Séminaire Lotharingien de Combinatoire **89B** (2023)
Article #6, 12 pp.

Proceedings of the 35^{th} Conference on Formal Power Series and Algebraic Combinatorics (Davis)

An Algebraic Perspective on Ramsey Numbers

Jesús A. De Loera*[1] and William J. Wesley†[1]

[1] *Department of Mathematics, University of California, Davis*

Abstract. We study the Ramsey numbers $R(r,s)$ through Hilbert's Nullstellensatz. We give a polynomial encoding whose solutions correspond to Ramsey graphs, those that do not contain a copy of K_r or $\bar{K}_s$. The Ramsey number is reached the first time the system has no solution. We construct Nullstellensatz certificates of this fact whose degrees are equal to the restricted online Ramsey numbers. These results generalize to other numbers in Ramsey theory, such as Rado, van der Waerden, and Hales–Jewett numbers.

Keywords: Ramsey theory, Hilbert's Nullstellensatz, polynomial ideals.

1 Introduction

Ramsey numbers are some of the most interesting and mysterious combinatorial numbers [19]. In its simplest, most popular form, the *Ramsey number* $R(r,s)$ is the smallest positive integer n such that every 2-coloring of the edges of K_n contains a copy of K_r in the first color or K_s in the second color. Ramsey numbers can be generalized by allowing more than two colors and graphs other than K_r and K_s. The number $R(G_1, G_2, \ldots, G_k)$ is the smallest positive integer n such that every k-coloring of the edges of K_n contains a copy of G_i in color i for some i. If $G_i = K_{r_i}$ for all i, we simply write $R(r_1, r_2, \ldots, r_k)$. All of these numbers are finite by Ramsey's theorem [38]. The goal of this article is to uncover further structure and complexity of Ramsey numbers through algebraic-geometric means.

Our paper introduces algebraic interpretations of $R(r,s)$ and related numbers and graphs using polynomial ideals, varieties, and Nullstellensatz identities (see [9] for an introduction). We tie the values and complexity of $R(r,s)$ to systems of *polynomial equations*. We show that these encodings give interesting information in the computational complexity of Ramsey numbers and Ramsey graphs. The precise models appear in Section 2. Before we state our main results, let us recall some relevant prior context and results:

Computing exact values for Ramsey numbers is a challenge. In fact there are only nine values of $R(r,s)$ with $3 \leq r \leq s$ whose exact values are known, and the only known

*deloera@math.ucdavis.edu.
†wjwesley@math.ucdavis.edu

nontrivial Ramsey numbers with more than two colors are $R(3,3,3) = 17$ and $R(3,3,4)$ = 30 [21, 7]. Ramsey numbers as small as $R(5,5)$ remain unknown, and the best known bounds are $43 \leq R(5,5) \leq 48$. See [17, 1]. The numbers $R(G_1, G_2)$ are known for some families of graphs, but many cases remain open (see, for example, [37] for a survey of small Ramsey numbers and their best known bounds). The best known asymptotic lower and upper bounds for diagonal Ramsey numbers $R(s,s)$ are given in [41] and [39], respectively.

While we know in practice computing Ramsey numbers is extremely difficult (and considered harder than fighting a war with an alien civilization), it is not clear what is the appropriate computational complexity class to show hardness of computing Ramsey numbers $R(r,s)$. For example, the closely related *arrowing decision problem* asks whether given three graphs F, G, H is there is a red-blue edge-coloring of F that contains neither a red G or a blue H? This decision problem was shown to be in co-NP for fixed choices of G, H [4]. Later Schaefer [40] showed that in general it is in the polynomial hierarchy to answer this queries, but it is not clear what to do with this complexity question when F, G, H are complete graphs K_N, K_r, K_s because there is only one value $R(r,s)$ for each input N, r, s, hence it is not clear how it can be hard for any of the usual classes like NP. See details in [40, 4, 22].

