

CHAPTERS 8 AND 10

EUCLIDEAN COLORINGS AND CONSTRUCTIVE RAMSEY BOUNDS

WILLIAM GASARCH AND NEAL SHANDILYA

ABSTRACT. These chapters give a self-contained account of the set-intersection method behind classical lower bounds for the chromatic number of Euclidean space and explicit lower bounds for diagonal Ramsey numbers. We prove the forms of Oddtown, Fisher's inequality, and the Frankl–Wilson polynomial method needed for the applications, and use them to derive the standard sequence of Euclidean and Ramsey constructions. For Euclidean space, the binary-layer construction gives lower bounds of every fixed polynomial degree and, after optimizing the layer and modulus, the exponential base $(1 + \sqrt{2})/2$. For diagonal Ramsey numbers, the same method gives explicit polynomial lower bounds and the classical scale

$$\exp\left(\left(\frac{1}{4} + o(1)\right) \frac{(\log k)^2}{\log \log k}\right).$$

We also analyze the parameter choices in these constructions. For the Euclidean certificates we obtain a stability estimate around the optimal layer and modulus densities. For the Ramsey certificates we allow unequal degree bounds and arbitrary ground-set sizes, prove a uniform optimization bound, and show that near-optimal parameters satisfy $c/p \rightarrow 1$ and $m = p^{3+o(1)}$. An appendix extends the uniform intersection bound to prime powers, compares primes and prime powers at finite ground-set size, and relates the possible gain to prime gaps. Writing $\beta = (1 + \sqrt{2})/2$, the binary construction yields $\chi(\mathbb{E}^n) \geq \beta^n \exp(-Cn^{0.05})$ for some absolute $C > 0$. Under the Cramér gap hypothesis its optimized uniform certificate is $(\sqrt{2}\beta^{5/2} + o(1))\beta^n$, giving the same chromatic lower bound. The Ramsey leading coefficient also persists for every uniformity with the diagonal-residue coloring rule. The optimization statements concern these specified certificate families, not the optimal chromatic or Ramsey behavior of the underlying graphs.

Contents

BILL TO NEAL: The first version of this document was 19 pages. This version is over 40 pages. What happened?

BILL TO NEAL: I renamed the file `chien.tex`. We really should not call it `ramseylines.tex` since that might be the file for the entire document.

BILL TO NEAL: Normally book chapters don't have abstracts. If we submit this to a journal that takes expository work, we will consider the journal and possibly modify that abstract. No change for now.

INTRODUCTION

Unit-distance coloring in Euclidean space and explicit Ramsey constructions both lead to extremal questions for uniform set systems. In the Euclidean setting, a color class inside a finite configuration must avoid the intersection pattern corresponding to unit distance. In the Ramsey setting, a homogeneous vertex set must satisfy the intersection restrictions imposed by one edge color. After the vertices are represented by uniform subsets of a finite ground set, the relevant bounds are therefore bounds on families with restricted pairwise intersections.

The algebraic method separates diagonal and off-diagonal intersection values. A polynomial is chosen to vanish at the permitted off-diagonal values while remaining nonzero at the size of a member of the family. Evaluation on incidence vectors then produces linearly independent functions in a polynomial space of controlled dimension. The dimension of that space bounds the family. The elementary forms of this argument are proved when they are first used. The sharper uniform versions are collected in Appendix ??.

Chapter ?? applies this method to Euclidean coloring. Fixed polynomial degree gives lower bounds of arbitrarily large fixed power, while a growing modulus leads to an exponential lower bound and an entropy optimization. Chapter ?? applies the same intersection bounds to both colors of a complete graph. There the construction must control two kinds of homogeneous family and is compared with the much larger lower bound supplied by the probabilistic method.

Two Progressions. The bounds in Chapter ?? occur at the following asymptotic scales:

$$n + 1 \longrightarrow n + 2 \longrightarrow \frac{n(n-1)}{6} \longrightarrow c_d n^d \longrightarrow (\beta + o(1))^n \longrightarrow (1.239 \dots + o(1))^n,$$

$$\beta = \frac{1 + \sqrt{2}}{2}.$$

BILL TO NEAL. This introduction is hard to read for someone not in the area. Even for someone who is in the area. Here is a simpler version. I will assume that $\chi(E^n)$ was defined earlier though the reader may not recall it.

Simpler Version

Recall the following definition.

Definition 0.1. Let $n \geq 2$. Let G_n be the graph with vertices $\mathbf{E}^n$ and edges

$$\{(x, y) : d(x, y) = 1\}.$$

Then $\chi(\mathbf{E}^n)$ is the chromatic number of G_n .

Note 0.2. Recall that $5 \leq \chi(\mathbf{E}^2) \leq 7$

In this chapter we obtain asymptotic lower bounds on $\chi(\mathbf{E}^2)$. The techniques we employ can also be used to obtain constructive asymptotic lower bounds on the Ramsey numbers. We will present this in a later chapter.

In this chapter we present the following sequence of results.

- (1) $\chi(\mathbf{E}^n) \geq n + 1$. This is elementary and uses a simplex. It is similar to the proof that $\chi(\mathbf{E}^2) \geq 2$ which we did in Theorem FILL IN.
- (2) $\chi(\mathbf{E}^n) \geq n + 2$. This is elementary and uses a spindle. It is similar to the proof that $\chi(\mathbf{E}^2) \geq 3$ which we did in Theorem FILL IN.
- (3) $\chi(\mathbf{E}^n) \geq \frac{n(n-1)}{6}$. This uses a Oddtown. Oddtown is a theorem involving set intersection and mod 2. It is proved with easy linear algebra.
- (4) $\chi(\mathbf{E}^n) \geq c_d n^d$. This uses a generalization of Oddtown that replaces mod 2 with mod p where p is a prime. It is proved with polynomials and linear algebra.
- (5) $\chi(\mathbf{E}^n) \geq (\beta + o(1))^n$ where $\beta = \frac{1+\sqrt{2}}{2} \sim 1.207$. This uses the same lemma as the prior point but picks the parameters more carefully.
- (6) $\chi(\mathbf{E}^n) \geq (1.238 + o(1))^n$. This was proved by Raigorodskii [?]. He used vectors in $\{-1, 0, 1\}^n$.

The display records a progression of methods, not a pointwise ordering for every dimension. The first two bounds come from a simplex and a spindle. The quadratic bound uses Oddtown on a layer of triples. A fixed prime p replaces the parity condition by a congruence condition and gives polynomial degree $p - 1$, hence lower bounds of every fixed power. Allowing p to grow proportionally with the dimension turns both the vertex count and the color-class bound exponential. Optimizing their quotient gives the base β . Raigorodskii's later improvement to $1.239 \dots$ uses vectors in $\{-1, 0, 1\}^m$ and is quoted in Section ??.

For Chapter ??, the analogous sequence of construction sizes is

$$k^3 \longrightarrow k^{p+1} \longrightarrow \exp\left(\frac{(\log k)^2}{4 \log \log k}\right) \longrightarrow \exp(ck^{1/C}) \longrightarrow k2^{k/2}.$$

The first three terms are obtained from the elementary intersection constructions developed here. The fourth represents later extractor-based explicit constructions, and the fifth is the probabilistic existence scale. Constants and lower-order terms are suppressed in this overview. Section ?? also records an algebraic construction that improves the coefficient $1/4$ without reaching the extractor scale.

Parameter Optimization. The simplex and spindle arguments, the Ramsey recurrence and first-moment bound, and the Frankl–Wilson constructions are classical. Our additional analysis concerns the numerical guarantees obtained from specified intersection certificates when their parameters are allowed to vary.

For the Ramsey certificates, Theorem ?? allows arbitrary ground-set size and unequal degree bounds. Its upper estimate uses only that the modulus is an integer at least two, so the leading coefficient cannot be improved by replacing primes with prime powers. The coefficient $1/4$ and the balanced cubic construction are classical: Frankl and Wilson [?], Section 6, already allow arbitrary ground sets and prime powers, and Pikhurko [?], Section 9.3, optimizes the prime against the certificate budget. The refinement established here is the uniform upper estimate for unequal degrees together with a stability statement for parameters near equality. Gopalan [?] proves broader degree-product barriers for symmetric-polynomial representations. The relation is discussed in Section ??.

The Euclidean analysis similarly optimizes the layer and modulus densities within the binary construction. Theorem ?? and Corollary ?? give the optimum and a finite stability estimate. The Ramsey stability estimate in Theorem ?? is primarily asymptotic, with overhead of order $\log \log \log k / \log \log k$. Proposition ?? relates the finite advantage of prime powers to the distance D_m from a_*m to the nearest prime, with logarithmic gain $O((1 + D_m^2)/m)$. Corollary ?? makes the resulting error in the classical binary bound explicit:

$$\chi(\mathbf{E}^n) \geq \beta^n \exp(-Cn^{0.05}).$$

Under the Cramér gap hypothesis $p_{j+1} - p_j = O(\log^2 p_j)$, the optimized uniform certificate is $(\sqrt{2}\beta^{5/2} + o(1))\beta^n$, and hence $\chi(\mathbf{E}^n) \geq (\sqrt{2}\beta^{5/2} + o(1))\beta^n$. These statements quantify this construction. The larger known Euclidean exponential base already implies these chromatic inequalities. The results established here combine uniform certificate optimization, quantitative stability, robustness under every diagonal residue (Proposition ??), and this finite prime-gap analysis.

Scope. These optimizations apply to the stated intersection bounds. They do not rule out stronger estimates for the independent or homogeneous families of the same graphs. Example ?? gives a small instance in which the certificate is not exact. The chapter numbers are retained from the larger *Ramsey Lines* project.

Notation and Intersection Bounds. Write $[m] = \{1, \dots, m\}$ and $\binom{[m]}{r}$ for its r -element subsets. The incidence vector of $A \subseteq [m]$ is $\mathbf{1}_A \in \{0, 1\}^m$. A family is r -uniform if all of its members have size r . We use m for ground-set size, n for Euclidean dimension, r for uniformity, p for a prime, and q for a modulus. Each statement specifies whether q ranges over primes, prime powers, or all integers at least two. In Chapter 10, k denotes a forbidden homogeneous-set size and N the number of vertices. All logarithms are natural unless a base is indicated. Constants implicit in fixed- p asymptotics may depend on p . Here and below, e_i denotes the i th standard basis vector.

We use three tools, each proved in the text at its first application. Oddtown (Theorem ??) is the degree-one case over the field with two elements. The uniform Fisher inequality (Theorem ??) is the degree-one case over the reals. The polynomial intersection bound (Lemma ??) is the general case: over a field F , if s off-diagonal intersection values are permitted and the size of each set is not one of them, the family has at most $\sum_{j \leq s} \binom{m}{j}$ members. Chapter 8 uses that lemma over $\mathbb{F}_p$. Chapter 10 uses it over $\mathbb{F}_p$ in one color and over $\mathbb{Q}$ in the other. Table ?? records the three applications.

Appendix ?? contains the refinements that need the rank of a matrix. For a uniform family they replace $\sum_{j \leq s} \binom{m}{j}$ by $\binom{m}{s}$ and they extend the method to prime powers. The elementary constructions and their optimized leading constants are proved in the text. The appendix justifies the sharper uniform certificates and the extension from primes to prime powers.

Family	Uniformity	Off-diagonal restriction	Field, degree
Euclidean color class	$2p - 1$	Avoid $p - 1$. Equivalently avoid the diagonal residue modulo p	$\mathbb{F}_p$, $p - 1$
Red Ramsey family	$p^2 - 1$	Residues $0, \dots, p - 2$ modulo p	$\mathbb{F}_p$, $p - 1$
Blue Ramsey family	$p^2 - 1$	Integer values $p - 1, 2p - 1, \dots, (p - 1)p - 1$	$\mathbb{Q}$, $p - 1$

TABLE 1. The common intersection mechanism. In every row Lemma ?? bounds the family by $\sum_{j=0}^{p-1} \binom{m}{j}$, which Appendix ?? sharpens to $\binom{m}{p-1}$. Only the field and the list of permitted values change.

Organization. Sections 8.1 and 8.2 give the elementary upper bound and the two finite configurations that need no algebra. Section ?? sets up the intersection method on a single concrete example and proves Oddtown. Sections 8.4 and 8.5 run it at degree one and at degree $p - 1$, with the cases $p = 2$ and $p = 3$ written out in full before the general statement. Section 8.6 lets the prime grow and performs the entropy optimization. Section ?? proves the certificate optimum, and Section ?? places the result in the literature. Chapter 10 repeats the three steps for Ramsey colorings, in Sections 10.3, 10.4 and 10.5, after two sections of classical background, and proves the global certificate optimum and its stability statement in Section ??, and closes with subsequent constructions and a comparison of scales. Appendix ?? contains the uniform refinements and the prime-power theorems, Appendix ?? the off-diagonal literature, Appendix ?? historical notes and further reading, and Appendix ?? the questions these chapters raise.

8. ASYMPTOTICS FOR THE CHROMATIC NUMBER OF EUCLIDEAN SPACE

Let $\chi(\mathbb{E}^n)$ be the least number of colors in a coloring of all of $\mathbb{E}^n$ in which points at distance one receive different colors. No measurability assumption is imposed. For $n = 2$ this is the Hadwiger-Nelson problem, and de Grey's 2018 construction raised the planar lower bound from four to five [?].

We focus on the behavior of $\chi(\mathbb{E}^n)$ as the dimension grows. An upper bound requires a coloring of all of space. A lower bound can come from any finite unit-distance graph embedded in $\mathbb{E}^n$. The bounds below progress from linear to polynomial to exponential.

8.1. An Elementary Upper Bound. The following elementary bound gives a useful reference point, although it is weak. A small cube contains no unit-distance pair. Its color can therefore be reused on cubes separated far enough from it.

Theorem 8.1. *For every integer $n \geq 1$,*

$$\chi(\mathbb{E}^n) \leq (\lceil \sqrt{n} \rceil + 1)^n.$$

Proof. Put $a = 1/\sqrt{n}$ and partition $\mathbb{R}^n$ into the half-open cubes

$$Q_z = a(z + [0, 1)^n), \quad z \in \mathbb{Z}^n.$$

Set $h = \lceil \sqrt{n} \rceil + 1$ and color Q_z by the vector of residues of the coordinates of z modulo h . This uses h^n colors.

Two points of the same cube differ by less than a in every coordinate, so their distance is less than $\sqrt{n}a = 1$. If two different cubes have the same color, then their indices differ by at least h in some coordinate. The corresponding coordinates of any two points, one from each cube, therefore differ by strictly more than $(h - 1)a \geq 1$. Thus no monochromatic pair is at distance one. $\square$

Note 8.2. For $n = 2$ the proof uses squares, for $n = 3$ cubes, and so on. The $n = 2$ case of Theorem ?? yields $\chi(\mathbb{E}^2) \leq 9$. The standard hexagonal coloring gives $\chi(\mathbb{E}^2) \leq 7$. See the lattice constructions in Arman et al. [?], whose higher-dimensional lattice constructions give effective upper bounds for comparison with the cube argument. The hexagonal 7-coloring is the two-dimensional case of a *lattice-sublattice* coloring: color the Voronoi cells of a lattice by the cosets of a sublattice chosen so that no two cells of one coset contain a unit-distance pair. Squares are the Voronoi cells of $\mathbb{Z}^n$, which is a poor lattice for the purpose. Better lattices give $\chi(\mathbb{E}^3) \leq 15$ (Coulson [?], and independently Radoičić and Tóth [?]), $\chi(\mathbb{E}^4) \leq 49$, $\chi(\mathbb{E}^5) \leq 140$, and $\chi(\mathbb{E}^n) \leq 3^n$ for all $n \leq 38$ and for $n = 48, 49$ (Arman, Bondarenko, Prymak, and Radchenko [?]. The bound in dimension four had been announced earlier by Coulson and Payne). Theorem ?? gives 27, 81 and 1024 in dimensions three, four and five, so it is worse than every recorded value. Its logarithm is of order $n \log n$, not $O(n)$.

The hexagon itself generalizes more literally than one might expect. Arman, Bondarenko, Prymak, and Radchenko [?] prove $\chi(\mathbb{E}^{2h}) \leq 7^h$ whenever $\mathbb{E}^{2h}$ carries an Eisenstein lattice of covering-packing ratio at most $3/2$, which happens for $2h \in \{2, 4, 6, 8, 24\}$. The plane is the case $h = 1$, and the same theorem gives 49, 343, 2401 and 7^{12} in dimensions 4, 6, 8 and 24. The hexagonal coloring is thus one instance of a family, and suitable lattices can improve substantially on the cube bound.

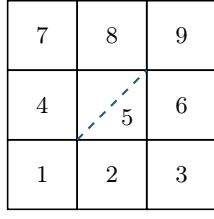
Coulson [?], Theorem 4.5, proved that a lattice-sublattice scheme in $\mathbb{E}^n$ must use at least $2^{n+1} - 1$ colors, so this family of colorings can never certify a base below two, and the 15-coloring of $\mathbb{E}^3$ is optimal within the family. Asymptotically the right descendant of the hexagon idea is a covering by slightly shrunk Voronoi cells, which is how Prosanov [?] improves the Larman-Rogers bound $(3 + o(1))^n$ quoted in Section ??.

