of size 5, being an induced subgraph of F (Proposition 16). Hence it is a $(4,5)$-Ramsey graph and $|N(v)| \le R(4,5) - 1 = 24$. The graph $F[M(v)]$ contains no independent set of size 4, since such a set together with v, which is adjacent to no vertex of $M(v)$, is an independent set of size 5 in F; and it contains no K_5, again by Proposition 16. Hence it is a $(5,4)$-Ramsey graph and $|M(v)| \le R(5,4) - 1 = 24$. Since $|N(v)| + |M(v)| = 48$, both hold with equality, which completes the proof. □

The evenness in Proposition 22 is the precise reason the parity route of Proposition 18 stops: the regular configuration that a parity argument would need to exclude is arithmetically consistent at 49 vertices.

Proposition 23. *Let F be any graph on n vertices, and for a vertex v write $F_v^+ = F[N(v)]$ and $F_v^- = F[M(v)]$, with $e(\cdot)$ the number of edges and $d(v) = |N(v)|$. It holds that*

$$\sum_v \Big(e(F_v^-) - e(F_v^+) \Big) = \frac{1}{2} \sum_v d(v) \, \big(n - 2d(v) \big). \tag{25}$$

Proof. Classify the unordered triples of vertices by the number of edges they induce, and let t_i denote the number of triples inducing exactly i edges, for $i = 0, 1, 2, 3$. Counting pairs of adjacent neighbours, a triple contributes to $\sum_v e(F_v^+)$ exactly when it is a triangle, once for each of its three vertices, so

$$\sum_v e(F_v^+) = 3\, t_3. \tag{26}$$

Counting edges among non-neighbours, a triple contributes exactly when it induces one edge, once, at its third vertex, so

$$\sum_v e(F_v^-) = t_1. \tag{27}$$

Counting ordered pairs of a neighbour and a non-neighbour, a triple with two edges contributes once at each of its two leaves, and a triple with one edge once at each endpoint of its edge, so

$$\sum_v d(v) \, \big(n - 1 - d(v) \big) = 2\, t_2 + 2\, t_1, \tag{28}$$

and counting unordered pairs of neighbours, a triangle contributes three times and a two-edge triple once at its centre, so

$$\sum_v \binom{d(v)}{2} = t_2 + 3\, t_3. \tag{29}$$

Writing $n - 2d(v) = \big(n - 1 - d(v) \big) - \big(d(v) - 1 \big)$ and combining (28) and (29),

$$\frac{1}{2} \sum_v d(v) \, \big(n - 2d(v) \big) = (t_2 + t_1) - (t_2 + 3\, t_3) = t_1 - 3\, t_3, \tag{30}$$

which equals $\sum_v e(F_v^-) - \sum_v e(F_v^+)$ by (26) and (27), and completes the proof. □

Let F now be a hypothetical $(5,5)$-Ramsey graph on 49 vertices. By Proposition 22 it is 24-regular, so (25) reads

$$\sum_v \Big(e(F_v^-) - e(F_v^+) \Big) = \frac{1}{2} \cdot 49 \cdot 24 \cdot (49 - 48) = 588, \tag{31}$$

an average of exactly 12 per vertex; moreover every F_v^+ is a $(4,5)$-Ramsey graph on 24 vertices, and every F_v^- is a $(5,4)$-Ramsey graph on 24 vertices, whose complement is a $(4,5)$-Ramsey graph on 24 vertices, so that $e(F_v^-) = \binom{24}{2} - e = 276 - e$ for the complement's edge count e. Bounds on the edge counts of $(4,5)$-Ramsey graphs on 24 vertices therefore bound the left side of (31), and the question is whether they can contradict it.

What can be said by hand is the following. In a $(4,5)$-Ramsey graph on 24 vertices, every vertex w has $|N(w)| \le R(3,5) - 1 = 13$, since its neighbourhood graph contains no triangle and no independent set of size 5, and $|M(w)| \le R(4,4) - 1 = 17$, since its non-neighbourhood graph contains no K_4 and no independent set of size 4; hence every degree lies in $[6, 13]$, and

$$72 \le e \le 156 \tag{32}$$

for the number of edges e of any such graph, both bounds resting on Proposition 19 alone. The window (32) bounds each summand of (31) between $(276-156)-156=-36$ and $(276-72)-72=132$, an interval that contains the required average 12 with room to spare, so no contradiction is available from (32).