In recent years, Pak and collaborators [36, 25, 35] have proposed another way to measure complexity is by looking at counting sequences. We propose that their point of view could be another way to assert hardness of $R(r,s)$ by counting of Ramsey graphs: *Ramsey* (r,s)*-graphs* are graphs with no red clique of size r, and no independent set of size s. Clearly, the number of vertices of a Ramsey (r,s)-graph is less than the Ramsey number $R(r,s)$. We are interested in the number of Ramsey (r,s)-graphs on n vertices denoted by $RG(n,r,s)$. What is the complexity of counting the sequence of numbers $\{RG(n,r,s)\}_{n=1}^{\infty}$? From Ramsey's theorem this sequence consists of $R(r,s) - 1$ positive numbers and then an infinite tail of zeroes. We give some examples of $RG(n,r,s)$ in the columns of the table below, which are computed using the #SAT solver RELSAT [2], following the work of successful computations in Ramsey theory using SAT solvers in, for example, [23] and [6] (see also the database at [33]). The hardness of $R(r,s)$ can then be rephrased as the question of whether the counting function $RG(n,r,s)$ is in $\#P$.

n	$RG(n,3,3)$	$RG(n,3,4)$	$RG(n,3,5)$	$RG(n,3,6)$	$RG(n,3,7)$	$RG(n,4,4)$
2	2	2	2	2	2	2
3	6	7	7	7	7	8
4	18	40	41	41	41	62
5	12	322	387	388	388	892
6	0	2812	5617	5788	5789	22484
7	0	13842	113949	133080	133500	923012
8	0	17640	2728617	4569085	4681281	55881692
9	0	0	55650276	220280031	245743539	4319387624

Our Contributions:

In Section 2, we reintroduce the sequence $\{RG(n,r,s)\}_{n=1}^{\infty}$ as the number of solutions of certain zero-dimensional ideals over the polynomial ring $\overline{\mathbb{F}_2}[x_1,\dots,x_n]$. The solutions are indicator vectors that yield all Ramsey graphs (note, here they are not counted up to symmetry or automorphism classes). Some simple properties of $RG(n,r,s)$, such as the fact that $RG(n,r,s) \le RG(n,r+1,s)$, follow immediately from Theorem 1.

Theorem 1. *The Ramsey number $R(G_1,\dots,G_k)$ is at most n if and only if there is no solution to the following system over $\overline{\mathbb{F}_2}$, where $K_n = (V,E)$ is the complete graph on n vertices. Moreover, when the system has solutions, the number of solutions to this system is equal to the number of graphs of order n that avoid copies of G_i in color i. In particular, when $k=2$, $G_1 = K_r$, and $G_2 = K_s$, this is the number of Ramsey graphs $RG(n,r,s)$.*

$$p_{H,i} := \prod_{e\in E(H)} x_{i,e} = 0 \qquad \forall i, 1 \le i \le k, \quad \forall H \subseteq K_n,\ H \cong G_i, \tag{1.1}$$

$$q_e := 1 + \sum_{i=1}^{k} x_{i,e} = 0 \qquad \forall e \in E, \tag{1.2}$$

$$u_{i,j,e} := x_{i,e}x_{j,e} = 0 \qquad \forall e \in E,\ \forall i,j,\ i \ne j. \tag{1.3}$$

When $k=2$, $G_1 = K_r$, and $G_2 = K_s$, the Ramsey ideal *$RI(n,r,s)$ is ideal of the polynomial ring $\overline{\mathbb{F}_2}[x_{1,e},x_{2,e}]_{e\in E(K_n)}$ generated by the polynomials p_H, q_e and $u_{i,j,e}$. Then we have*

$$RI(n,r,s) \supseteq RI(n,r+1,s) \supseteq \cdots \supseteq RI(n,n,s) \supseteq RI(n,n+1,s) = RI(n,n+2,s) = \dots$$

and

$$RI(n,r,s) \supseteq RI(n,r,s+1) \supseteq \cdots \supseteq RI(n,r,n) \supseteq RI(n,r,n+1) = RI(n,r,n+2) = \dots$$

A key interesting consequence of Theorem 1 is that the very first value of n for which the system of equations has no solution is equal to the Ramsey number. One important result for our purposes is the famous *Hilbert's Nullstellensatz*, which states that a system of polynomial equations $f_1 = \cdots = f_m = 0$ over an algebraically closed field K has no solution if and only if there exist coefficient polynomials $\beta_1,\dots,\beta_m$ such that

$$\sum_{i=1}^{m} \beta_i f_i = 1. \tag{1.4}$$

We call such an identity (1.4) a *Nullstellensatz certificate*. The *degree* of a certificate is the largest degree of the polynomials β_i. Note that in our case the existence of a Nullstellensatz certificate is equivalent to an upper bound on the Ramsey number. The strong connection between combinatorial problems and the Hilbert Nullstellensatz has been investigated in, for example, [5, 32, 12, 10, 16, 15, 29, 11]. Here we show a surprising connection of Ramsey numbers to Nullstellensatz certificates.