8.2. The Simplex and the Spindle. The $n + 1$ points $e_i/\sqrt{2}$ in $\mathbb{R}^{n+1}$ are pairwise at distance one and lie in an affine hyperplane of dimension n . An isometry of that hyperplane with $\mathbb{E}^n$ proves $\chi(\mathbb{E}^n) \geq n + 1$.

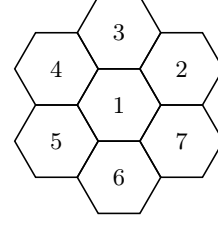
A spindle improves the simplex lower bound by one. The construction starts with a configuration that forces two nonadjacent vertices to share a color. Two copies are then positioned so that the forced color equality contradicts a unit-distance edge.

Theorem 8.3. *For every integer $n \geq 2$, $\chi(\mathbb{E}^n) \geq n + 2$.*

Proof. Take a regular $(n - 1)$ -simplex of side one with n vertices in a hyperplane of $\mathbb{E}^n$. Centering the vectors $e_i/\sqrt{2}$ shows that its circumradius squared is $(n - 1)/(2n)$. On



(a) Squares, 9 colors



(b) Hexagons, 7 colors

FIGURE 1. Two periodic colorings of the plane. In (a), the cube coloring of Theorem ?? at $n = 2$: squares of side $1/\sqrt{2}$, colored by the residues of their index vector modulo $\lceil\sqrt{2}\rceil + 1 = 3$. The dashed diagonal has length one. Half-open boundaries ensure that distances inside one square are strictly smaller than one, while two squares of the same color are three steps apart. In (b), the hexagonal 7-coloring: the hexagons are the Voronoi cells of the triangular lattice, and the seven colors are the cosets of a sublattice of index seven. Note ?? discusses what each picture does in higher dimensions.

the perpendicular line through its circumcenter there are two points u, v , one on each side, at distance one from every base vertex. Their separation is

$$D = 2\sqrt{1 - \frac{n-1}{2n}} = \sqrt{\frac{2(n+1)}{n}}, \quad 2D > 1. \quad (8.1)$$

In any proper coloring with $n+1$ colors the n base vertices use distinct colors, so both apices must use the remaining color.

Now take two congruent copies of the configuration with their first apices identified at u . Since $n \geq 2$, we may rotate the second copy about u inside a two-dimensional plane through u and v until its other apex v' satisfies $\|v - v'\| = 1$. This is possible because two points on the sphere of radius D about u can have any separation in $[0, 2D]$. Each copy forces its two apices to share a color, so v and v' share the color of u although they are at distance one, a contradiction. $\square$

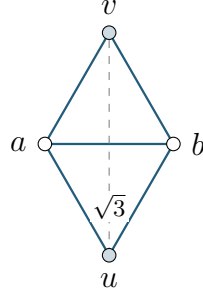
Any further unit distances between the two copies only impose more coloring constraints. The contradiction uses just the edges described in the proof. Figure ?? shows the case $n = 2$, the Moser spindle [?].

8.3. A Concrete Model for the Intersection Method. The same algebraic mechanism is used repeatedly in this chapter and in Chapter ?. We begin with the layer of three-element subsets, where the geometric encoding and the intersection restriction can be seen directly, before stating the general polynomial bound.

The triple layer. Fix m and send each three-element subset $A \subseteq [m]$ to the point $x_A = \mathbf{1}_A/2$ in $\mathbb{R}^m$. All of these points satisfy $\sum_i x_i = 3/2$, so they lie in an affine hyperplane of dimension $m-1$, which is a copy of $\mathbb{E}^{m-1}$. Two distinct triples have incidence vectors that differ in exactly the coordinates of $A \triangle B$, each by $1/2$, so

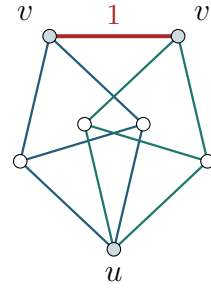
$$\|x_A - x_B\|^2 = \frac{|A \triangle B|}{4} = \frac{6 - 2|A \cap B|}{4} = \frac{3 - |A \cap B|}{2}.$$

(a) A forced equality



Since a, b use two colors, u, v share the third.

(b) The spindle



Both copies force u, v, v' to share a color.

FIGURE 2. The planar spindle construction. Every solid segment has length one. The dashed segment in (a) has length $\sqrt{3}$ and is not an edge. The two copies in (b) share u and are rotated so that $|v - v'| = 1$. The highlighted edge contradicts the color forced on its endpoints. Crossings without a dot are not vertices.

There are only three possibilities:

$$|A \cap B| = 0 \implies \|x_A - x_B\|^2 = \frac{3}{2},$$

$$|A \cap B| = 1 \implies \|x_A - x_B\|^2 = 1,$$

$$|A \cap B| = 2 \implies \|x_A - x_B\|^2 = \frac{1}{2}.$$

Unit distance is exactly intersection of size one.

Thus a color class in this finite unit-distance graph is a family of triples in which no two members intersect in exactly one element. Figure ?? illustrates the incidence-vector calculation. The remaining argument is stated entirely in terms of intersections.

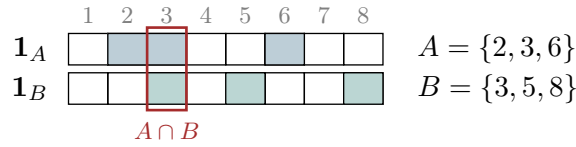


FIGURE 3. The encoding, for $m = 8$. The two rows are incidence vectors. The boxed column is the single shared element. The difference $\mathbf{1}_A/2 - \mathbf{1}_B/2$ is nonzero exactly on $A \triangle B = \{2, 5, 6, 8\}$, with entries $\pm 1/2$, so the squared distance is $4 \cdot (1/2)^2 = 1$. One shared element means unit distance. Zero or two shared elements do not.

General distance encoding. The same computation applies to every uniform layer.

Lemma 8.4 (Distance encoding). *Let $0 \leq r \leq m$, let $c > 0$, and put $x_A = \mathbf{1}_A/c$ for $A \in \binom{[m]}{r}$. Then these points lie in the hyperplane $\sum_i x_i = r/c$, and*

$$\|x_A - x_B\|^2 = \frac{2(r - |A \cap B|)}{c^2}. \quad (8.2)$$

In particular, if $r > 0$ and $c = \sqrt{2p}$, then unit distance corresponds to $|A \cap B| = r - p$.

Proof. Each vector has r nonzero coordinates. Their difference has a coordinate of magnitude $1/c$ at each element of $A \triangle B$ and is zero elsewhere. Since $|A \triangle B| = 2r - 2|A \cap B|$, the assertions follow. $\square$

The hyperplane in Lemma ?? can be identified isometrically with $\mathbb{E}^{m-1}$. We do not need the chosen points to span it. Consequently, if every color class has size at most M , the configuration requires at least $|V|/M$ colors. All Euclidean lower bounds below use this quotient.

Diagonal and off-diagonal intersections. The resulting extremal problem is combinatorial. Oddtown is the degree-one case over the field with two elements.

Theorem 8.5 (Oddtown). *Let $A_1, \dots, A_b \subseteq [m]$. If every $|A_i|$ is odd and every $|A_i \cap A_j|$ with $i \neq j$ is even, then $b \leq m$.*

Proof. Let u_i be the incidence vector of A_i over the field with two elements. Then $u_i \cdot u_j$ is 1 when $i = j$ and 0 otherwise. Suppose $\sum_i c_i u_i = 0$. Taking the inner product with u_j leaves $c_j = 0$. So the b vectors are linearly independent in an m -dimensional space. $\square$

This is the classical Oddtown argument. See Berlekamp [?] and Appendix ??.

Polynomial form of the argument. In Oddtown, the relevant polynomial is t over $\mathbb{F}_2$: it vanishes on the permitted off-diagonal residue and is nonzero on the diagonal. Frankl–Wilson replaces t by a polynomial with several roots. Permitting s off-diagonal values therefore leads to a polynomial of degree s and a dimension bound of order $\binom{m}{s}$. Table ?? summarizes the versions used below.

Statement	Family	Permitted off-diagonal	Bound	Device
Oddtown, Thm ??	odd sizes	even intersections	m	product over $\mathbb{F}_2$
Fisher, Thm ??	r -uniform	one value λ	m	squared norm over $\mathbb{R}$
Lemma ??	any	s values in a field	$\sum_{j \leq s} \binom{m}{j}$	multilinear polynomials
Thm ??	r -uniform	s residues mod p	$\binom{m}{s}$	rank over $\mathbb{Q}$
Thm ??	r -uniform	residues mod $q = p^h$	$\binom{m}{m}_{q-1}$	integer-valued polynomial

TABLE 2. The method at five strengths. The three rows above the rule are proved in the text and are all that Chapters ?? and ?? use. The two below it are the refinements of Appendix ??, which improve finite bounds but no exponential rate.

The first three rows are sufficient for the main constructions. Passing from degree one to degree s permits several off-diagonal intersection values and yields the polynomial bound of Lemma ?? . Uniformity sharpens the sum of binomial coefficients to a single coefficient by the rank argument of Appendix ?? . Prime powers provide additional finite parameter choices through an integer-valued polynomial. These last two refinements improve finite bounds without changing the leading asymptotic rates proved in the main chapters.

8.4. A Quadratic Lower Bound. Applying Oddtown to the triple layer of Section ?? gives the first polynomial lower bound.

Theorem 8.6. *For every integer $n \geq 2$,*

$$\chi(\mathbf{E}^n) \geq \left\lceil \frac{n(n-1)}{6} \right\rceil.$$

Proof. Set $m = n + 1$ and use the triples of $[m]$, embedded as $x_A = \mathbf{1}_A/2$ in an affine hyperplane of dimension $m - 1 = n$. By Section ??, unit distance is exactly intersection of size one, so distinct triples in one color class meet in zero or two elements. Every triple has odd size, so Theorem ?? bounds each color class by m . There are $\binom{m}{3}$ vertices, so at least $\lceil \binom{m}{3}/m \rceil = \lceil n(n-1)/6 \rceil$ colors are needed. $\square$

The proof already contains the two ingredients used later. A color class is bounded by $m = \binom{m}{1}$, the binomial coefficient associated with a degree-one polynomial, and the chromatic lower bound is obtained by dividing the number of vertices by the largest possible color class. For small dimensions this is weaker than the spindle bound, but it is the first bound here that grows faster than linearly. The next step replaces parity by residues modulo an arbitrary prime.

8.5. Every Fixed Polynomial is Eventually Exceeded. The parity argument is the degree-one case of a more general polynomial method. Allowing s off-diagonal values leads to a polynomial of degree s . The following elementary form of the Frankl–Wilson method [?] uses a polynomial that vanishes at every permitted off-diagonal intersection while remaining nonzero on the diagonal.

Lemma 8.7 (Polynomial intersection bound). *Let F be a field and let $L \subseteq F$ have s elements, where $0 \leq s \leq m$. Let $\mathcal{F}$ be a family of subsets of $[m]$ such that the image of $|A|$ in F lies outside L for every $A \in \mathcal{F}$, while the image of $|A \cap B|$ lies in L for all distinct $A, B \in \mathcal{F}$. Then*

$$|\mathcal{F}| \leq \sum_{j=0}^s \binom{m}{j}.$$

Proof. For $A \in \mathcal{F}$ define

$$P_A(x_1, \dots, x_m) = \prod_{\lambda \in L} \left(\sum_{i \in A} x_i - \lambda \right).$$

Replace each positive power x_i^a by x_i . Since $x_i^a = x_i$ on $\{0, 1\}$, the resulting multilinear polynomial Q_A has the same values on incidence vectors and degree at most s . Writing u_B for the incidence vector of B ,

$$Q_A(u_B) = \prod_{\lambda \in L} (|A \cap B| - \lambda),$$

which the hypotheses make zero for $A \neq B$ and nonzero for $A = B$. Hence if $\sum_A c_A Q_A = 0$ as a function on $\{0, 1\}^m$, evaluating at u_B leaves $c_B Q_B(u_B) = 0$, so $c_B = 0$: the Q_A are linearly independent. They lie in the span of the squarefree monomials $\prod_{i \in S} x_i$ with $|S| \leq s$, and there are $\sum_{j \leq s} \binom{m}{j}$ of those. Empty products are read as one, so the argument also covers $s = 0$. $\square$

The layer size is chosen to make the modular restriction unique.

Choice of the layer $2p - 1$

With scale $c = \sqrt{2p}$, Lemma ?? makes unit distance equivalent to intersection size $r - p$. The modular argument requires this to be the only off-diagonal intersection congruent to r modulo p . Since the other candidates are $r - 2p, r - 3p, \dots$, this holds for $p \leq r < 2p$. All layers in this interval have the same degree cost $p - 1$. When $2p - 1 \leq m/2$, the largest layer in the interval is therefore $r = 2p - 1$, with forbidden intersection $p - 1$. Section ?? later optimizes over the full admissible interval.

The cases $p = 2$ and $p = 3$ illustrate the construction before the general statement.

Example 8.8 ($p = 2$). The layer is $r = 2p - 1 = 3$ and the scale is $c = \sqrt{2p} = 2$, which is the triple construction of Section ?. Unit distance is $|A \cap B| = r - p = 1$. Modulo 2 the permitted off-diagonal residue is $L = \{0\}$, one value, so the polynomial has degree one and Lemma ?? bounds a color class by $\binom{m}{0} + \binom{m}{1} = m + 1$. The quotient is $\binom{m}{3}/(m + 1) \sim m^2/6$, the quadratic bound of Theorem ?? again. Oddtown does marginally better, because it also knows that the sets have odd size, and gives m .

Example 8.9 ($p = 3$). Now the layer is $r = 5$ and the scale is $c = \sqrt{6}$, so

$$\|x_A - x_B\|^2 = \frac{2(5 - |A \cap B|)}{6} = \frac{5 - |A \cap B|}{3},$$

and unit distance is $|A \cap B| = 2$. Distinct 5-sets meet in 0, 1, 2, 3 or 4 elements, and of these only 2 is congruent to $5 \equiv 2$ modulo 3. So in a color class every off-diagonal intersection is congruent to 0 or 1 modulo 3, while every member has size congruent to 2: two permitted residues, a polynomial of degree two, and a color class of size at most $\binom{m}{0} + \binom{m}{1} + \binom{m}{2} \sim m^2/2$. There are $\binom{m}{5} \sim m^5/120$ vertices, so

$$\chi(\mathbb{E}^{m-1}) \gtrsim \frac{m^5/120}{m^2/2} = \frac{m^3}{60}.$$

The exponent 3 is the difference $5 - 2$ between the degree of the vertex count and the degree of the class bound, and $1/60 = (p-1)!/(2p-1)! = 2/120$. The general statement below says exactly this for every prime.

Theorem 8.10 (Frankl-Wilson binary construction). *Let p be prime and let $m \geq 2p - 1$. Then*

$$\chi(\mathbb{E}^{m-1}) \geq \left\lceil \frac{\binom{m}{2p-1}}{\sum_{j=0}^{p-1} \binom{m}{j}} \right\rceil. \quad (8.3)$$

Proof. Use the $(2p - 1)$ -subsets of $[m]$ with $x_A = \mathbf{1}_A/\sqrt{2p}$. The points lie in an affine hyperplane of dimension $m - 1$, and Lemma ?? gives

$$\|x_A - x_B\|^2 = \frac{2p - 1 - |A \cap B|}{p}.$$

So a color class avoids intersection $p - 1$. For distinct vertices the intersection lies in $\{0, \dots, 2p - 2\}$, in which $p - 1$ is the only value congruent to $2p - 1$ modulo p . Hence in a

color class every off-diagonal intersection has residue in $L = \{0, 1, \dots, p-2\}$, while the size $2p-1$ has residue $p-1 \notin L$. Lemma ?? over $\mathbb{F}_p$, with $s = |L| = p-1$, bounds each color class by $\sum_{j=0}^{p-1} \binom{m}{j}$. Dividing the number of vertices by this bound proves (??). $\square$

Remark 8.11 (The role of uniformity). The family here is uniform, and Appendix ?? uses that to replace the denominator of (??) by the single binomial coefficient $\binom{m}{p-1}$ (Theorem ??). Since

$$\binom{m}{p-1} \leq \sum_{j=0}^{p-1} \binom{m}{j} \leq p \binom{m}{p-1} \quad \text{whenever } p-1 \leq m/2,$$

the two versions differ by at most a factor of p . Nothing below changes as a result, not even a leading constant. Only the finite numbers in Table ?? improve. The sharper version is the one that needs the rank of a matrix, which is why it is in the appendix.

Residues are essential here. On the layer $r = 2p-1$, excluding the single value $p-1$ leaves $r-1$ possible off-diagonal values. The exact-value Ray–Chaudhuri–Wilson bound would give $\binom{m}{r-1}$, and a quotient only $(m-r+1)/r$. Reduction modulo p compresses the allowed values to $p-1$ residues and gives the much smaller denominator used here.