The census of $(4,5)$-Ramsey graphs on 24 vertices is known by computation: the minimum edge count is 116 and the maximum is 132, with exactly two graphs attaining the maximum [MR95, AM24]. The final proposition records what the identity then yields, and what it cannot.

Proposition 24. *Assume the computed values $e(4,5,24)=116$ and $E(4,5,24)=132$ for the minimum and maximum edge counts of $(4,5)$-Ramsey graphs on 24 vertices [MR95, AM24]. Then in any $(5,5)$-Ramsey graph F on 49 vertices, every vertex v satisfies $e(F_v^+)=132$ and $e(F_v^-)=144$; that is, every neighbourhood induces an edge-maximal $(4,5)$-Ramsey graph on 24 vertices, and the complement of every non-neighbourhood does likewise. Moreover, no bound of the form $e(F_v^+)\geq m$ and $e(F_v^-)\leq 276-m$ can contradict (31) for any graph class: a contradiction would require $m\geq 133$, while $m\leq E(4,5,24)=132$ for every m realised by a $(4,5)$-Ramsey graph on 24 vertices.*

Proof. The first assertion follows by pinning each summand of (31) to the bottom of its range, and the second by computing what range a bound of the stated form permits. With the assumed census values, each vertex of F satisfies $116\leq e(F_v^+)\leq 132$ and, through the complement, $144\leq e(F_v^-)\leq 160$, so each summand of (31) lies in $[144-132,\ 160-116]=[12,44]$. The sum of 49 terms, each at least 12, equals $588=49\cdot 12$ exactly when every term equals 12, and a term equals 12 only if $e(F_v^-)=144$ and $e(F_v^+)=132$, since $e(F_v^-)\geq 144$ and $e(F_v^+)\leq 132$; this proves the first assertion. For the second, a bound of the stated form caps each summand at $(276-m)-m=276-2m$, and the total at $49\,(276-2m)$; this is smaller than 588 exactly when $276-2m<12$, that is, when $m\geq 133$. Since every $(4,5)$-Ramsey graph on 24 vertices has at most $E(4,5,24)=132$ edges, no realisable m satisfies this, which completes the proof. □

Remark 25. Proposition 24 explains, on the page, why the route to $R(5,5)\leq 49$ could not stop at extremal edge counts: the identity (25) is exactly feasible at 49 vertices, pinned to the boundary of the census window. The proof of [MR97] proceeded through finer counting identities driven by further census data, and its successors consumed the computational effort recorded in [AM24]; the experts' stated view is that further progress requires new theoretical insight [AM24]. The forcing statement in Proposition 24 is a concrete constraint any such insight may exploit: a hypothetical $(5,5)$-Ramsey graph on 49 vertices has all of its 49 neighbourhood graphs drawn from a census class of exactly two graphs.

7 Conclusion and Future Work

In this paper we have used symmetry reductions for Paley graphs, a self-contained proof of the Shearer–Mathon doubling bound, and classical counting arguments to establish bounds on $R(5,5)$ whose proofs are checkable by hand from the printed page, and to map exactly where the hand-checkable regime ends.

Several interesting questions regarding hand-checkable certificates for Ramsey bounds remain unsolved. Among them are the following three questions.

- Is there an algebraically structured witness, checkable in a few pages, certifying $R(5,5)\geq n$ for some n strictly between 38 and 43? By Remark 9 such a witness carries neither the Paley

structure nor any cyclic structure of small order, so a different symmetry would have to be found.

- In Section 6 we proved that the excess identity with extremal edge counts cannot yield $R(5,5) \leq 49$, and that it forces every neighbourhood of a hypothetical $(5,5)$-Ramsey graph on 49 vertices into a census class of two graphs. Is there a census-free counting argument, checkable by hand, that yields $R(5,5) \leq 49$, or even $R(5,5) < 62$ without the value $R(4,5) = 25$? The gap between the hand window (32) and the computed census is a measure of how far pure counting currently falls short.
- Gauthier and Brown ask whether $R(4,5) = 25$ is intrinsically computational [GB24]. The same question stands one level down: does $\omega(P_p)$ admit hand-checkable determination for the next Paley witnesses in the survey's tables, such as P_{101} with its clique number 5 underlying $R(6,6) \geq 102$ [Rad26]? The set S_{101} has 24 vertices, and the analysis of Section 3 would need one further level of reduction to remain short.