In Theorem 2 we give a general construction for Nullstellensatz certificates of Ramsey number upper bounds using the polynomial encoding from Theorem 1. In other words, assuming the number of vertices of a Ramsey ideal is n and $n \geq R(G_1, \ldots, G_k)$, we give upper bounds for the degrees of the Nullstellensatz certificates. Surprisingly our construction of Nullstellensatz certificates for the Ramsey ideals yields certificate degrees given by the *restricted online Ramsey numbers* $\tilde{R}(G_1, \ldots, G_k; n)$, first introduced by Conlon et al. in [8]. These numbers are defined in terms of the following *Builder-Painter game*. Each turn Builder selects one edge e of K_n, and Painter selects a color in $[k]$ and colors e with this color. Builder wins the game once a monochromatic G_i in color i is constructed for some i. The number $\tilde{R}(G_1, \ldots, G_k; n)$ is the minimum number of edges Builder needs to guarantee a victory. We also use the simplified notation $\tilde{R}(r_1, \ldots, r_k; n)$ for $\tilde{R}(K_{r_1}, \ldots, K_{r_k}; n)$. It is trivial that $\tilde{R}(G_1, \ldots, G_k) \leq \binom{R(G_1, \ldots, G_k)}{2}$, but it was shown in [18] that in the case of 2-color classical Ramsey numbers that $\tilde{R}(r, r; n) \leq \binom{n}{2} - \Omega(n \log n)$ for $n = R(r, r)$. While this degree bound is linear in the number of variables, $k\binom{n}{2}$, it is an improvement over the upper bounds given in, for instance, [26, 28].

Theorem 2. *If $n \geq R(G_1, \ldots, G_k)$, then there is an explicit Nullstellensatz certificate of degree $\tilde{R}(G_1, \ldots, G_k; n) - 1$ that the statement $R(G_1, \ldots, G_k) > n$ is false using the encoding in Theorem 1. In particular, in the case of 2-color classical Ramsey numbers, this implies that if $n \geq R(r, s)$, then there exists a Nullstellensatz certificate of degree $\tilde{R}(r, s; n) - 1$ that the statement $R(r, s) > n$ is false.*

The proof of Theorem 2 does not rely on the graph-theoretic properties of Ramsey numbers, and in fact it applies to the whole of Ramsey theory. In particular, we can modify the encoding in Theorem 1 to suit several well-known problems in Ramsey theory (see, for example, [19, 27]). We express these problems using the general framework below.

Definition 3. *Let k be a positive integer, and let $\{S_n\}$ be a sequence of sets. For c in $[k]$, the set of colors, let $\mathcal{P}_n^c$ be a subset of S_n. A triple $A := (\{S_n\}, \{\mathcal{P}_n^c\}; k)$ is a Ramsey-type problem if the following hold:*

(i) $S_i \subseteq S_{i+1}$ *for* $i \geq 1$,

(ii) $\mathcal{P}_i^c \subseteq \mathcal{P}_{i+1}^c$ *for* $i \geq 1$, $1 \leq c \leq k$,

(iii) There exists an integer N such that for all $i \geq N$ and every k-coloring of S_i there is a color c and some element $X \in \mathcal{P}_i^c$ where each element of X is assigned color c.

The smallest such N is called the Ramsey-type number for A, and is denoted $R(A)$.

We see that in the problem of computing classical Ramsey numbers $R(r,s)$, we have $S_n = E(K_n) = \{(i,j) : 1 \leq i < j \leq n\}$. The families $\mathcal{P}_n^1$ and $\mathcal{P}_n^2$ consist of all the sets of edges of induced subgraphs of K_n containing r and s vertices, respectively. As another example, the problem of computing *Schur numbers* asks for the smallest n such that every k-coloring $[n]$ contains a monochromatic solution to the equation $x + y = z$. In this case we have $S_n = [n]$, and for all c we have $\mathcal{P}_n^c = \{\{x,y,z\} : \{x,y,z\} \subseteq [n], x + y = z\}$.

As we see in Section 2, the encoding in Theorem 1 can be modified to give bounds for many other Ramsey-type numbers, including Schur, Rado, van der Waerden, and Hales–Jewett numbers [19, 27]. We can define numbers analogous to the restricted online Ramsey numbers for Ramsey-type problems in terms of another Builder-Painter game. We define this game for a fixed n as follows.