Corollary 8.12. *For every fixed real $d > 0$ we have $\chi(\mathbf{E}^n)/n^d \rightarrow \infty$.*

Proof. For a fixed prime p , $\sum_{j=0}^{p-1} \binom{m}{j} = \binom{m}{p-1} (1 + O(1/m))$, since consecutive terms have ratio $O(1/m)$. Cancellation then gives

$$\frac{\binom{m}{2p-1}}{\sum_{j=0}^{p-1} \binom{m}{j}} = (1 + O(1/m)) \frac{(p-1)!}{(2p-1)!} \prod_{j=p-1}^{2p-2} (m-j) = \left(\frac{(p-1)!}{(2p-1)!} + o(1) \right) m^p. \quad (8.4)$$

Choose a fixed prime $p > d$ and apply Theorem ?? with $m = n+1$. $\square$

The exponent p in (??) is the difference between the vertex-count degree $2p-1$ and the color-class degree $p-1$. To reach exponential growth, p must grow with m , and the fixed- p expansion is then replaced by an entropy estimate.

8.6. An Exponential Lower Bound Using Primes. The Frankl–Wilson construction becomes exponential when the prime grows with the dimension. If p is proportional to m , both the vertex count and the color-class bound in (??) are exponential in m . Optimizing their quotient therefore reduces to a difference of two entropy terms.

Theorem 8.13. *Let $\beta = (1 + \sqrt{2})/2 = 1.207106781\dots$. Then*

$$\liminf_{n \rightarrow \infty} \chi(\mathbf{E}^n)^{1/n} \geq \beta.$$

Equivalently, for every $1 < b < \beta$ and all sufficiently large n , $\chi(\mathbf{E}^n) \geq b^n$. In particular, for large n , $\chi(\mathbf{E}^n) \geq 1.2^n$.

Proof. Let $H(t) = -t \log t - (1-t) \log(1-t)$ for $0 < t < 1$. For integers $r = r(m)$ with $r/m \rightarrow t$, Stirling's formula gives

$$\log \binom{m}{r} = mH(r/m) + O(\log m) = mH(t) + o(m). \quad (8.5)$$

Fix $0 < a < 1/2$ and let p be the largest prime at most am . By the prime number theorem, $p = am + o(m)$. The denominator in (??) satisfies $\binom{m}{p-1} \leq \sum_{j < p} \binom{m}{j} \leq m \binom{m}{p-1}$, so its logarithm is $\log \binom{m}{p-1} + O(\log m)$. With (??), Theorem ?? therefore gives

$$\log \chi(\mathbf{E}^{m-1}) \geq m(H(2a) - H(a)) + o(m). \quad (8.6)$$

Put $f(a) = H(2a) - H(a)$. Since $H'(t) = \log((1-t)/t)$,

$$f'(a) = 2H'(2a) - H'(a) = \log \frac{(1-2a)^2}{4a(1-a)}.$$

The argument of the logarithm decreases from $+\infty$ to 0 on $(0, 1/2)$, so f' vanishes exactly once there, and f' is positive before that point and negative after it: the solution is the unique maximizer. Writing $u = 1 - 2a$, the equation $(1 - 2a)^2 = 4a(1 - a)$ becomes $u^2 = 1 - u^2$, so $u = 1/\sqrt{2}$ and

$$a_* = \frac{1 - 1/\sqrt{2}}{2} = \frac{2 - \sqrt{2}}{4} = 0.1464466094 \dots \quad (8.7)$$

To evaluate the maximum, combine the two $\log a$ terms in f :

$$f(a) = -a \log(4a) - (1 - 2a) \log(1 - 2a) + (1 - a) \log(1 - a).$$

At the stationary point $4a = (1 - 2a)^2/(1 - a)$, so $-a \log(4a) = -2a \log(1 - 2a) + a \log(1 - a)$ and the display collapses to

$$f(a_*) = \log \frac{1 - a_*}{1 - 2a_*} = \log \left(\frac{(2 + \sqrt{2})/4}{1/\sqrt{2}} \right) = \log \frac{1 + \sqrt{2}}{2} = \log \beta.$$

Now take $a = a_*$ and $m = n + 1$ in (??). Replacing m by n changes the right-hand side by $O(1)$, so

$$\log \chi(\mathbf{E}^n) \geq (n + 1) \log \beta + o(n) = n \log \beta + o(n).$$

Logarithms are natural, so exponentiating gives $\chi(\mathbf{E}^n) \geq \exp(n \log \beta + o(n))$. Fix $1 < b < \beta$. Then

$$\frac{\chi(\mathbf{E}^n)}{b^n} \geq \exp \left(n \log \frac{\beta}{b} + o(n) \right) \rightarrow \infty,$$

because $\log(\beta/b) > 0$ dominates the $o(n)$ error. Hence $\chi(\mathbf{E}^n) \geq b^n$ for all sufficiently large n , and since $1.2 < \beta$ this applies to $b = 1.2$. $\square$

Remark 8.14 (Interpretation of the optimum). The number a_* is easier to read as a shape than as a root. Since $2a_* = 1 - 1/\sqrt{2} = 0.2929 \dots$, the optimal layer consists of the subsets whose size is about 29.3 percent of the ground set, and since the forbidden intersection $p - 1$ is about half of the uniformity $2p - 1$, the excluded pairs are those sharing about half of their elements. The largest layer of all, $r = m/2$, is *not* the best choice: it maximizes the number of vertices, but at $a = 1/4$ the rate is only $H(1/2) - H(1/4) = 0.1308 \dots$, a base of 1.139... rather than 1.207.... More vertices are not worth having if they also let each color class grow. At the optimum the two marginal effects cancel exactly: the stationarity condition $2H'(2a) = H'(a)$ says that the rate at which a larger layer gains vertices equals the rate at which the algebraic bound lets one class absorb them.

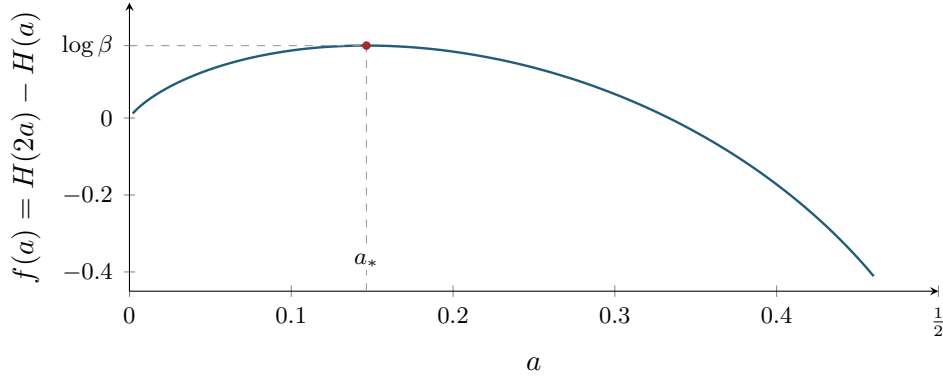


FIGURE 4. The exponential rate of the ratio (??) when $p/m \rightarrow a$. The vertex layer contributes $H(2a)$ and the bound on a color class costs $H(a)$, so the whole optimization is the difference. The maximum is at $a_* = (2 - \sqrt{2})/4 = 0.1464\dots$, where $f(a_*) = \log \beta = 0.1882\dots$ and $\beta = (1 + \sqrt{2})/2$. Choosing the prime as large as possible below a_*m costs only $o(m)$, by the prime number theorem. The same picture applies when p is replaced by another admissible modulus. Appendix ?? makes that precise.

Remark 8.15. If one prefers base two, the same statement reads $\chi(\mathbf{E}^n) \geq 2^{(n+o(n)) \log_2 \beta}$ with $\log_2 \beta = 0.2715\dots$. The base of the exponential must match the base of the logarithm. The prime number theorem is used only to approximate the density a_* , not for any error term.

Dimension n	Theorem ?? (no ranks)		Theorem ?? (uniform)	
	prime p	guaranteed colors	prime p	guaranteed colors
10	2	14	2	15
20	3	88	3	97
50	7	23,086	7	26,445
100	13	234,821,433	17	273,702,586
200	29	42,061,254,827,603,893	29	50,053,437,472,123,893

TABLE 3. Exact finite bounds from the binary construction. For each $m = n + 1$ the unrounded ratio is maximized over the primes with $2p - 1 \leq m$ and then rounded up. The left pair uses the denominator $\sum_{j < p} \binom{m}{j}$ proved in the text. The right pair uses the uniform denominator $\binom{m}{p-1}$ from Appendix ??, and uses the same family of vertex sets. The optimizing prime need not be the same in the two columns. All entries were computed with exact integer arithmetic. They are certified lower bounds from this construction, not values of $\chi(\mathbf{E}^n)$.

Table ?? optimizes the displayed subfamily $r = 2p - 1$. It does not by definition perform the full layer optimization introduced below. We compare the prime subfamily

$r = 2p - 1 \leq m$ with the full prime certificate family normalized to $r \leq m/2$. Complementing an admissible larger layer replaces r by $m - r$ and preserves its quotient, as explained in Definition ???. An exact check finds equal maximum values for these two families for $5 \leq m \leq 400$. This is finite evidence, not an endpoint theorem. The range $2t - 1 \leq m$ in Proposition ?? is the same top-layer range, with t allowed to vary over integers before restriction to primes or prime powers. At $m = 4$ the full maxima are $3/2$ and $6/5$ for the uniform and sum denominators, versus 1 and $4/5$ in the fixed-layer subfamily.

Summary of the construction. We began with triples, where parity gave a quadratic lower bound. Replacing parity by congruence modulo a fixed prime gave arbitrarily large polynomial degrees. Allowing the prime itself to grow with the dimension turned polynomial growth into exponential growth. The construction never changed: the vertices were always one uniform layer of subsets, the edges were always the unit-distance pairs, and the only parameter p was allowed to grow with the dimension. The next section considers what the parameter cannot do.

8.7. The Best Rate Certified by a Single Residue. The entropy calculation above varies p with the dimension but keeps the layer at $2p - 1$. We now allow the layer to vary as well. The object being optimized is the quotient supplied by the intersection theorem, not the chromatic number of the resulting graph.

Definition 8.16 (Binary intersection certificate). For integers m, r, q with $2 \leq q \leq r < 2q$ and $r \leq m/2$, put

$$B_D(m, r, q) = \frac{\binom{m}{r}}{\binom{m}{q-1}}, \quad B_S(m, r, q) = \frac{\binom{m}{r}}{\sum_{j=0}^{q-1} \binom{m}{j}}.$$

For $m \geq 4$, let $B_D(m)$ and $B_S(m)$ be the maxima over these parameters with q prime. The subscripts distinguish the uniform dimension bound from the sum bound proved in the main text.

For a prime q , either quotient is a lower-bound certificate for $\chi(\mathbf{E}^{m-1})$: use r -subsets scaled by $\sqrt{2q}$ and forbid intersection $r - q$. It is the only off-diagonal intersection congruent to r modulo q . For B_S this is Lemma ???. The sharper B_D uses Theorem ??.

A nonempty edge relation requires both $q \leq r$ and $m \geq r + q$. Otherwise the layer is edgeless. In the nonempty case, complementation preserves distances, replaces r by $m - r$, and preserves the certificate value since $\binom{m}{r} = \binom{m}{m-r}$ and the denominator is unchanged. The forbidden intersection becomes $m - r - q$, whose gap from the new uniformity is still q . We may therefore assume $r \leq m/2$. The possible off-diagonal intersections are then $0, \dots, r - 1$, and uniqueness of the diagonal residue requires $r < 2q$.

Theorem 8.17 (Optimal binary certificate rate). *With $\beta = (1 + \sqrt{2})/2$,*

$$\log B_S(m) = m \log \beta + o(m), \quad \log B_D(m) = m \log \beta + o(m).$$

Both statements remain true if the maxima also allow prime powers. The upper bound even holds when every integer $q \geq 2$ is allowed in the quotients. If admissible parameters

satisfy $\log B_D(m, r, q) = m \log \beta + o(m)$, then

$$\frac{q}{m} \longrightarrow a_*, \quad \frac{r}{m} \longrightarrow 2a_*, \quad a_* = (2 - \sqrt{2})/4.$$

Proof. Extend H continuously to $[0, 1]$. The uniform entropy estimate

$$mH(t/m) - \log(m+1) \leq \log \binom{m}{t} \leq mH(t/m) \quad (0 \leq t \leq m)$$

follows by taking the largest term in the binomial distribution with parameter t/m . In particular, changing t by one costs $O(\log m)$, including at the endpoints. Set $a = q/m$ and $\rho = r/m$. Since $a \leq \rho < 2a$ and $\rho \leq 1/2$, monotonicity of H on $[0, 1/2]$ gives, uniformly in the parameters,

$$\frac{1}{m} \log B_D(m, r, q) \leq H(\min\{2a, 1/2\}) - H(a) + O\left(\frac{\log m}{m}\right).$$

For $0 \leq a \leq 1/4$ the main term is $H(2a) - H(a)$, whose unique maximum is $\log \beta$ at a_* by Theorem ???. For $1/4 \leq a \leq 1/2$ it is $\log 2 - H(a) \leq \log 2 - H(1/4) < \log \beta$. This proves the upper bound even for integer q . Since

$$B_D(m, r, q)/q \leq B_S(m, r, q) \leq B_D(m, r, q),$$

the two logarithms differ by at most $\log m$. Primes $p = a_*m + o(m)$ with $r = 2p - 1$ give the matching lower bound. The prime-power assertions follow because their parameter set lies between the primes and the integers. Their validity as certificates is proved in Appendix ??.

For the last assertion, compactness and the unique maximum of the displayed continuous upper bound force $a \rightarrow a_*$. The uniform entropy estimate then forces $H(\rho) \rightarrow H(2a_*)$. As $\rho \leq 1/2$ and H is strictly increasing there, $\rho \rightarrow 2a_*$. $\square$

The classical density optimization is also discussed in Pikhurko [?], Section 6.4. The formulation above makes its scope explicit. The following corollary gives a finite-error version of parameter stability.

Corollary 8.18 (Quantitative stability of the binary certificate). *Let m, r, q satisfy the integer constraints in the definition, and let $X \in \{S, D\}$. Suppose $\delta \geq 0$ and*

$$\frac{\log B_X(m, r, q)}{m} \geq \log \beta - \delta.$$

Put $a = q/m$, $\rho = r/m$, and

$$E_m = \delta + \frac{\log m + \log(m+1)}{m}.$$

If $E_m \leq 1/100$, then

$$4(a - a_*)^2 + \log(3/2)(2a - \rho) \leq E_m. \quad (8.8)$$

In particular,

$$|a - a_*| \leq \frac{1}{2} \sqrt{E_m}, \quad 0 \leq 2a - \rho \leq \frac{E_m}{\log(3/2)}, \quad |\rho - 2a_*| \leq \sqrt{E_m} + \frac{E_m}{\log(3/2)}.$$

For every $0 < \gamma < 4\sqrt{2}$ there is $E_0(\gamma) > 0$ such that $E_m \leq E_0(\gamma)$ strengthens the deficit estimate to

$$\gamma(a - a_*)^2 + \log(3/2)(2a - \rho) \leq E_m, \quad |a - a_*| \leq \sqrt{E_m/\gamma}.$$

Proof. Since $\binom{m}{q-1} = \binom{m}{q} q/(m - q + 1)$, the entropy estimates in the preceding proof give the explicit bound

$$\log B_X(m, r, q) \leq \log B_D(m, r, q) \leq m\{H(\rho) - H(a)\} + \log(m + 1) + \log m.$$

Thus $\log \beta - H(\rho) + H(a) \leq E_m$. If $a \geq 1/4$, monotonicity gives $H(\rho) - H(a) \leq \log 2 - H(1/4)$, whose gap from $\log \beta$ is greater than $1/100$. Hence $a < 1/4$. For $f(a) = H(2a) - H(a)$, direct differentiation gives

$$f''(a) = -\frac{1}{a(1-a)(1-2a)} \leq -8 \quad (0 < a < 1/4).$$

Here $a(1-a)(1-2a) \leq a(1-2a) \leq 1/8$. Since $f'(a_*) = 0$ and $f(a_*) = \log \beta$, integration yields $\log \beta - f(a) \geq 4(a - a_*)^2$. Therefore $|a - a_*| \leq \sqrt{E_m}/2 \leq 1/20$, which implies $a < 1/5$. On $[\rho, 2a] \subset (0, 2/5)$ we have $H'(t) = \log((1-t)/t) \geq \log(3/2)$, and consequently

$$H(2a) - H(\rho) \geq \log(3/2)(2a - \rho).$$

Adding the last two deficit bounds proves (??). The remaining displayed assertions follow directly. Finally, $-f''(a_*)/2 = 4\sqrt{2}$ and f'' is continuous near a_* . For $0 < \gamma < 4\sqrt{2}$, choose $h > 0$ such that $-f''(t)/2 \geq \gamma$ whenever $|t - a_*| \leq h$. If $E_m \leq \min\{1/100, 4h^2\}$, the crude bound places the segment from a_* to a in this interval. Integration gives $\log \beta - f(a) \geq \gamma(a - a_*)^2$, with the layer-gap term unchanged. $\square$

The square-root density error and the linear layer-gap error have different sources: the entropy difference has a nondegenerate maximum in a , whereas H is strictly increasing at $2a_*$. For example, at $\delta = 0$ the bound on $|a - a_*|$ is 0.02146 for $m = 10^4$ and 0.00263 for $m = 10^6$. These are direct evaluations of the conditional estimate.