The techniques presented in this paper are not intrinsically limited to the diagonal case; applications of the reduction lemma and the doubling construction to off-diagonal numbers and to other algebraically defined witness families are topics for possible future work.

Availability

Artifacts are available from the authors on request.

Acknowledgements

This paper was made possible by the research tooling generated by Transformer Lab.

References

[AM24] Vigleik Angeltveit and Brendan D. McKay. R(5,5) <= 46. 2024. Journal of Graph Theory, to appear.

[BDR88] Izak Broere, Dipl Doman, and John N. Ridley. The clique numbers and chromatic numbers of certain Paley graphs. *Quaestiones Mathematicae*, 11(1):91–93, 1988.

[CFL+26] Stefano Coniglio, Fabio Furini, Ivana Ljubić, Pablo San Segundo, Johannes Thuerauf, and Emiliano Traversi. An Integer Programming Approach to Compute Lower Bounds for Ramsey Numbers Using Circulant Graphs. 2026.

[EPS81] Ronald J. Evans, John R. Pulham, and John Sheehan. On the number of complete subgraphs contained in certain graphs. *Journal of Combinatorial Theory, Series B*, 30(3):364–371, 1981.

[ES35] Paul Erdős and George Szekeres. A combinatorial problem in geometry. *Compositio Mathematica*, 2:463–470, 1935.

[Exo89] Geoffrey Exoo. A Lower Bound for R(5,5). *Journal of Graph Theory*, 13(1):97–98, 1989.

[GAYKS24] Mohammad Ghebleh, Salem Al-Yakoob, Ali Kanso, and Dragan Stevanović. Reinforcement learning for graph theory, I. Reimplementation of Wagner's approach. 2024.

[GB24] Thibault Gauthier and Chad E. Brown. A Formal Proof of R(4,5)=25. 2024. In: Proceedings of the 15th International Conference on Interactive Theorem Proving (ITP 2024).

[GG55] Robert E. Greenwood and Andrew M. Gleason. Combinatorial Relations and Chromatic Graphs. *Canadian Journal of Mathematics*, 7:1–7, 1955.

[GJQ+22] Lachlan Ge, Yasiru Jayasooriya, Alex Qiu, Michael Sun, and Victor Yuan. Study of Exoo's Lower Bound for Ramsey number R(5,5). 2022.

[HK03] Heiko Harborth and Stefan Krause. Ramsey Numbers for Circulant Colorings. *Congressus Numerantium*, 161:139–150, 2003.

[Kal66] John G. Kalbfleisch. *Chromatic Graphs and Ramsey's Theorem*. PhD thesis, University of Waterloo, 1966.

[Mat87] Rudolf Mathon. Lower Bounds for Ramsey Numbers and Association Schemes. *Journal of Combinatorial Theory, Series B*, 42(1):122–127, 1987.

[MR95] Brendan D. McKay and Stanisław P. Radziszowski. R(4,5) = 25. *Journal of Graph Theory*, 19(3):309–322, 1995.

[MR97] Brendan D. McKay and Stanisław P. Radziszowski. Subgraph Counting Identities and Ramsey Numbers. *Journal of Combinatorial Theory, Series B*, 69(2):193–209, 1997.

[Rad26] Stanisław P. Radziszowski. Small Ramsey Numbers. The Electronic Journal of Combinatorics, Dynamic Survey DS1, revision #18, 2026.

[Ram30] Frank P. Ramsey. On a Problem of Formal Logic. *Proceedings of the London Mathematical Society*, s2-30(1):264–286, 1930.

[She86] James B. Shearer. Lower Bounds for Small Diagonal Ramsey Numbers. *Journal of Combinatorial Theory, Series A*, 42(2):302–304, 1986.

[Wag21] Adam Zsolt Wagner. Constructions in combinatorics via neural networks. 2021.

[Wal68] Kenneth Walker. Dichromatic Graphs and Ramsey Numbers. *Journal of Combinatorial Theory*, 5(3):238–243, 1968.

[XXER04] Xiaodong Xu, Zheng Xie, Geoffrey Exoo, and Stanisław P. Radziszowski. Constructive Lower Bounds on Classical Multicolor Ramsey Numbers. *The Electronic Journal of Combinatorics*, 11(1):#R35, 2004.