For each turn, Builder selects one object from S_n and Painter assigns it a color in $[k]$. Builder wins once there is a color c and an element $X \in \mathcal{P}_n^c$ where every element of X is assigned color c. Define the number $\tilde{R}_k(\mathcal{P}_n^1, \ldots, \mathcal{P}_n^k; S_n)$ to be the smallest number of turns for which Builder is guaranteed a victory. In this notation, the restricted online Ramsey number $\tilde{R}(r,s;n)$ is equal to $\tilde{R}_2(\mathcal{P}_n^1, \mathcal{P}_n^2; S_n)$ with $\mathcal{P}_n$ and S_n defined as above for the Ramsey number $R(r,s)$. Theorem 4 generalizes Theorems 1 and 2.

Theorem 4. *Let $A = (\{S_n\}, \{\mathcal{P}_n^c\}; k)$ be a Ramsey-type problem. Then for each n, the Ramsey-type number for A is strictly greater than n if and only if the following system of equations has no solution over $\overline{\mathbb{F}_2}$.*

$$\begin{aligned} p_{X,c} &:= \prod_{s \in X} x_{c,s} = 0 && \forall X \in \mathcal{P}_n^c,\ 1 \leq c \leq k \\ q_s &:= 1 + \sum_{i=1}^{k} x_{i,s} = 0 && \forall s \in S_n, \\ u_{i,j,s} &:= x_{i,s} x_{j,s} = 0 && \forall s \in S_n,\ \forall i,j,\ 1 \leq i < j \leq k. \end{aligned}$$

If $n \geq R(A)$, then the minimal degree of a Nullstellensatz certificate for this system is at most $\tilde{R}_k(\mathcal{P}_n^1, \ldots, \mathcal{P}_n^k; S_n) - 1$. Moreover, the number of solutions to this system is equal to the number of k-colorings of S_n such that for every color c, each set $X \in \mathcal{P}_n^c$ contains an object that is not assigned color c.

For example, in the case of Schur numbers, the number of solutions to this system is exactly the number of k-colorings of $[n]$ that do not contain any monochromatic solutions to $x + y = z$. In Section 2 we give some examples of values of $\tilde{R}(r,s;n)$ and $\tilde{R}(\mathcal{P}_n^1, \ldots, \mathcal{P}_n^k; S_n)$ and discuss the Nullstellensatz certificates for the associated polynomial systems.

2 Ramsey and Hilbert's Nullstellensatz

In this section we give several encodings of the problem of finding an upper bound for $R(r,s)$ in terms of the feasibility of a system of polynomial equations. In the simplest version of the encoding, the variables correspond to edges in the graph K_n, and the solutions of the system correspond to graph colorings that avoid monochromatic copies of K_r and K_s. If the system is infeasible for some n, then no such coloring exists, hence $R(r,s) \leq n$.

Many combinatorial problems can be encoded as a system of polynomial equations, including colorings, independence sets, partitions, etc. (see, e.g., [5, 3, 14, 12, 16, 24, 30, 32]). A Nullstellensatz certificate for such a combinatorial polynomial system is therefore a proof that a combinatorial theorem is true. We are interested on bounding the Nullstellensatz degree for our Ramsey systems.

There are known general "algebraic geometers" upper bounds for the degree of a Nullstellensatz certificate, so the above procedure terminates, even when these bounds are exponential and sharp in general [26]. However, the exponential bounds should not be bad news for combinatorialists. First, it has been shown [28] that for "combinatorial ideals", the bounds are much better, linear in the number of variables. Over finite fields there are degree bounds that are independent of the number of variables [20], and a recent paper [34] gives substantial improvements to these bounds. The bounds we give in Theorems 2 and 4 for our systems of equations are better than the above bounds. Moreover, it has been documented that in practice the degrees of Nullstellensatz certificates of NP-hard problems (e.g., non-3-colorability), tend to be small "in practice" (see, for example, [31, 29, 15] and the references therein), especially when the polynomial encodings are over finite fields. Note also that when we know the degree of the Nullstellensatz certificate, one can compute explicit coefficients of the Nullstellensatz certificate using a linear algebra system derived by equating the monomials of the identity. This has been exploited in practical computation with great success, see [10, 15, 29].

We now prove Theorem 1 of our encoding for Ramsey numbers over $\overline{\mathbb{F}_2}$ below.