8.8. Known Asymptotic Bounds. The known asymptotic bounds for ordinary colorings are

$$(1.239 \dots + o(1))^n \leq \chi(\mathbf{E}^n) \leq (3 + o(1))^n. \quad (8.9)$$

Raigorodskii proved the lower bound for ordinary colorings [?]. See also the survey of Raigorodskii and Sinenikov-Murylev [?]. The upper bound is the classical Larman-Rogers bound [?]. Prosanov [?] gave a new proof using coverings by shrunken Voronoi cells together with a fractional-to-integral covering estimate.

Raigorodskii's larger base comes from a different construction rather than a different choice of prime in the binary model. Once $p/m \rightarrow a$, the rate of the ratio (??) is $H(2a) - H(a)$, whose maximum gives the base β . This describes the limit of that certificate and does not give an upper bound for the chromatic number of the finite graph. Raigorodskii instead works in $\{-1, 0, 1\}^m$ with two weight parameters. A binary layer fixes only the number of ones, whereas a ternary layer can prescribe the numbers of positive and negative entries independently. This adds another parameter for balancing the vertex count against the color-class restriction. We quote the improvement with attribution because its proof is outside the scope of these chapters. Appendix ?? explains

why prime powers give further finite choices in (??) but do not change its optimized exponential rate either.

10. APPLICATION TO RAMSEY THEORY*

This starred chapter assumes familiarity with basic Ramsey theory.

For positive integers a, b , let $R(a, b)$ be the least N such that every red-blue coloring of the edges of K_N contains a red K_a or a blue K_b , and write $R(k) = R(k, k)$. A vertex set is *homogeneous* if all edges inside it have the same color, so a coloring on N vertices with no homogeneous k -set proves $R(k) > N$.

The first two sections recall the classical upper bound and the probabilistic lower bound. See Li and Lin [?], Chapter 6, especially Section 6.2, pp. 131–138. The remaining sections construct explicit colorings. Oddtown and Fisher give a cubic construction, Lemma ?? gives every fixed polynomial degree, and a growing prime gives a superpolynomial construction. We distinguish throughout between an existence proof for a coloring and an efficient deterministic rule for its edges.

The two-color constraint. Chapter ?? required a bound for one type of color class inside a fixed geometric graph. A Ramsey construction must control red and blue homogeneous families simultaneously. The two intersection conditions are complementary, so a parameter choice that improves one certificate may worsen the other. The uniformity $p^2 - 1$ in Section ?? balances the two polynomial degrees. Section ?? gives a quantitative form of this balance for the certificate families studied here.

An algorithmic distinction is also useful. The first-moment argument proves the existence of much larger Ramsey colorings without providing an efficient rule for their edges. The definitions below make the notions of explicit and strongly explicit construction precise.

Definition 10.1. A graph family is *explicit* if a deterministic algorithm produces its full adjacency matrix in time polynomial in its number N of vertices. It is *strongly explicit* if, from the family parameters and two vertex labels of $O(\log N)$ bits, adjacency can be decided deterministically in time polynomial in $\log N$. For families indexed by a target parameter k , we also require that any auxiliary parameters be produced deterministically from k within the same time bound. The families below have $\log k = O(\log N)$. Thus parameter selection is included, rather than supplied as unbounded preprocessing. Theorem ?? verifies this requirement for its growing-prime choice.

10.1. An Elementary Upper Bound. The recurrence behind the usual diagonal upper bound goes back to Erdős and Szekeres [?]. We include the standard proof to fix the scale used later.

Theorem 10.2 (Erdős-Szekeres). *For every integer $k \geq 2$,*

$$R(k) \leq \binom{2k-2}{k-1} \leq \frac{4^{k-1}}{\sqrt{k}}.$$

More generally, $R(a, b) \leq \binom{a+b-2}{a-1}$ for positive integers a, b .

Proof. For integers $a, b \geq 2$ we first show that

$$R(a, b) \leq R(a-1, b) + R(a, b-1). \tag{10.1}$$

Put $u = R(a-1, b)$ and $v = R(a, b-1)$. In any red-blue coloring of K_{u+v} , choose a vertex x . Among its $u+v-1$ neighbors, at least u are joined to x in red or at least v are joined to x in blue. In the first case the red neighborhood contains a blue K_b or a red K_{a-1} , which extends with x to a red K_a . The second case is symmetric. This proves (??).

Since $R(1, b) = R(a, 1) = 1$, induction on $a+b$ and Pascal's identity give

$$R(a, b) \leq \binom{a+b-3}{a-2} + \binom{a+b-3}{a-1} = \binom{a+b-2}{a-1}$$

when $a, b \geq 2$, with the boundary cases given by the same formula. Taking $a = b = k$ proves the first inequality.

For the second, put $t = k-1$. For every integer $i \geq 1$, squaring shows that $(2i-1)/(2i) \leq \sqrt{i/(i+1)}$. Hence

$$\frac{\binom{2t}{t}}{4^t} = \prod_{i=1}^t \frac{2i-1}{2i} \leq \prod_{i=1}^t \sqrt{\frac{i}{i+1}} = \frac{1}{\sqrt{t+1}}.$$

□

This proof bounds every coloring. Lower bounds need colorings that avoid homogeneous sets, and random edges give a remarkably strong existence result.

10.2. A Probabilistic Exponential Lower Bound. Erdős's 1947 probabilistic argument [?] gives a much larger existence bound than the explicit constructions below, although it does not identify a coloring.

Theorem 10.3 (First-moment lower bound). *If $k \geq 2$ and $N \geq 0$ are integers such that*

$$2 \binom{N}{k} 2^{-\binom{k}{2}} < 1, \tag{10.2}$$

then $R(k) > N$. In particular, if $0 < c < 1/(e\sqrt{2})$ is fixed, then for all sufficiently large k ,

$$R(k) > \lfloor ck2^{k/2} \rfloor.$$

Thus $R(k) = \Omega(k2^{k/2})$.

Proof. Color each edge of K_N red or blue independently, with probability $1/2$ for each color, and let X count the homogeneous k -sets. A fixed k -set is all red with probability $2^{-\binom{k}{2}}$ and all blue with the same probability, and for $k \geq 2$ these events are disjoint. By linearity of expectation,

$$\mathbb{E}X = 2 \binom{N}{k} 2^{-\binom{k}{2}}.$$

If this is less than one then some coloring has $X = 0$. Otherwise every coloring would have $X \geq 1$, forcing $\mathbb{E}X \geq 1$. Such a coloring has no homogeneous k -set, so $R(k) > N$. The case $N < k$ is vacuous.

For the stated constant, substitute $N = \lfloor ck2^{k/2} \rfloor$ and use $\binom{N}{k} \leq (eN/k)^k$ to obtain $\mathbb{E}X \leq 2(ec\sqrt{2})^k$, which tends to zero when $c < 1/(e\sqrt{2})$. □

The proof neither identifies a successful coloring nor gives a deterministic algorithm producing one in time polynomial in N . Exhaustive search finds a witness in principle, but that is a different computational guarantee.

10.3. A Constructive Cubic Lower Bound. We next construct an explicit coloring. The first example turns Oddtown and Fisher into an edge-coloring argument and serves as a concrete introduction to the method. Oddtown is Theorem ???. Fisher is the corresponding real-vector argument with inner products in place of parity.

Theorem 10.4 (Uniform Fisher inequality). *Let $A_1, \dots, A_b$ be distinct r -subsets of $[m]$ with $|A_i \cap A_j| = \lambda$ for all $i \neq j$, where $0 \leq \lambda < r$. Then $b \leq m$.*

Proof. Let $u_i \in \mathbb{R}^m$ be the incidence vector of A_i and suppose $\sum_i c_i u_i = 0$ for real c_i . Taking the squared length of the left side and using $u_i \cdot u_j = \lambda$ for $i \neq j$ and $u_i \cdot u_i = r$,

$$0 = \left\| \sum_i c_i u_i \right\|^2 = (r - \lambda) \sum_i c_i^2 + \lambda \left(\sum_i c_i \right)^2.$$

Both terms are nonnegative and $r - \lambda > 0$, so every c_i is zero. The b vectors are therefore linearly independent in $\mathbb{R}^m$. $\square$

The vertices below are explicitly enumerable subsets of $[m]$ and each edge color is read off from an intersection size, which is exactly the notion of explicitness in Definition ??.

Theorem 10.5. *For every integer $k \geq 4$ there is an explicitly specified coloring on $\binom{k-1}{3}$ vertices with no homogeneous k -set. Hence*

$$R(k) > \binom{k-1}{3} = \left(\frac{1}{6} + o(1) \right) k^3.$$

Proof. Put $m = k - 1$ and use the three-element subsets of $[m]$ as vertices. Color $\{A, B\}$ red when $|A \cap B|$ is even and blue when $|A \cap B| = 1$. Distinct triples meet in zero, one, or two elements, so this colors every edge.

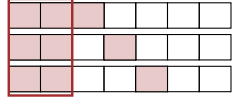
A red homogeneous family consists of odd sets with pairwise even intersections, so Theorem ?? bounds it by m . In a blue homogeneous family every two distinct triples meet in exactly one point, so Theorem ?? with $r = 3$ and $\lambda = 1$ gives the same bound. Neither color has a k -set.

The triples can be enumerated deterministically and each pair colored by comparing entries, which is polynomial in the number of vertices. $\square$

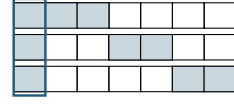
The cubic bound is far below the random one. Its value here is that the edge rule and the obstruction to a large homogeneous family can both be inspected directly.

10.4. Constructive Lower Bounds of Every Polynomial Degree. To increase the degree, replace parity by congruence modulo a prime p . The uniformity $p^2 - 1$ is obtained by balancing the red and blue certificate degrees. Start with $r = cp - 1$, where $c \geq 1$ is an integer, and color an edge blue when its intersection is congruent to $p - 1$ modulo p and red otherwise. A red family then permits the $p - 1$ off-diagonal residues $0, \dots, p - 2$, while a blue family permits the $c - 1$ integer intersection values

$$p - 1, 2p - 1, \dots, (c - 1)p - 1.$$



(a) Red: intersections of size two



(b) Blue: intersections of size one

FIGURE 5. The two obstacles in the coloring of Theorem ??, drawn as incidence vectors for $m = 7$. Each row is a triple, and the boxed columns are the elements common to all three. On the left every pairwise intersection has size two, so all of these edges are red. The sets have odd size and even pairwise intersections, so Oddtown caps such a family at m . On the right every pairwise intersection has size exactly one, so all of these edges are blue, and Fisher caps that family at m . A homogeneous k -set would be one of these two pictures with k rows. For a general prime the same two pictures hold with $(p^2 - 1)$ -sets, with “even” replaced by “residue other than $p - 1$ modulo p ” and “exactly one” by “one of the $p - 1$ values $jp - 1$ ”.

So the two polynomial degrees are $p - 1$ and $c - 1$.

Choice of the uniformity $p^2 - 1$

For $r = cp - 1$, a red homogeneous family permits the $p - 1$ residues $0, \dots, p - 2$ modulo p , giving degree $p - 1$. A blue homogeneous family permits the $c - 1$ exact values $p - 1, 2p - 1, \dots, (c - 1)p - 1$, giving degree $c - 1$. The larger degree determines the weaker of the two certificate bounds, so the balanced choice is $c = p$, equivalently $r = p^2 - 1$. This is an optimization of the two stated certificates, not of all possible edge rules.

This is the classical Frankl–Wilson Ramsey graph [?]. Lemma ?? bounds homogeneous families in both colors. The two applications use different fields.

Theorem 10.6 (Frankl–Wilson coloring). *Let p be prime and $m \geq p^2 - 1$. Put*

$$r = p^2 - 1, \quad S(m, p) = \sum_{j=0}^{p-1} \binom{m}{j}.$$

There is an explicit coloring on $\binom{m}{r}$ vertices in which every homogeneous set has at most $S(m, p)$ vertices. Consequently

$$R(S(m, p) + 1) > \binom{m}{p^2 - 1}. \quad (10.3)$$

Proof. The vertices are the r -subsets of $[m]$, with the rule

$$\{A, B\} \text{ is } \begin{cases} \text{red,} & |A \cap B| \not\equiv p - 1 \pmod{p}, \\ \text{blue,} & |A \cap B| \equiv p - 1 \pmod{p}. \end{cases}$$

For a red homogeneous family, apply Lemma ?? over $\mathbb{F}_p$ with $L = \{0, 1, \dots, p - 2\}$. The size $r = p^2 - 1$ is congruent to $p - 1$ modulo p , hence lies outside L , while every

off-diagonal residue lies in L . With $s = |L| = p - 1$ the family has at most $S(m, p)$ members.

For a blue homogeneous family, distinctness gives $|A \cap B| < r$, so the permitted integer intersection values are exactly

$$L' = \{p - 1, 2p - 1, \dots, (p - 1)p - 1\},$$

which has $p - 1$ elements, none equal to $r = p^2 - 1$. Now apply Lemma ?? over $\mathbb{Q}$ with $L = L'$: the size r lies outside L' and every off-diagonal intersection lies in L' . Again $s = p - 1$, so this family also has at most $S(m, p)$ members.

For explicitness, enumeration is polynomial in the output size. When $1 \leq r \leq m - 1$ we have $N = \binom{m}{r} \geq m$, and generating all subsets and computing all intersections takes $O(N^2 m)$ elementary membership operations with polynomial bit overhead. When $r = m$ the graph has one vertex. $\square$

Remark 10.7. The two colors use the same lemma over different fields. Over $\mathbb{F}_p$ the permitted set is a set of residues. Over $\mathbb{Q}$ it is a set of exact integer values, and there the polynomial $f(t) = \prod_{j=1}^{p-1} (t - (jp - 1))$ simply vanishes at every off-diagonal intersection. No rank computation is needed in either case. Appendix ?? replaces $S(m, p)$ by $D(m, p) = \binom{m}{p-1}$ for both colors, at the cost of a rank argument. Since $D \leq S \leq pD$, the improvement is a factor of at most p and is invisible in everything below. At $p = 2$ we get $r = 3$ and $S(m, 2) = m + 1$, one more than the bound m obtained directly from Oddtown and Fisher in Theorem ??.

Corollary 10.8. *Every fixed prime p gives a constructive lower bound $R(k) = \Omega_p(k^{p+1})$. More precisely, the construction has a vertex count asymptotic to*

$$\frac{((p - 1)!)^{p+1}}{(p^2 - 1)!} k^{p+1}. \quad (10.4)$$

Hence for every real $d > 0$ there are $c_d > 0$ and k_d such that an explicit coloring proves $R(k) > c_d k^d$ for every integer $k \geq k_d$.

Proof. Fix p and put $r = p^2 - 1$. For sufficiently large k choose $m \geq r$ maximal with $S(m, p) < k$. Then

$$S(m, p) < k \leq S(m + 1, p), \quad \frac{S(m + 1, p)}{S(m, p)} \rightarrow 1,$$

the last limit because $S(m, p) = \binom{m}{p-1}(1 + O(1/m))$ for fixed p and $\binom{m+1}{p-1}/\binom{m}{p-1} = (m+1)/(m-p+2) \rightarrow 1$. Here p is fixed and $m \rightarrow \infty$ as $k \rightarrow \infty$, so $S(m, p) \sim k$. Since $S(m, p) \sim m^{p-1}/(p-1)!$,

$$m \sim ((p - 1)! k)^{1/(p-1)}.$$

Theorem ?? gives a coloring with no homogeneous k -set and with

$$\binom{m}{r} \sim \frac{m^{p^2-1}}{(p^2 - 1)!} \sim \frac{((p - 1)!)^{p+1}}{(p^2 - 1)!} k^{p+1}$$

vertices, the exponent coming from $(p^2 - 1)/(p - 1) = p + 1$. Given $d > 0$, choose a fixed prime with $p + 1 \geq d$ and let c_d be half the positive coefficient in (??). At

$p = 2$ the maximal choice is $m = k - 2$, one fewer ground-set element than in the direct Oddtown–Fisher construction. $\square$

10.5. Optimizing the Prime Parameter. This completes the combinatorial construction. Both m and p can still vary, and increasing m produces more vertices while also increasing the bound on a homogeneous family. To compare the two effects we first allow a general power scale $m = \lfloor p^\alpha \rfloor$ with $\alpha > 2$, which keeps the uniformity $p^2 - 1$ below the ground-set size and exposes the leading coefficient before any particular scale is chosen. We use the elementary estimate

$$(n/t)^t \leq \binom{n}{t} \leq (en/t)^t \quad (n \geq t \geq 1), \quad (10.5)$$

whose lower bound follows by multiplying $(n-i)/(t-i) \geq n/t$ for $0 \leq i < t$ and whose upper bound follows from $t! \geq (t/e)^t$.