Proof of Theorem 1. Suppose there is a solution $\mathbf{x}$ to the system over $\overline{\mathbb{F}_2}$. For each edge e of K_n and each color i, the system has a variable $x_{i,e}$. The polynomials $u_{i,j,e}$ guarantee that for a given e, at most one variable $x_{i,e}$ is nonzero. From the polynomials q_e, we then see that exactly one index i such that $x_{i,e} = 1$, and let $\phi(\mathbf{x})$ be the coloring χ where $\chi(e)$ is this index. Color each edge e of K_n with the color $\chi(e)$. In the equations involving the polynomials p_H, for each subgraph H of K_n with $H \cong G_i$, there is at least one edge e in H with $x_{i,e} = 0$. Therefore $\chi(e) \neq i$, so there is no monochromatic copy of G_i in color i.

Conversely, if we have a coloring χ of the edges of K_n with no monochromatic G_i in color i, then let $\psi(\chi)$ be the solution $\mathbf{x}$ where $x_{i,e}$ is 1 if $\chi(e) = i$ and 0 otherwise. One can check easily that $\mathbf{x}$ satisfies the system of equations. The maps ϕ and ψ are inverses of each other, and so the number of solutions to the system is equal to the number of colorings of K_n with no monochromatic G_i in color i.

For the first chain of ideals, observe that for a fixed i, the polynomial $\prod_{e\in E(H)} x_{i,e}$ divides $\prod_{e\in E(H')} x_{i,e}$ if and only if H is a subgraph of H'. Since every copy of K_{r+1} in K_n contains a copy of K_r as a subgraph, in the ideal $RI(n, r+1, s)$, every polynomial of the form $\prod_{e\in E(H')} x_{i,e}$ with $H' \cong K_{r+1}$ is divisible by a generator $\prod_{e\in E(H)} x_{i,e}$ of $RI(n,r,s)$ with $H \cong K_r$. The ideals in the chain are equal for $r > n$ since in this case K_r is not a subgraph of K_n. The proof for the second chain of ideals is similar. □

Before we prove Theorem 2, we show a special case as a warm-up example. There is a simple certificate of the fact that $R(r,2) \leq r$.

Example 5. *For all r, there exists a Nullstellensatz certificate of degree $\binom{r}{2} - 1$ of the statement $R(r,2) \leq r$.*

Proof. Label the edges of K_r from 1 to $n = \binom{r}{2}$. The following identity is a certificate that $R(r,2) \leq r$. Polynomials in parentheses are part of the system of equations in Theorem 1.

$$\begin{aligned} 1 = {} & (1 + x_{1,1} + x_{2,1}) + x_{1,1}(1 + x_{1,2} + x_{2,2}) + x_{1,1}x_{1,2}(1 + x_{1,3} + x_{2,3}) + \dots \\ & + x_{1,1}x_{1,2}\cdots x_{1,n-1}(1 + x_{1,n} + x_{2,n}) \\ & + x_{2,1} + x_{1,1}(x_{2,2}) + x_{1,1}x_{1,2}(x_{2,3}) + \cdots + x_{1,1}x_{1,2}\cdots x_{1,n-1}(x_{2,n}) \\ & + (x_{1,1}\cdots x_{1,n}) \end{aligned}$$

□

In the proof of Theorem 2, we show how to translate a strategy for Builder into a Nullstellensatz certificate. This method can be used to construct a certificate for all (known) upper bounds for $R(G_1, \dots, G_s)$. Notably, better strategies for Builder yield lower degree certificates. In Example 5, this is not a concern since the order in which Builder selects edges does not matter, and in fact $\tilde{R}(r,2;r) = \binom{r}{2}$. Painter simply colors every edge Builder selects the first color, and Builder wins when all $\binom{r}{2}$ edges are selected.

The proofs of Theorems 2 and 4 are similar, and in fact Theorem 2 follows from Theorem 4, but for the sake of concreteness we begin with Theorem 2.

Proof of Theorem 2. Number the edges of K_n from 1 to $\binom{n}{2}$. A t-turn game state g is a set $\{(e_{i_1}, c_1), (e_{i_2}, c_2), \dots, (e_{i_t}, c_t)\}$ of pairs of edges $e_{i_j} \in E$ chosen by Builder and colors $c_j \in [k]$ chosen by Painter. A game is complete if there is some color $c \in [k]$ where Painter has colored a monochromatic G_c in color c. Let $d := \tilde{R}(G_1, \dots, G_k; n)$. If Builder follows an optimal strategy for choosing edges, then the game lasts at most d turns, that is $t \leq d$.