Proposition 10.9 (Optimization among fixed power scales). *Fix a real $\alpha > 2$ and for a prime p put*

$$S_{p,\alpha} = \sum_{j=0}^{p-1} \binom{\lfloor p^\alpha \rfloor}{j}, \quad N_{p,\alpha} = \binom{\lfloor p^\alpha \rfloor}{p^2 - 1}.$$

For sufficiently large k choose the largest prime p with $S_{p,\alpha} < k$. Then the coloring of Theorem ?? has no homogeneous k -set and

$$\log N_{p,\alpha} = \left(\frac{\alpha - 2}{(\alpha - 1)^2} + o(1) \right) \frac{(\log k)^2}{\log \log k}. \quad (10.6)$$

The coefficient has its unique maximum at $\alpha = 3$, where it equals $1/4$.

Proof. Since $\binom{\lfloor p^\alpha \rfloor}{p-1} \leq S_{p,\alpha} \leq p \binom{\lfloor p^\alpha \rfloor}{p-1}$ and $\log p = O(p)$, estimate (??) gives, for fixed α as $p \rightarrow \infty$,

$$\log S_{p,\alpha} = (\alpha - 1)p \log p + O_\alpha(p), \quad (10.7)$$

$$\log N_{p,\alpha} = (\alpha - 2)p^2 \log p + O_\alpha(p^2). \quad (10.8)$$

Here $\log \lfloor p^\alpha \rfloor = \alpha \log p + O(p^{-\alpha})$, so the floor affects neither leading term.

The quantities $S_{p,\alpha}$ tend to infinity and are strictly increasing in p : enlarging the ground set increases every existing term, and the larger prime adds further nonnegative terms. So the choice of p is well defined, and if q is the next prime then maximality gives $S_{p,\alpha} < k \leq S_{q,\alpha}$. As $k \rightarrow \infty$ we have $p \rightarrow \infty$, and the prime number theorem gives $q/p \rightarrow 1$, so applying (??) at both endpoints yields

$$\log k = (\alpha - 1 + o(1)) p \log p.$$

Taking logarithms gives $\log \log k = (1 + o(1)) \log p$, whence

$$p = (1 + o(1)) \frac{\log k}{(\alpha - 1) \log \log k}, \quad (10.9)$$

and substituting (??) into (??) gives (??). Finally

$$\frac{d}{d\alpha} \frac{\alpha - 2}{(\alpha - 1)^2} = \frac{3 - \alpha}{(\alpha - 1)^3},$$

so the coefficient increases on $(2, 3)$ and decreases on $(3, \infty)$. $\square$

Choice of the ground-set scale $m = p^3$

Let $m = \lfloor p^\alpha \rfloor$. Then $\log S_{p,\alpha} = (\alpha - 1)p \log p + O(p)$ for the homogeneous-family certificate, while $\log N_{p,\alpha} = (\alpha - 2)p^2 \log p + O(p^2)$ for the vertex count. The condition $S_{p,\alpha} < k$ gives $p \approx \log k / ((\alpha - 1) \log \log k)$. After substitution, the leading coefficient in $\log N_{p,\alpha}$ is $(\alpha - 2)/(\alpha - 1)^2$. This expression is maximized at $\alpha = 3$, where its value is $1/4$. Thus $m = p^3$ is optimal among fixed power scales. Section ?? removes the fixed-power restriction.

We now fix the integer scale $m = p^3$ for the explicit construction. Section ?? later allows arbitrary ground-set sizes and unequal degree bounds.

Theorem 10.10 (Explicit superpolynomial scale). *There is a strongly explicit family of colorings, indexed by all sufficiently large integers k , with no homogeneous k -set and with vertex counts $N(k)$ satisfying*

$$\log N(k) = (1 + o(1)) \frac{(\log k)^2}{4 \log \log k}. \quad (10.10)$$

Consequently, for every $\varepsilon > 0$ and every sufficiently large integer k ,

$$R(k) > \exp \left((1 - \varepsilon) \frac{(\log k)^2}{4 \log \log k} \right).$$

Proof. Set $S_p = \sum_{j < p} \binom{p^3}{j}$ and $N_p = \binom{p^3}{p^2 - 1}$, choose the largest prime with $S_p < k$, and put $N(k) = N_p$. Theorem ?? supplies the coloring, whose homogeneous sets have size at most $S_p < k$. At $\alpha = 3$ the estimates of Proposition ?? read

$$\log S_p = 2p \log p + O(p), \quad \log N_p = p^2 \log p + O(p^2),$$

and the same proposition gives (??) for every sufficiently large k , including values outside the subsequence $k = S_p + 1$.

All parameters are integers and can be found deterministically: for example, enumerate primes by trial division and evaluate S_p until it first reaches k , then take the preceding prime. If q is the first prime with $S_q \geq k$, then $q/p \rightarrow 1$. The search tests $O(p)$ integers. Trial division and the binomial recurrence use polynomially many operations on $O(p \log p)$ -bit integers. This is polynomial in p and $\log k$, whereas $\log N_p = \Theta(p^2 \log p)$. Thus the parameter search is polynomial in the output size, and enumerating the subsets and applying the intersection rule is polynomial in $N(k)$ by Theorem ?. The final inequality follows from (??) and $R(k) > N(k)$. $\square$

The logarithm in (??) grows faster than $d \log k$ for every fixed d , but slower than any positive multiple of k . So this construction is superpolynomial in k and still far below the probabilistic size $k 2^{k/2}$ of Section ?. The coefficient $1/4$ comes from balancing two binomial growth rates, not from a new edge rule.

Summary of the construction. Parity gives a cubic coloring, a fixed prime gives every fixed polynomial degree, and a growing prime gives a superpolynomial construction. The

choices $r = p^2 - 1$ and $m = p^3$ balance the two certificate degrees and the fixed-power ground-set scale, respectively. These constructions remain far below the probabilistic scale $k2^{k/2}$. Section ?? determines the asymptotic limit of the specified certificates before later sections compare them with other constructions.

Strong explicitness of the three constructions. Label a vertex by its sorted list of elements. For triples, and for the fixed-prime construction, the label has $O(r \log m) = O(\log N)$ bits with r fixed. In the growing-prime construction $r = p^2 - 1$, $m = p^3$, and

$$r \log_2 m = (3 + o(1))p^2 \log_2 p = (3 + o(1)) \log_2 N.$$

Two sorted lists can be intersected in $O(r)$ comparisons, followed by one residue test. This is deterministic polynomial time in $\log N$ in each of the three regimes, so all three satisfy the strongly explicit definition above.

10.6. Optimality and Stability of the Intersection Certificates. The upper bound in this section needs only that the modulus is an integer at least two. Primality enters the validity of the graph certificate and the matching construction, not the optimization bound. The larger of the two degrees controls the cost of the certificate, while their product determines the layer size. We therefore expect near-optimality to balance the degrees. The proof makes this uniform over every ground-set size.

This uses the same optimization mechanism as Section ??, in a different regime. There the layer and modulus are proportional to m , giving an entropy difference with an interior maximum. Here the degrees are small relative to m . The sparse estimate $\log \binom{m}{s} \approx s \log(m/s)$ turns the budget into a quadratic objective. Completing its square replaces the entropy calculation.

Proposition 10.11 (Unequal intersection degrees). *Let p be prime, $c \geq 1$ an integer, and $m \geq r = pc - 1$. Color pairs of r -subsets blue when their intersection has residue $p - 1$ modulo p , and red otherwise. Put $d = \max\{p, c\}$ and*

$$T_S(m, p, c) = \sum_{j=0}^{d-1} \binom{m}{j}, \quad T_D(m, p, c) = \binom{m}{d-1}.$$

Every homogeneous family has size at most $T_S(m, p, c)$. Appendix ?? sharpens this to $T_D(m, p, c)$.

Proof. The red family permits $p - 1$ residues, while the blue family permits the $c - 1$ integers $p - 1, 2p - 1, \dots, (c - 1)p - 1$. Apply Lemma ?? over $\mathbb{F}_p$ and $\mathbb{Q}$, respectively. The two sums are increasing in their upper index, so their maximum is T_S . For the uniform refinement, the corresponding bounds are $\binom{m}{p-1}$ and $\binom{m}{c-1}$. When $c \geq 2$, we have $m \geq pc - 1 \geq 2d - 1$, so both indices lie below $m/2$ and their maximum is T_D . When $c = 1$, the red bound equals the vertex count and the blue bound is one, giving the same conclusion. The edge rule is explicit by the enumeration argument already given. $\square$

Definition 10.12 (Certified vertex count). For an integer $k \geq 2$ and $X \in \{S, D\}$, define

$$F_X(k) = \max \left(\{1\} \cup \left\{ \binom{m}{pc-1} : p \text{ prime, } c \geq 1, m \geq pc - 1, T_X(m, p, c) < k \right\} \right).$$

The strict inequality is part of the definition: it certifies the absence of a homogeneous k -set using precisely these intersection bounds. It is a sufficient condition on a coloring, not a necessary condition for its actual clique and independence numbers to be below k .

These maxima are finite. For $c = 1$ the certified vertex count is below k . For $c \geq 2$, write $u = \min\{p, c\}$, $d = \max\{p, c\}$ and $s = d - 1$. Since $m/s \geq (pc - 1)/(d - 1) \geq u \geq 2$,

$$\binom{m}{s} \geq (m/s)^s \geq 2^s.$$

Thus $s < \log_2 k$, and then $(m/s)^s < k$ also bounds m .

Example 10.13 (The certificate need not detect the graph's performance). Take $p = c = 2$ and $m = 5$. Complementing the ten triples identifies them with the pairs of [5]: a red family is a pairwise intersecting family of pairs, and a blue family consists of disjoint pairs. The largest red family has size four, since an intersecting family of edges is a star or a triangle. A largest blue family has size two. Thus the coloring has no homogeneous 5-set. Nevertheless $T_D = 5$ and $T_S = 6$, so neither certificate satisfies its required strict inequality at $k = 5$.

Theorem 10.14 (Sharp optimization of the certificates). *For $X = S$ and $X = D$,*

$$\log F_X(k) = \left(\frac{1}{4} + o(1) \right) \frac{(\log k)^2}{\log \log k}. \quad (10.11)$$

The same conclusion holds if one restricts the maximum to $c = p$. In particular, arbitrary ground-set sizes and unequal degrees cannot improve the leading coefficient of these certificates. The same upper estimate holds if the formal maximum allows every integer $p \geq 2$. Primes already attain the matching lower bound.

Proof. The lower bound for F_S , already with $c = p$ and $m = p^3$, is Theorem ???. Since $T_D \leq T_S$, it remains to prove the upper bound for F_D . Put $L = \log k$ and $\ell = \log L$, and consider any admissible parameters. The case $c = 1$ gives $\log N < L = o(L^2/\ell)$, so assume $c \geq 2$ and use u, d, s as above, with $r = du - 1$ and $N = \binom{m}{r}$. The certificate and (??) give

$$s \log(m/s) < L, \quad (d - 1) \log u < L. \quad (10.12)$$

Consequently

$$\begin{aligned} \log N &\leq r(1 + \log(m/r)) \\ &< \frac{r}{s} L - r(\log(r/s) - 1) \\ &\leq (u + 1)L - (du - 1)(\log u - 1), \end{aligned} \quad (10.13)$$

because $u \leq r/s = u + (u - 1)/(d - 1) \leq u + 1$. This inequality holds for every admissible m, p, c , with no power-scale assumption and no use of primality.

If $u \leq L/\ell^2$, then (??) gives $d \leq L/\log 2 + 1$ and $r = O(uL)$. Dropping the nonpositive term $-r \log(r/s)$ in the second line above yields $\log N \leq (u + 1)L + r = O(L^2/\ell^2) = o(L^2/\ell)$.

In the remaining range $u > L/\ell^2$, the bounds $u \leq d \leq L/\log 2 + 1$ imply, uniformly, $\log u = \ell + O(\log \ell)$. Here $d \geq u$ and $\log u - 1 > 0$. Hence (??) gives

$$\log N \leq (u+1)L - (u^2-1)(\log u - 1) \leq uL - A_L u^2 + O(L),$$

where $A_L = \ell - 2\log \ell - 1 = (1 + o(1))\ell$ is positive for large L . Completing the square bounds the last expression by $L^2/(4A_L) + O(L) = (1/4 + o(1))L^2/\ell$. This is uniform over all the parameters, so it also bounds their maximum. The lower construction is in the restricted class $c = p$, which proves the remaining assertion. $\square$

Stability in rate form. Write $L = \log k$ and $\ell = \log L$. A normalized deficit at most δ forces the smaller degree to be within $O(\sqrt{\delta + \log \ell/\ell})$ of $1/2$ after multiplication by ℓ/L , and bounds the normalized degree imbalance by $O(\delta + \log \ell/\ell)$. In particular, a deficit tending to zero forces

$$p, c = (1 + o(1))\frac{L}{2\ell}, \quad m = p^{3+o(1)}.$$

The following theorem records an explicit error inequality behind this asymptotic statement. Its overhead decays very slowly because $\ell = \log \log k$.

Theorem 10.15 (Stability with an explicit asymptotic error). *Let $p \geq 2$, $c \geq 1$, $m \geq pc - 1$ be integers, and define the formal costs*

$$T_D(m, p, c) = \binom{m}{\max\{p, c\} - 1}, \quad T_S(m, p, c) = \sum_{j=0}^{\max\{p, c\}-1} \binom{m}{j}.$$

Suppose $T_D(m, p, c) < k$, set $N = \binom{m}{pc-1}$, $L = \log k$, $\ell = \log L$, and suppose $\ell \geq 64$. Define

$$\eta = \frac{2\log \ell + 1}{\ell}, \quad A = 1 - \eta, \quad E = \frac{\delta}{A} + \frac{\eta}{4A^2} + \frac{2\ell}{AL}.$$

Suppose $\delta \geq 0$, $E \leq 1/16$, and

$$\frac{\ell \log N}{L^2} \geq \frac{1}{4} - \delta. \tag{10.14}$$

Write $u = \min\{p, c\}$, $d = \max\{p, c\}$, $x = u\ell/L$, and $y = d\ell/L$. Then

$$\left(x - \frac{1}{2A}\right)^2 + x(y - x) \leq E. \tag{10.15}$$

In particular,

$$|x - \tfrac{1}{2}| \leq \sqrt{E} + \frac{\eta}{2A} \leq 2\sqrt{E}, \quad 0 \leq y - x \leq 4E, \quad \frac{\log m}{\log p} = 3 + O(\sqrt{E}), \tag{10.16}$$

with an absolute implied constant, uniform in all the parameters. The same assertions hold with T_S in place of T_D . Since $E = O(\delta + \log \ell/\ell)$, this gives square-root control of the normalized smaller degree and of the logarithmic ground-set scale, and linear control of the normalized degree imbalance.

Proof. Put $z = \ell \log N / L^2$. The hypotheses give $\delta \leq E \leq 1/16$, so $z \geq 3/16$. If $c = 1$, then $N < k$, hence $z < \ell/L < 3/16$, a contradiction. Thus $c \geq 2$ and the budget and envelope from the preceding proof apply.

First suppose $u \leq L/\ell^2$. Using $d \leq L/\log 2 + 1$ and $\log N \leq (u+1)L + r$, where $r = du - 1$, gives

$$z \leq \frac{1 + 1/\log 2}{\ell} + \frac{\ell}{L} + \frac{1}{L\ell} < \frac{3}{16} \quad (\ell \geq 64),$$

again a contradiction. Therefore $u > L/\ell^2$ and $\log u - 1 \geq A\ell > 0$. Also $u \leq L/\log 2 + 1$, so $\log u - 1 < \ell$ in this range. On dividing (??) by L^2/ℓ , we obtain

$$\begin{aligned} z &\leq x - xy \frac{\log u - 1}{\ell} + \frac{\ell}{L} + \frac{\ell(\log u - 1)}{L^2} \\ &\leq x - Axy + \frac{2\ell}{L} \\ &= \frac{1}{4A} - A \left(x - \frac{1}{2A} \right)^2 - Ax(y - x) + \frac{2\ell}{L}. \end{aligned}$$

Combining this with (??) proves (??).

In particular $x \geq 1/(2A) - \sqrt{E} \geq 1/4$, so $y - x \leq 4E$. Moreover

$$|x - \frac{1}{2}| \leq \sqrt{E} + \frac{\eta}{2A} \leq 2\sqrt{E},$$

because $E \geq \eta/(4A^2)$ and $0 < \eta < 1$. It follows that both x and y equal $1/2 + O(\sqrt{E})$ and are bounded above and away from zero by absolute constants.

For completeness, the exact estimates for the ground-set size are

$$\frac{(1/4 - \delta)L^2}{\ell r} + \log r - 1 \leq \log m < \frac{L}{d-1} + \log(d-1). \quad (10.17)$$

The lower estimate follows from $\log N \leq r(1 + \log(m/r))$. The upper one is (??). To evaluate them uniformly, note that

$$\frac{r\ell^2}{L^2} = xy - \frac{\ell^2}{L^2} = \frac{1}{4} + O(\sqrt{E}), \quad \frac{(d-1)\ell}{L} = \frac{1}{2} + O(\sqrt{E}).$$

Both expressions are bounded away from zero. Their logarithms give $\log r = 2\ell + O(\log \ell)$ and $\log(d-1) = \ell + O(\log \ell)$. Since $\log \ell/\ell = O(E)$ and $\delta \leq E$, (??) now yields $\log m/\ell = 3 + O(\sqrt{E})$. Finally $p\ell/L$ lies between x and y , so $\log p/\ell = 1 + O(\log \ell/\ell)$, proving the ratio assertion. All constants are uniform on the bounded ranges just obtained. Since $T_D \leq T_S$, the sum-certificate assertion follows as well. $\square$

The explicit constants are not numerically effective at moderate k . At $\ell = 64$ and $\delta = 0$, $E = 0.04986$. The sharper and coarser bounds on $|x - 1/2|$ are 0.30849 and 0.44658, respectively. The coarser bound first falls below 0.05 at about $\ell = 7700$, corresponding to $k = \exp(\exp(7700))$. The result is therefore best viewed as an asymptotic stability statement, unlike the finite estimates following Corollary ???. The conclusion $m = p^{3+o(1)}$ concerns logarithmic exponents and does not assert $m/p^3 \rightarrow 1$.

Relation to earlier parameter optimizations. Frankl and Wilson [?], Section 6, Theorem 8, already allow an arbitrary ground-set size and prime-power modulus, with

uniformity $q^2 - 1$. Their choice $m = p^3$ gives the coefficient $1/4$. Pikhurko [?], Section 9.3, chooses the ground-set size from the certificate budget and optimizes in p , obtaining $p \sim L/(2\ell)$. Thus neither varying m nor the balanced optimum is by itself a new principle. Theorem ?? supplies a uniform upper estimate for the stated class, including unequal degrees. Theorem ?? measures the loss from imbalance and displacement with an explicit finite error.

Gopalan [?], Theorems 4 and 10, proves product lower bounds for the degrees of symmetric OR representations. Theorem 17 connects such representations to uniform-layer Ramsey certificates. His discussion after the proof of Theorem 4 includes a sharp product bound for the Frankl–Wilson case. These are essential antecedents to a limitation theorem for this method. Our optimization fixes the two binomial certificates in Definition ?? and tracks their leading constant and near-equality parameters. It is not a replacement for Gopalan’s broader representation results. His Section 6 also distinguishes limitations of the estimates from upper bounds on the graphs themselves.

The next proposition shows that the coefficient $1/4$ is not an artifact of choosing the top uniformity $pc - 1$ in the interval with blue degree $c - 1$.

Proposition 10.16 (Allowing every diagonal residue). *The leading coefficient remains $1/4$ if one allows any uniformity $r \geq p$ and colors blue when $|A \cap B| \equiv r \pmod{p}$, with p prime. In this extension set $c = \lfloor r/p \rfloor + 1$, $d = \max\{p, c\}$, and use the degree costs $T_S = \sum_{j=0}^{d-1} \binom{m}{j}$ and $T_D = \binom{m}{d-1}$. The upper estimate again holds for formal costs with every integer $p \geq 2$. Uniformities $r < p$ only give complete red graphs and certified vertex counts below k .*

Proof. For a prime modulus, the red family permits $p - 1$ residues and the blue family permits $c - 1$ exact values. These are precisely their polynomial degrees. The larger uniform bound is $\binom{m}{d-1}$: if $i = \min\{p, c\} - 1$ and $j = d - 1$, then $i \leq j$ and $i + j = p + c - 2 \leq p(c - 1) \leq r \leq m$, so symmetry and unimodality give $\binom{m}{i} \leq \binom{m}{j}$.

For the upper estimate put $u = \min\{p, c\}$ and $s = d - 1$. Now $p(c - 1) \leq r \leq pc - 1$, rather than $r = pc - 1$. If $s > m/2$, then $r > s$ and $m - r < m - s < m/2$, whence $N = \binom{m}{m-r} \leq \binom{m}{m-s} = T_D < k$. We may therefore assume $s \leq m/2$. The certificate budget yields $s \log(m/s) < L$ and $d \leq L/\log 2 + 1$. Moreover

$$d(u - 1) \leq r \leq du - 1, \quad u - 1 \leq r/s \leq u + 1.$$

As before, $\log N < (r/s)L - r(\log(r/s) - 1)$. If $u \leq L/\ell^2$, dropping $-r \log(r/s) \leq 0$ gives $\log N = O(L^2/\ell^2)$. Otherwise $\log(u - 1) = \ell + O(\log \ell)$ uniformly and, for large k ,

$$\log N < (u + 1)L - d(u - 1)(\log(u - 1) - 1).$$

Set $v = u - 1$ and $A_L = \ell - 2 \log \ell - 2 > 0$. Since $d \geq v$, the right side is at most $vL - A_L v^2 + 2L \leq L^2/(4A_L) + 2L$. This proves the required upper coefficient. The original balanced construction belongs to the extended class and supplies the lower bound. The argument uses only integrality for its upper estimate. $\square$

10.7. Beyond These Intersection Certificates. A recent algebraic comparison is especially relevant to the scope of Theorem ?. Ihringer and Mattheus [?], Theorem 1.3,

give an explicit finite-geometric construction with diagonal vertex count at least

$$\exp\left((1 - o(1)) \frac{(\log k)^2}{\log \log k}\right)$$

and no homogeneous k -set. Their August 2026 preprint replaces the coefficient $1/4$ by 1 using projective points and a trace adjacency rule. This is outside the class in Definition ?? . It illustrates why the certificate optimum cannot be described as a limit on algebraic constructions.

The stronger extractor-based results use a different language, but the obstruction can be stated in elementary terms. Let $F: [N] \times [N] \rightarrow \{0, 1\}$ take both values on every product $A \times B$ with $|A|, |B| \geq K$, and color the edge $\{x, y\}$ with $x < y$ by $F(x, y)$. If a homogeneous set had $2K$ vertices, split it into its K smallest and K largest labels. Every pair across the two parts is evaluated in the same order, so F would be constant on their product, a contradiction. Ordering the arguments this way avoids assuming that F is symmetric, and the factor two does not affect the scales below.

A two-source disperser formalizes such nonconstancy for independent weak random sources. Uniform distributions on large sets give the product-set formulation above. A two-source extractor asks for much more: the output distribution must be close to uniform, and in particular a one-bit extractor with error below $1/2$ cannot be constant on such a product. Lower source-entropy requirements therefore give smaller guaranteed homogeneous-set thresholds.

Barak, Rao, Shaltiel, and Wigderson [?] constructed explicit Ramsey graphs on N vertices with no homogeneous set of size $2^{(\log N)^{o(1)}}$. Chattopadhyay and Zuckerman [?] reached the threshold $2^{(\log \log N)^{O(1)}}$ using two-source extractors. Li [?], Corollaries 1.9 and 7.7, gives, for an absolute constant $C > 1$, strongly explicit graphs with no homogeneous set of size $(\log N)^C$. Constants and rounding are absorbed in these asymptotic descriptions.

The last statement implies a constructive lower bound of the form

$$R(k) \geq \exp(ck^{1/C}) \tag{10.18}$$

for some $c > 0$ and all sufficiently large k : take $N = \lfloor \exp(c_0 k^{1/C}) \rfloor$ with c_0 small enough that the homogeneous-set threshold stays below k . This is substantially larger than the intersection scale, although still subexponential in k .

An explicit family with no homogeneous set larger than $A \log N$, for a fixed constant A , would give a constructive exponential lower bound: take $N = \lfloor \exp(k/(2A)) \rfloor$. The gap between a polylogarithmic threshold and a logarithmic one is exactly what remains. Huang, Li, and Zhong [?], full version, Appendix D, recast that step through range avoidance, where one seeks an output outside the image of a circuit with fewer input bits than output bits. This gives another computational formulation of the obstruction, not a further numerical improvement.

10.8. A Comparison with General Diagonal Bounds. The distinction between explicit construction and unrestricted existence survives all of the recent advances. Table ?? collects the scales. Each entry is the size of a coloring with no homogeneous k -set, so a larger entry is a stronger bound.

Method	Size of a coloring with no homogeneous k -set	Guarantee
Triples	$\binom{k-1}{3}$	Strongly explicit
Fixed prime p	$((p-1)!)^{p+1}/(p^2-1)! + o(1))k^{p+1}$	Strongly explicit
Growing prime	$\exp((1+o(1))(\log k)^2/(4 \log \log k))$	Strongly explicit
Ihringer–Mattheus [?]	$\exp((1-o(1))(\log k)^2/\log \log k)$	Explicit (as stated in [?])
Li [?]	$\exp(ck^{1/C})$ for some $c > 0$, $C > 1$	Strongly explicit
First moment	$\lfloor ck2^{k/2} \rfloor$, fixed $c < 1/(e\sqrt{2})$	Existence

TABLE 4. Constructive and probabilistic scales. Fixed-prime asymptotics keep p constant. In the Li row the constants are small enough to absorb rounding and the threshold convention. This is a comparison of guarantees, not a list of exact Ramsey numbers.

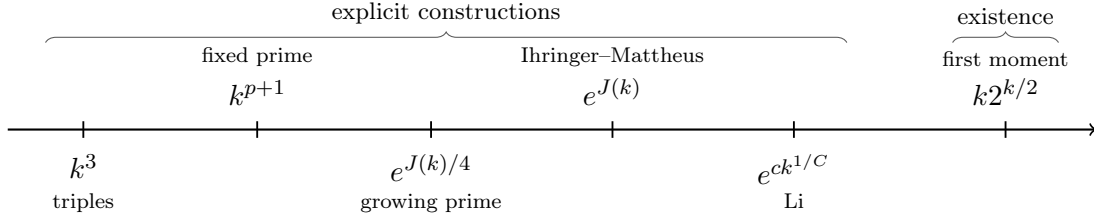


FIGURE 6. Increasing growth scales, with $J(k) = (\log k)^2/\log \log k$ and lower-order terms suppressed. The first three constructions are proved here. The next two are quoted from Ihringer–Mattheus and Li. The last is an existence bound. The two middle algebraic marks display the distinction between the coefficient $1/4$ for the optimized intersection certificates and the coefficient 1 achieved by a different algebraic family.

For general diagonal lower bounds, Spencer [?] improved the first-moment constant by a factor of two:

$$R(k) \geq \left(\frac{\sqrt{2}}{e} + o(1) \right) k2^{k/2}. \quad (10.19)$$

No improvement to the exponential base $\sqrt{2}$ is known in the diagonal case. See Wigderson’s survey [?]. On the upper side, Campos, Griffiths, Morris, and Sahasrabudhe [?] proved $R(k) \leq (4 - \delta)^k$ for some fixed $\delta > 0$ and all sufficiently large k , and Gupta, Ndiaye, Norin, and Wei [?] give the more explicit bound

$$R(k) \leq (4e^{-0.14/e})^{k+o(k)} = (3.799202\dots)^{k+o(k)}. \quad (10.20)$$

These general upper bounds constrain every coloring, explicit or not. Appendix ?? records recent lower bounds when the two forbidden clique sizes differ.

CONCLUSION

The Euclidean and Ramsey applications use the same basic comparison: a large uniform layer supplies the vertices, while an intersection theorem bounds a color class or homogeneous family. In the Euclidean binary construction, entropy optimization gives the densities $q/m \rightarrow a_*$ and $r/m \rightarrow 2a_*$. In the Ramsey certificate family, the corresponding optimization gives asymptotically equal degree bounds and a ground-set exponent 3.

The two stability estimates have different ranges of usefulness. The Euclidean estimate gives effective finite control on the density error. The Ramsey estimate is principally asymptotic. For the Euclidean construction, prime gaps determine the loss from replacing the optimal real density by an available prime and therefore control the finite comparison with prime powers, including the explicit remainder in Corollary ?. Proposition ? shows that the Ramsey leading coefficient persists under every diagonal residue and uniformity. The questions in Appendix ? concern improvements to the family bounds and changes to the underlying constructions.

APPENDIX A. UNIFORM REFINEMENTS OF THE INTERSECTION BOUND

The elementary constructions in Chapters 8 and 10 use Lemma ?, whose bound is a sum $\sum_{j \leq s} \binom{m}{j}$. For a *uniform* family that sum can be replaced by the single coefficient $\binom{m}{s}$, which improves the finite numbers by at most a factor of $s+1$ when $s \leq m/2$, as in the applications here, and then changes logarithms by only $O(\log m)$. The improvement does use one thing the text avoids: the rank of a matrix over $\mathbb{Q}$. The same device extends the method from primes to prime powers, and Section ? shows what that is worth.

A.1. A Common Rank Argument. For uniform families, a monomial of degree $j \leq s$ can be rewritten using monomials of degree exactly s , by summing over the extensions inside a member of the family, as recorded in the next lemma.

Lemma A.1 (Uniform polynomial rank bound). *Let $\mathcal{F} = \{A_1, \dots, A_b\}$ be an r -uniform family on $[m]$, where $0 \leq r \leq m$, and let $f \in \mathbb{Q}[t]$ have degree at most s , where $0 \leq s \leq r$. Then $M = (f(|A_i \cap A_j|))_{i,j=1}^b$ satisfies $\text{rank}_{\mathbb{Q}} M \leq \binom{m}{s}$.*

Proof. For fixed i , multilinearize $f(\sum_{a \in A_i} x_a)$ on incidence vectors. The result has degree at most s . Write $x_S = \prod_{a \in S} x_a$. On the incidence vector u_B of any r -set B and for $|S| = j \leq s$,

$$\sum_{\substack{T \supseteq S \\ |T|=s}} x_T(u_B) = \binom{r-j}{s-j} x_S(u_B). \quad (\text{A.1})$$

If $S \not\subseteq B$ both sides vanish. If $S \subseteq B$ the left side counts the s -subsets of B containing S . The binomial coefficient is nonzero in $\mathbb{Q}$, so (A.1) can be solved for $x_S(u_B)$. Every row of M is therefore a linear combination of the $\binom{m}{s}$ vectors $(x_T(u_{A_j}))_{j=1}^b$ with $|T| = s$. $\square$

The restriction to $\mathbb{Q}$ matters: $\binom{r-j}{s-j}$ can vanish in positive characteristic. The next corollary reaches a modular conclusion without ever dividing by that coefficient modulo p .

Corollary A.2 (Modular nonsingularity). *Under the hypotheses of Lemma ??, suppose also that $f(0), \dots, f(r)$ are integers. If p is prime and*

$$f(r) \not\equiv 0 \pmod{p}, \quad f(|A_i \cap A_j|) \equiv 0 \pmod{p} \quad (i \neq j),$$

then $b \leq \binom{m}{s}$.

Proof. The integer matrix M reduces modulo p to a nonzero scalar multiple of the identity, so $\det M \not\equiv 0 \pmod{p}$ and hence $\det M$ is a nonzero integer. Thus $\text{rank}_{\mathbb{Q}} M = b$, and Lemma ?? applies. $\square$

The rational coefficients of f need not reduce modulo p . It is the integer *values*, and the resulting integer matrix, that are reduced. This distinction is what makes prime powers possible.

Theorem A.3 (Uniform prime intersection theorem). *Let p be prime, let L be a set of s distinct residues modulo p , and let $\mathcal{F}$ be an r -uniform family on $[m]$ with $0 \leq s \leq r \leq m$. If $r \bmod p \notin L$ and*

$$|A \cap B| \bmod p \in L \quad (A, B \in \mathcal{F}, A \neq B),$$

then $|\mathcal{F}| \leq \binom{m}{s}$.

Proof. Choose integer representatives of L and put $f(t) = \prod_{\ell \in L} (t - \ell)$. Every off-diagonal value is divisible by p and $f(r)$ is not, so Corollary ?? applies with degree s . $\square$

With exact intersection values in place of residues, the same rank bound is the theorem of Ray-Chaudhuri and Wilson [?]: an r -uniform family whose pairwise intersections take at most s distinct values has at most $\binom{m}{s}$ members. Theorem ?? is the modular form, due to Frankl and Wilson [?].

Example A.4. If $p = 3$, $r \equiv 2 \pmod{3}$, and every off-diagonal intersection is congruent to 0 or 1 modulo 3, then $L = \{0, 1\}$ gives $|\mathcal{F}| \leq \binom{m}{2}$. The degree is the number of permitted off-diagonal residues, not the uniformity.

Note A.5. Theorem ?? applies verbatim to the families of Chapters 8 and 10, since all of them are uniform. It replaces the denominator of (??) by $\binom{m}{p-1}$, which is the right-hand pair of columns in Table ??, and it replaces $S(m, p)$ by $D(m, p) = \binom{m}{p-1}$ in Theorem ??, so that (??) becomes $R(D(m, p) + 1) > \binom{m}{p^2-1}$. The blue Ramsey family needs Lemma ?? directly rather than Theorem ??: there $f(t) = \prod_{j=1}^{p-1} (t - (jp - 1))$ makes M diagonal over $\mathbb{Q}$ with nonzero diagonal entry $f(r)$, so $\text{rank}_{\mathbb{Q}} M = b$, and the lemma with $s = p - 1$ gives $b \leq \binom{m}{p-1}$.

A.2. Prime Powers. For a proper prime power $q = p^h$ with $h \geq 2$, the forbidden condition is a congruence modulo q , and $\mathbb{Z}/q\mathbb{Z}$ is not a field, so Lemma ?? cannot simply be applied over it. The substitute is an integer-valued polynomial whose values detect the residue $q - 1$ modulo q after reduction modulo p .

Lemma A.6 (Prime-power residue detector). *If $q = p^h$ with p prime and $h \geq 1$, then for every integer $N \geq 0$,*

$$\binom{N}{q-1} \equiv \begin{cases} 1, & N \equiv q-1 \pmod{q}, \\ 0, & \text{otherwise} \end{cases} \pmod{p}.$$

Proof. Write $N = dq + u$ with $0 \leq u < q$. Repeated use of $(1+z)^p \equiv 1+z^p \pmod{p}$ gives

$$(1+z)^N \equiv (1+z^q)^d (1+z)^u \pmod{p}.$$

To contribute to the coefficient of z^{q-1} the first factor must supply its constant term, and the remaining coefficient is 1 if $u = q-1$ and 0 otherwise. $\square$

Prime powers also admit a proof by linear independence: instead of reducing the polynomial modulo p , which is impossible because its denominator $(q-1)!$ is divisible by p when $h \geq 2$, we clear denominators in the linear relation and reduce the resulting integers. The family need not even be uniform.

Theorem A.7 (Prime powers without ranks). *Let $q = p^h$ be a prime power and let r be an integer with $q-1 \leq r \leq m$. Let $\mathcal{F}$ be a family of subsets of $[m]$ such that*

$$|A| \equiv r \pmod{q} \quad (A \in \mathcal{F}), \quad |A \cap B| \not\equiv r \pmod{q} \quad (A, B \in \mathcal{F}, A \neq B).$$

Then $|\mathcal{F}| \leq \sum_{j=0}^{q-1} \binom{m}{j}$.

Proof. Choose $c \in \{0, \dots, q-1\}$ with $r+c \equiv q-1 \pmod{q}$ and set

$$f(t) = \binom{t+c}{q-1} = \frac{(t+c)(t+c-1) \cdots (t+c-q+2)}{(q-1)!},$$

a polynomial of degree $q-1$ over $\mathbb{Q}$ that takes integer values at all nonnegative integers. By Lemma ??, for an integer $N \geq 0$ we have $f(N) \equiv 1 \pmod{p}$ when $N \equiv r \pmod{q}$ and $f(N) \equiv 0 \pmod{p}$ otherwise.

For $A \in \mathcal{F}$ let Q_A be the multilinearization of $f(\sum_{i \in A} x_i)$ on $\{0,1\}^m$. It has rational coefficients and degree at most $q-1$, and $Q_A(u_B) = f(|A \cap B|)$. By the hypotheses and the previous paragraph,

$$Q_A(u_B) \equiv \begin{cases} 1 \pmod{p}, & A = B, \\ 0 \pmod{p}, & A \neq B. \end{cases}$$

Suppose $\sum_A c_A Q_A = 0$ as a function on $\{0,1\}^m$, with rational c_A not all zero. Multiply through by a common denominator and divide by the greatest common divisor, so that the c_A are integers not all divisible by p . Evaluating at u_B gives the integer relation $\sum_A c_A f(|A \cap B|) = 0$, and reducing it modulo p kills every term with $A \neq B$ and leaves $c_B \equiv 0 \pmod{p}$. Since B was arbitrary, p divides every c_A , a contradiction. So the Q_A are linearly independent. They lie in the span of the squarefree monomials of degree at most $q-1$, of which there are $\sum_{j \leq q-1} \binom{m}{j}$. $\square$

Theorem A.8 (Uniform prime-power theorem). *Let $q = p^h$ be a prime power with $q-1 \leq r \leq m$, and let $\mathcal{F}$ be an r -uniform family on $[m]$ with $|A \cap B| \not\equiv r \pmod{q}$ for all distinct $A, B \in \mathcal{F}$. Then $|\mathcal{F}| \leq \binom{m}{q-1}$.*

Proof. Take f as in the proof of Theorem ?? . It has degree $q - 1 \leq r$ and integer values, with $f(r) \equiv 1$ and $f(|A \cap B|) \equiv 0$ modulo p for distinct members. Apply Corollary ?? with $s = q - 1$. $\square$

The prime-power theorem and its integer-valued-polynomial method are due to Frankl and Wilson [?]. The polynomial is evaluated over $\mathbb{Q}$ first. Its factorial denominator is never inverted modulo p .

Corollary A.9. *For every prime power q with $2q - 1 \leq m$,*

$$\chi(\mathbf{E}^{m-1}) \geq \left\lceil \frac{\binom{m}{2q-1}}{\binom{m}{q-1}} \right\rceil, \quad \text{and} \quad \chi(\mathbf{E}^{m-1}) \geq \left\lceil \frac{\binom{m}{2q-1}}{\sum_{j=0}^{q-1} \binom{m}{j}} \right\rceil$$

where the second inequality has a proof without a rank argument.

Proof. Embed the $(2q - 1)$ -subsets of $[m]$ as $\mathbf{1}_A / \sqrt{2q}$. By Lemma ?? , unit distance corresponds to intersection $q - 1$, which is the only integer in $[0, 2q - 2]$ congruent to $2q - 1$ modulo q . A color class therefore satisfies the hypotheses of Theorem ?? and of Theorem ?? with $r = 2q - 1$. Divide the vertex count by each bound. $\square$

A.3. Primes versus Prime Powers. Prime powers can improve finite bounds while leaving the optimized asymptotic rate unchanged.

Asymptotics. Suppose $q = q(m)$ ranges over prime powers with $q/m \rightarrow a \in (0, 1/2)$. By (??), the logarithm of the ratio in Corollary ?? is $m(H(2a) - H(a)) + o(m)$, exactly as in the proof of Theorem ?? . The denominator $\binom{m}{q-1}$ and the sum $\sum_{j < q} \binom{m}{j}$ differ by at most a factor of m , which is $o(m)$ after taking logarithms. So every prime-power choice is governed by the same function f , whose maximum is $\log \beta$. Since the prime number theorem already supplies primes with $p = a_* m + o(m)$, the optimum is attained along primes. Prime powers cannot improve the exponential base, and neither can any other choice of q in this family.

Finite values. For a fixed m , the eligible prime powers form a strictly larger set than the eligible primes, so maximizing over them can only help, and it sometimes helps. Table ?? shows this for the dimensions of Table ?? : at $n = 50$ the prime power 8 beats every prime, and at $n = 100$ the prime power 16 beats the best prime 17 by about 17.5 percent. Over the whole range $4 \leq m \leq 400$, some prime power strictly beats every eligible prime for 105 of the 397 values of m , with a largest gain of about a factor of 1.43. This computation gives no uniform multiplicative bound as m grows. Proposition ?? below gives a quantitative upper bound in terms of prime gaps.

Corollary A.10 (Prime Powers in the Ramsey Certificates). *Theorems ?? and ?? also hold when the modulus p in Definition ?? is allowed to be any prime power.*

Proof. For modulus q and uniformity $qc - 1$, the red bound follows from Theorem ?? or Theorem ?? . The blue family still has the $c - 1$ exact intersection values $jq - 1$ for $1 \leq j < c$, so its rational-polynomial bound is unchanged. The optimization upper bound and stability proof use only that the modulus is an integer at least two. The matching lower bound already uses primes. $\square$

Dimension n	Best prime		Best prime power	
	p	guaranteed colors	q	guaranteed colors
10	2	15	2	15
20	3	97	3	97
50	7	26,445	8	27,542
100	17	273,702,586	16	321,643,039
200	29	50,053,437,472,123,893	29	50,053,437,472,123,893

TABLE 5. The effect of prime powers on Corollary ??, with $m = n + 1$ and the uniform denominator $\binom{m}{q-1}$. Computed with exact integer arithmetic by maximizing the unrounded ratio over all eligible parameters and rounding up.

A.4. Prime Gaps and the Finite Gain. The optimal density need not land on a prime. Its distance to the nearest prime controls the loss, because the entropy objective has a nondegenerate maximum. To compare multiplicative gains tending to one, we need a more accurate remainder than the $O(\log m)$ entropy estimate.

Proposition A.11 (Prime-gap control of the uniform quotient). *Put $a_* = (2 - \sqrt{2})/4$, $\beta = (1 + \sqrt{2})/2$, and*

$$R_m(t) = \frac{\binom{m}{2t-1}}{\binom{m}{t-1}}, \quad D_m = \min_{p \text{ prime}} |p - a_* m|, \quad g_* = \frac{1}{2} \log 2 + \frac{3}{2} \log \beta.$$

For $m \geq 3$ define

$$G(m) = \frac{\max_{q \text{ prime power}, 2q-1 \leq m} R_m(q)}{\max_{p \text{ prime}, 2p-1 \leq m} R_m(p)}.$$

Here prime powers include primes. For all sufficiently large m , with absolute implied constants,

$$\log \max_{p \text{ prime}, 2p-1 \leq m} R_m(p) = m \log \beta + g_* + O\left(\frac{1 + D_m^2}{m}\right), \quad (\text{A.2})$$

$$0 \leq \log G(m) \leq C \frac{1 + D_m^2}{m}, \quad (\text{A.3})$$

where C is an absolute constant. In particular, the classical Baker–Harman–Pintz estimate gives $\log G(m) = O(m^{0.05})$. Under the Riemann hypothesis it gives $\log G(m) = O(\log^2 m)$. Under the Cramér gap hypothesis $p_{j+1} - p_j = O(\log^2 p_j)$, it gives

$$\log G(m) = O(\log^4 m/m), \quad G(m) \rightarrow 1.$$

These are consequences of the stated prime-gap inputs. No optimality of the unconditional exponent is asserted.

Proof. Write $f(a) = H(2a) - H(a)$. Uniformly when $a = t/m$ lies in a compact subinterval of $(0, 1/2)$, Stirling’s formula and the identities

$$\binom{m}{2t-1} = \binom{m}{2t} \frac{2t}{m-2t+1}, \quad \binom{m}{t-1} = \binom{m}{t} \frac{t}{m-t+1}$$

give

$$\log R_m(t) = mf(a) + g(a) + O(m^{-1}), \quad g(a) = \frac{1}{2} \log 2 + \frac{3}{2} \log \frac{1-a}{1-2a}. \quad (\text{A.4})$$

Here $f(a_*) = \log \beta$, $g(a_*) = g_*$, and

$$f(a) = \log \beta - 4\sqrt{2}(a - a_*)^2 + O(|a - a_*|^3).$$

In particular the Taylor coefficient is $4\sqrt{2}$. The coefficient 4 in Corollary ?? is a uniform curvature bound, not this local coefficient. The local refinement of Corollary ?? approaches $4\sqrt{2}$ as the deficit tends to zero.

For $2t \leq m$, the uniform entropy estimate gives $\log R_m(t) = mf(t/m) + O(\log m)$. The only remaining endpoint, $2t = m + 1$, has $R_m(t) \leq 1$ and cannot maximize the quotient for large m . Since f has its unique maximum at a_* , and an integer within one of a_*m attains $m \log \beta + O(1)$, all maximizing integers lie in a fixed compact neighborhood of a_* for large m . On that neighborhood,

$$f(a) \leq \log \beta - c(a - a_*)^2, \quad g(a) \leq g_* + C_1|a - a_*|$$

for positive absolute constants c, C_1 . Completing the square in $-cm(a - a_*)^2 + C_1|a - a_*|$ therefore proves

$$\max_{2 \leq t \leq (m+1)/2} \log R_m(t) \leq m \log \beta + g_* + O(m^{-1}). \quad (\text{A.5})$$

The prime number theorem gives $D_m = o(m)$, so a nearest prime is eligible and lies in the same neighborhood for large m . Substitution in (??), using $D_m \leq 1 + D_m^2$, gives

$$\log R_m(p) \geq m \log \beta + g_* - C_2(1 + D_m^2)/m.$$

Together with (??), this proves both estimates, since prime powers lie between primes and all integers.

Baker, Harman, and Pintz [?] give $D_m = O(m^{0.525})$. Under RH, $D_m = O(\sqrt{m} \log m)$. See Dudek [?]. The stated Cramér hypothesis gives $D_m = O(\log^2 m)$. Substitution into (??) proves the three consequences. $\square$

Corollary A.12 (A remainder for the binary construction). *For some absolute $C > 0$ and all sufficiently large n ,*

$$\chi(\mathbf{E}^n) \geq \beta^n \exp(-Cn^{0.05}).$$

Under the Cramér gap hypothesis, the uniform certificate satisfies

$$\max_{p \text{ prime}, 2p-1 \leq n+1} R_{n+1}(p) = (\sqrt{2} \beta^{5/2} + o(1)) \beta^n.$$

Consequently, under the same hypothesis,

$$\chi(\mathbf{E}^n) \geq (\sqrt{2} \beta^{5/2} + o(1)) \beta^n.$$

Proof. Apply (??) with $m = n + 1$ and use the uniform chromatic certificate. Under the gap hypothesis, $(1 + D_m^2)/m = o(1)$ and $e^{g_*} \beta = \sqrt{2} \beta^{5/2}$. $\square$

This refines the error for this binary construction. It does not improve the larger known exponential base in (??). The unconditional estimate above does not establish a polynomial loss relative to β^n . It also does not prove that such a loss is impossible without a stronger prime-gap hypothesis.

APPENDIX B. FURTHER BOUNDS OFF THE DIAGONAL

This optional appendix surveys general lower bounds beyond the constructive diagonal bounds developed in Chapter ???. These are results of the named authors, not further outputs of the intersection construction.

Nonintegral clique sizes in $R(\ell, C\ell)$ are rounded up, and $C > 1$ is fixed unless a separate limit is stated.

For every fixed $C > 1$, Ma, Shen, and Xie [?] proved that there is an $\varepsilon = \varepsilon(C) > 0$ such that, for all sufficiently large ℓ ,

$$R(\ell, C\ell) \geq (p_C^{-1/2} + \varepsilon)^\ell, \quad C = \frac{\log p_C}{\log(1 - p_C)}, \quad 0 < p_C < \frac{1}{2}. \quad (\text{B.1})$$

There is exactly one such p_C , since the displayed ratio decreases continuously from infinity to one as p runs from zero to $1/2$. This was the first exponential improvement over the corresponding Erdős lower bound. Hunter, Milojević, and Sudakov [?] gave a simpler proof using Gaussian random graphs and improved the quantitative bounds. Lin and Niu [?], Theorem 1.1, sharpened that analysis further. In the separate limit $C \rightarrow \infty$ their gain in the exponential base over the Hunter-Milojević-Sudakov bound is of order $p_C^{-1/2} / \log C$.

Bradač [?], Theorem 1.4, proves that for every fixed $C > 1$ and all sufficiently large ℓ ,

$$R(\ell, C\ell) \geq (2^{1-1/(2C)})^\ell, \quad (\text{B.2})$$

which improves the preceding bounds when C is close enough to one. The threshold for “sufficiently large” may depend on C , so these fixed-ratio statements cannot be specialized to the diagonal by setting $C = 1$.

Farther from the diagonal, Bradač [?], Theorem 1.3, proves that for every $\delta > 0$ there is an L with

$$R(\ell, t) \geq (t/\ell)^{(1-\delta)\ell} \quad (\ell \geq L, t \geq L\ell). \quad (\text{B.3})$$

Together with Theorem ?? this identifies the leading logarithmic scale when $\ell \rightarrow \infty$ and $t/\ell \rightarrow \infty$:

$$\log R(\ell, t) = (1 + o(1)) \ell \log(t/\ell),$$

since the binomial upper estimate gives $\log R(\ell, t) \leq (\ell - 1) \log(e(t + \ell - 2)/(\ell - 1)) = (1 + o(1)) \ell \log(t/\ell)$, while (??) supplies the matching lower ratio for each fixed $\delta > 0$. These off-diagonal improvements leave the exponential base in the diagonal lower bound (??) unchanged.

APPENDIX C. HISTORICAL NOTES AND FURTHER READING

The constructions and intersection theorems used in the main text are classical. This appendix records their sources and selected references. It is not needed for any proof above.

Oddtown. Berlekamp [?] proved the parity statement of Theorem ?? in 1969, in the language of set systems with even intersections. The incidence-vector presentation over the field with two elements is developed in Babai and Frankl [?], a standard reference for the linear-algebra method as a whole. Oddtown already contains the two ingredients used later: a field in which the diagonal and off-diagonal products differ, and a dimension bound from linear independence.

Fisher’s inequality. Fisher [?] proved in 1940 that a balanced incomplete block design has at least as many blocks as points. The set-system form used in Theorem ??, that a uniform family with all pairwise intersections equal has at most m members, is proved by the quadratic-form argument of Bose [?]. It is degree one over the reals, exactly as Oddtown is degree one over the field with two elements, and that is why the cubic Ramsey coloring of Section ?? needs two tools rather than one: parity controls the red color and an exact intersection size controls the blue.

Ray-Chaudhuri-Wilson, Frankl-Wilson, and the polynomial method. Ray-Chaudhuri and Wilson [?] proved in 1975 that an r -uniform family on $[m]$ whose pairwise intersections take at most s distinct values has at most $\binom{m}{s}$ members. Frankl and Wilson [?] replaced exact values by residues modulo a prime in 1981, added the prime-power case of Appendix ??, and drew both geometric consequences developed here: the exponential lower bound for $\chi(\mathbb{E}^n)$ and the explicit Ramsey graphs. The multilinear-polynomial proof we give for Lemma ??, where positive powers are replaced by their variables and squarefree monomials are counted, is the argument of Alon, Babai, and Suzuki [?], who used it to simplify and extend these theorems. That paper provides a convenient entry point to the later literature.

The chromatic number of Euclidean space. The planar problem is due to Hadwiger and Nelson. De Grey [?] raised its lower bound to five in 2018. In general dimension, the upper bound $(3 + o(1))^n$ is due to Larman and Rogers [?], with a later proof by Prosanov [?]. The exponential lower bound with base $(1 + \sqrt{2})/2$ is the Frankl-Wilson application proved in Section ?? . Raigorodskii [?] improved the base to $1.239\dots$ in 2000 using vectors with entries in $\{-1, 0, 1\}$, and the survey of Raigorodskii and Sineľnikov-Murylev [?] covers the intervening work. For small dimensions the best upper bounds come from lattice colorings, and the chronology is worth separating. Coulson [?] and, independently, Radoićić and Tóth [?] proved $\chi(\mathbb{E}^3) \leq 15$ in 2002 and 2003, the first by a sublattice scheme and the second by a linear one. Radoićić and Tóth also stated $\chi(\mathbb{E}^4) \leq 54$ without proof, and Coulson and Payne later stated the better bound $\chi(\mathbb{E}^4) \leq 49$, also without proof. Arman, Bondarenko, Prymak, and Radchenko [?] proved the 49 bound in 2024, using the D_4 lattice as an Eisenstein lattice, and verified optimality for sublattices of D_4 when the excluded distance is twice its covering radius. The same paper gives $\chi(\mathbb{E}^5) \leq 140$, the $7^{n/2}$ bounds in dimensions 2, 4, 6, 8, 24, and $\chi(\mathbb{E}^n) \leq 3^n$ for $n \leq 38$ and $n = 48, 49$.

Diagonal Ramsey numbers. The upper bound of Theorem ?? is from the 1935 paper of Erdős and Szekeres [?]. The lower bound of Theorem ?? is Erdős’s 1947 paper [?], one of the first uses of the probabilistic method. Spencer [?] improved its constant by a factor of two using the Lovász local lemma. The exponential base $\sqrt{2}$ has not moved since. On the upper side, Campos, Griffiths, Morris, and Sahasrabudhe [?] broke the base 4

in a result announced in 2023 and published in 2026, with the constant subsequently optimized by Gupta, Ndiaye, Norin, and Wei [?]. Wigderson’s Bourbaki survey [?] explains the proof.

Explicit Ramsey graphs. The Frankl–Wilson construction of Section ?? was a long-standing benchmark. Barak, Rao, Shaltiel, and Wigderson [?] surpassed its asymptotic scale with two-source dispersers, Chattopadhyay and Zuckerman [?] with two-source extractors, and Li [?] reached the polylogarithmic threshold. Huang, Li, and Zhong [?] discuss the remaining step in the language of range avoidance.

A companion in the measurable setting. The colorings in these chapters are arbitrary. Our finite configurations impose no measurability assumption. For the measurable side of Euclidean Ramsey problems, where spatial averaging, Fourier analysis, and linear programming become available and the answers can be stronger, see the companion paper of Hoff, Hu, and Liu [?].

APPENDIX D. QUESTIONS SUGGESTED BY THE CONSTRUCTIONS

The first four questions concern possible extensions of the analysis. No claim is made that their formulations are new. The final question records the established gap in explicit Ramsey constructions. The certificate bounds above describe the limitations of parameter changes within the families studied here.

Question 1 (Upper bounds from lattices). Theorem ?? gives $\chi(\mathbb{E}^n) \leq (\lceil \sqrt{n} \rceil + 1)^n$, whose logarithm is of order $n \log n$, while the truth is exponential. Lattice-sublattice colorings do much better in every dimension where they have been computed, giving $\chi(\mathbb{E}^n) \leq 3^n$ for $n \leq 38$ and for $n = 48, 49$ [?], and Larman and Rogers [?] give $(3 + o(1))^n$ in general. On the other side, no such scheme uses fewer than $2^{n+1} - 1$ colors (Coulson [?], Theorem 4.5). Is there a fixed $c < 3$ such that, for every sufficiently large n , a lattice-sublattice coloring uses at most c^n colors? How much of the interval $[2, 3]$ is achievable by this family? This is related to the questions in Section 5 of [?], which ask for a sublattice coloring below 3^n in every dimension and for the dimensions in which a lattice of covering-packing ratio at most two exists.

Question 2 (Finite Gains from Prime Powers). For $m \geq 3$ define the unrounded uniform ratio

$$G(m) = \frac{\max_{q \text{ a prime power}, 2q-1 \leq m} \binom{m}{2q-1} / \binom{m}{q-1}}{\max_{p \text{ prime}, 2p-1 \leq m} \binom{m}{2p-1} / \binom{m}{p-1}}.$$

Proposition ?? gives $\log G(m) = O(m^{0.05})$ unconditionally and $G(m) \rightarrow 1$ under the stated Cramér gap hypothesis. Can one prove $G(m) = O(1)$, or even $G(m) \rightarrow 1$, unconditionally? The finite search through $m = 400$ in Table ?? does not settle this question. The ratio here uses the uniform denominator in both maxima, so that changing the modulus is the only difference.

Question 3 (Improving the Graph Analysis). Can one improve the exponential lower bound obtained from a binary unit-distance layer by proving a stronger independent-set

bound than the certificate used in Theorem ??? In the notation of Keevash and Long [?], Theorem 1.1, the Frankl–Rödl theorem fixes $\alpha, \varepsilon \in (0, 1)$ with $\varepsilon \leq \alpha/2$, takes $r = \lfloor \alpha m \rfloor$, and assumes

$$\max\{0, 2r - m\} + \varepsilon m \leq t \leq r - \varepsilon m$$

for the forbidden intersection t . An independent family then has size at most $(1 - \delta)^m \binom{m}{r}$ for some $\delta = \delta(\alpha, \varepsilon) > 0$. At the binary optimum, $r/m \rightarrow 2a_*$ and $t/m \rightarrow a_*$, so the intersection lies strictly inside this permitted interval for a fixed small ε . The cited statement supplies a positive saving but does not specify a value that improves the optimized base here. Explicit general estimates are surveyed in Raigorodskii and Sinenikov-Murylev [?], Section 2.2.8, Theorem 8. Can a sharper quantitative analysis, or another method, beat the Frankl–Wilson rate on these layers? A matching limitation on chromatic number would require an upper-coloring argument. A second upper bound on independent-set size would not provide one.

Question 4 (Beyond the Specified Ramsey Certificates). For the edge rule on $(pc - 1)$ -subsets in Proposition ??, can a bound on the actual homogeneous families certify vertex counts with

$$\limsup_{k \rightarrow \infty} \frac{\log N(k) \log \log k}{(\log k)^2} > \frac{1}{4}?$$

The Ihringer–Mattheus construction in Section ?? demonstrates that the coefficient can already be larger in another algebraic family.

Question 5 (Explicit versus existential). Li [?] gives strongly explicit graphs on N vertices with no homogeneous set of size $(\log N)^C$ for an absolute constant $C > 1$, while an explicit family with threshold $A \log N$ would give a constructive exponential lower bound for $R(k)$ (Section ??). Can C be brought down to $1 + \varepsilon$ for every $\varepsilon > 0$? Can the threshold $A \log N$ be attained?

REFERENCES

- [1] Yusheng Li and Qizhong Lin, *Elementary Methods of Graph Ramsey Theory*, Applied Mathematical Sciences 211, Springer, 2022, Chapter 6, especially Section 6.2, pp. 131–138. <https://doi.org/10.1007/978-3-031-12762-5>.
- [2] Aubrey D. N. J. de Grey, “The chromatic number of the plane is at least 5,” *Geombinatorics* 28(1) (2018), 18–31. <https://arxiv.org/abs/1804.02385>.
- [3] Paul Erdős and George Szekeres, “A combinatorial problem in geometry,” *Compositio Mathematica* 2 (1935), 463–470. https://www.numdam.org/item/CM_1935__2__463_0/.
- [4] Paul Erdős, “Some remarks on the theory of graphs,” *Bulletin of the American Mathematical Society* 53 (1947), 292–294. <https://doi.org/10.1090/S0002-9904-1947-08785-1>.
- [5] Joel Spencer, “Ramsey’s theorem—a new lower bound,” *Journal of Combinatorial Theory, Series A* 18 (1975), 108–115. [https://doi.org/10.1016/0097-3165\(75\)90071-0](https://doi.org/10.1016/0097-3165(75)90071-0).
- [6] Yuval Wigderson, “Upper bounds on diagonal Ramsey numbers [after Campos, Griffiths, Morris, and Sahasrabudhe],” *Séminaire Bourbaki*, Exposé no. 1230, *Astérisque* 462, 85–138. <https://doi.org/10.24033/ast.1255>. Preprint arXiv:2411.09321. <https://arxiv.org/abs/2411.09321>.
- [7] Peter Frankl and Richard M. Wilson, “Intersection theorems with geometric consequences,” *Combinatorica* 1(4) (1981), 357–368. <https://doi.org/10.1007/BF02579457>.
- [8] Boaz Barak, Anup Rao, Ronen Shaltiel, and Avi Wigderson, “2-source dispersers for $n^{o(1)}$ entropy, and Ramsey graphs beating the Frankl–Wilson construction,” *Annals of Mathematics* 176(3) (2012), 1483–1543. <https://doi.org/10.4007/annals.2012.176.3.3>.

- [9] Eshan Chattopadhyay and David Zuckerman, “Explicit two-source extractors and resilient functions,” *Annals of Mathematics* 189(3) (2019), 653-705. Conference version, STOC 2016. <https://doi.org/10.4007/annals.2019.189.3.1>.
- [10] Xin Li, “Two Source Extractors for Asymptotically Optimal Entropy, and (Many) More,” in *Proceedings of the 64th IEEE Symposium on Foundations of Computer Science (FOCS)*, 2023, pp. 1271-1281. <https://doi.org/10.1109/FOCS57990.2023.00075>. Full version arXiv:2303.06802v2 (2023). <https://arxiv.org/abs/2303.06802v2>.
- [11] Jie Ma, Wujie Shen, and Shengjie Xie, “An exponential improvement for Ramsey lower bounds,” *Inventiones Mathematicae* 245(2) (2026), 1059–1115. <https://doi.org/10.1007/s00222-026-01421-9>. Preprint arXiv:2507.12926. <https://arxiv.org/abs/2507.12926>.
- [12] Zach Hunter, Aleksa Milojević, and Benny Sudakov, “Gaussian random graphs and Ramsey numbers,” arXiv:2512.17718 (2025). <https://arxiv.org/abs/2512.17718>.
- [13] Qizhong Lin and Lin Niu, “Sharper Ramsey lower bounds from refined Gaussian estimates,” arXiv:2605.25843v2 (2026), 2 July 2026. <https://arxiv.org/abs/2605.25843v2>.
- [14] Domagoj Bradač, “Off-diagonal Ramsey numbers,” arXiv:2605.28793 (2026), version 3, 16 June 2026. <https://arxiv.org/abs/2605.28793v3>.
- [15] Marcelo Campos, Simon Griffiths, Robert Morris, and Julian Sahasrabudhe, “An exponential improvement for diagonal Ramsey,” *Annals of Mathematics* 203(3) (2026), 869-932. <https://doi.org/10.4007/annals.2026.203.3.4>.
- [16] Parth Gupta, Ndiamé Ndiaye, Sergey Norin, and Louis Wei, “Optimizing the CGMS upper bound on Ramsey numbers,” arXiv:2407.19026 (2024), revised 29 August 2026, version 2. <https://arxiv.org/abs/2407.19026v2>.
- [17] Shengtang Huang, Xin Li, and Yan Zhong, “Range Avoidance and Remote Point: New Algorithms and Hardness,” in *17th Innovations in Theoretical Computer Science Conference (ITCS 2026)*, LIPIcs 362 (2026), 79:1-79:19. <https://doi.org/10.4230/LIPIcs.ITCS.2026.79>. Full version ECCC TR25-049, revision 5, 21 November 2025, Appendix D. <https://ecc.ecc.wi.zmann.ac.il/report/2025/049/>.
- [18] A. M. Raigorodskii, “On the chromatic number of a space,” *Russian Mathematical Surveys* 55(2) (2000), 351-352. Russian original *Uspekhi Mat. Nauk* 55(2) (2000), 147-148. DOI 10.1070/RM2000v055n02ABEH000281.
- [19] Roman Prosanov, “A new proof of the Larman-Rogers upper bound for the chromatic number of the Euclidean space,” *Discrete Applied Mathematics* 276 (2020), 115-120. <https://doi.org/10.1016/j.dam.2019.05.020>.
- [20] A. M. Raigorodskii and P. S. Sinelnikov-Murylev, “Johnson graphs, their random subgraphs, and some of their extremal characteristics,” *Russian Mathematical Surveys* 80(3) (2025), 471-530.
- [21] Leo Moser and William Moser, “Solution to problem 10,” *Canadian Mathematical Bulletin* 4 (1961), 187-189.
- [22] Elwyn R. Berlekamp, “On subsets with intersections of even cardinality,” *Canadian Mathematical Bulletin* 12(4) (1969), 471-474. <https://doi.org/10.4153/CMB-1969-059-3>.
- [23] D. G. Larman and C. A. Rogers, “The realization of distances within sets in Euclidean space,” *Mathematika* 19(1) (1972), 1-24. <https://doi.org/10.1112/S0025579300004903>.
- [24] Radoš Radoičić and Géza Tóth, “Note on the chromatic number of the space,” in *Discrete and Computational Geometry: The Goodman-Pollack Festschrift*, Algorithms and Combinatorics 25, Springer, 2003, pp. 695-698.
- [25] David Coulson, “A 15-colouring of 3-space omitting distance one,” *Discrete Mathematics* 256(1-2) (2002), 83-90.
- [26] Andrii Arman, Andriy Bondarenko, Andriy Prymak, and Danylo Radchenko, “Upper bounds on chromatic number of E^n in low dimensions,” *Electronic Journal of Combinatorics* 31(2) (2024), #P2.35. Preprint arXiv:2112.13438. <https://arxiv.org/abs/2112.13438>.

- [27] László Babai and Peter Frankl, *Linear Algebra Methods in Combinatorics*, Department of Computer Science, University of Chicago, preliminary version, 2022.
<https://people.cs.uchicago.edu/~laci/babai-frankl-book2022.pdf>.
- [28] R. A. Fisher, “An examination of the different possible solutions of a problem in incomplete blocks,” *Annals of Eugenics* 10 (1940), 52-75.
- [29] R. C. Bose, “A note on Fisher’s inequality for balanced incomplete block designs,” *Annals of Mathematical Statistics* 20 (1949), 619-620.
- [30] Dijen K. Ray-Chaudhuri and Richard M. Wilson, “On t -designs,” *Osaka Journal of Mathematics* 12(3) (1975), 737-744.
- [31] Noga Alon, László Babai, and Hiroshi Suzuki, “Multilinear polynomials and Frankl-Ray-Chaudhuri-Wilson type intersection theorems,” *Journal of Combinatorial Theory, Series A* 58(2) (1991), 165-180. [https://doi.org/10.1016/0097-3165\(91\)90058-0](https://doi.org/10.1016/0097-3165(91)90058-0).
- [32] Ryan Hoff, Gary Hu, and Yumo Liu, “Measurable Euclidean Ramsey theory for lines and finite configurations,” unpublished manuscript, 2026.
- [33] Oleg Pikhurko, *Algebraic Methods in Combinatorics*, lecture notes (2001), Sections 6.4 and 9.
<https://pikhurko.github.io/AlgMet.pdf>.
- [34] Parikshit Gopalan, “Constructing Ramsey graphs from Boolean function representations,” *Combinatorica* 34(2) (2014), 173-206. <https://doi.org/10.1007/s00493-014-2367-1>.
- [35] Ferdinand Ihringer and Sam Mattheus, “An improved algebraic construction for Ramsey numbers,” arXiv:2608.21769v1, 22 August 2026. <https://arxiv.org/abs/2608.21769v1>.
- [36] R. C. Baker, Glyn Harman, and János Pintz, “The difference between consecutive primes, II,” *Proceedings of the London Mathematical Society* 83(3) (2001), 532–562.
<https://doi.org/10.1112/plms/83.3.532>.
- [37] Adrian W. Dudek, “On the Riemann hypothesis and the difference between primes,” arXiv:1402.6417 (2014). <https://arxiv.org/abs/1402.6417>.
- [38] Peter Keevash and Eoin Long, “Frankl–Rödl-type theorems for codes and permutations,” *Transactions of the American Mathematical Society* 369 (2017), 1147–1162.
<https://doi.org/10.1090/tran/7015>.