For a t-turn game state g, define the monomial $\pi(g)$ to be $\pi(g) := \prod_{j=1}^{t} x_{c_j, e_{i_j}}$. Similarly, for any monomial $f = \prod_{j=1}^{t} x_{c_j, e_{i_j}}$ with distinct e_{i_j}, let $\sigma(f)$ denote the game state

$\{(e_{i_1}, c_1), (e_{i_2}, c_2), \ldots, (e_{i_t}, c_t)\}$. We will describe an algorithm to construct a Nullstellensatz certificate of the form

$$\sum_{i=1}^{k} \sum_{H \cong G_i} \beta_{H,i} p_{H,i} + \sum_{e \in E} \gamma_e q_e = 1. \tag{2.1}$$

Denote the left-hand side of Equation (2.1) by L. For each $i \in [k]$, initialize $\beta_{H,i}$ to 0 for all $H \cong G_i$. Initialize γ_e to 0 for all edges e except e_1, and set $\gamma_{e_1} := 1$. Then repeat the following:

1. Expand and simplify L so that L is a sum of monomials. If $L = 1$, then we are done. Otherwise, at least one term in L is a nonconstant monomial f.

2. If $\sigma(f)$ is a completed game state, then $p_{H,i}$ divides f for some color i and $H \cong G_i$. Then set $\beta_{H,i} \leftarrow \beta_{H,i} + \frac{f}{p_{H,i}}$. This results in $L \leftarrow L + f$, which cancels the original f in the certificate since it is an expression over $\overline{\mathbb{F}_2}$, which has characteristic 2.

3. If $\sigma(f)$ is not a completed game state, then let e be an edge that Builder should choose in an optimal strategy from the game state $\sigma(f)$. Set $\gamma_e \leftarrow \gamma_e + f$. Since $f q_e = f + \sum_{i=1}^{k} f x_{i,e}$, we obtain $L \leftarrow L + f + \sum_{i=1}^{k} f x_{i,e}$. This results in the cancellation of f in L, but adds k additional terms (one for each of Painter's k choices for coloring e) to L. Note that if $\sigma(f)$ is a t-turn game state, then $\sigma(f x_{i,e})$ is a $(t+1)$-turn game state for all i.

By the symmetry of K_n, it is arbitrary which edge Builder selects first. Therefore each nonconstant term that appears in L corresponds to a game state where Builder (but not necessarily Painter) has followed an optimal strategy. Since terms that correspond to completed games are cancelled out in step 3, this procedure terminates, resulting in a Nullstellensatz certificate. Because Builder follows an optimal strategy, the maximal degree of any term in any γ_e is $d-1$, so the degree of the certificate is $d-1$. □

To illustrate the importance of Builder's strategy in this method, observe that one can construct a degree 7 certificate for the statement $R(3,3) \leq 6$ using the following strategy: For the first five turns, Builder selects each edge incident to some vertex v. No matter how Painter colors these edges, three must be colored the same color. Call these edges vw_1, vw_2, vw_3. For the next three turns, Builder selects the edges w_1w_2, w_1w_3, and w_2w_3, and Painter must construct a monochromatic triangle. However, if Builder plays poorly and selects, for example, the edges $(1,2), (2,3), (3,4), (4,5), (5,6), (1,6), (1,4), (2,5)$, and $(3,6)$, then no matter what Painter does there are *no* monochromatic triangles, and this leads to a higher degree certificate.

The proof of Theorem 2 shows that the polynomials can "simulate" a tree of Builder-Painter games. However, in general the degrees of certificates can be strictly smaller than the bounds given in Theorem 2. For example, by a computational search, it can be shown that $\tilde{R}(3,3;6) = 8$. However, there exists a Nullstellensatz certificate of degree 5 using the encoding in Theorem 1, which is better than the bound given in Theorem 2. Due to space constraints we skip the proof of Theorem 4 but it can be found in [13].

As an application of Theorem 4, let $\mathcal{E}$ be a linear equation, and let $R_k(\mathcal{E})$ denote the k-color *Rado number* for $\mathcal{E}$, the smallest n such that every k-coloring of $[n]$ contains a monochromatic solution to $\mathcal{E}$. Let $X_{n,\mathcal{E}}$ be the set of all solutions over $[n]$ to $\mathcal{E}$. Let $\mathcal{P}_n^c := X_{n,\mathcal{E}}$ for all c. If $R_k(\mathcal{E})$ exists, then $(\{[n]\}, \{\mathcal{P}_n^c\}; k)$ is a Ramsey-type problem, and we have the following corollary.

Corollary 6. *Let $\mathcal{E}$ be the linear equation $\sum_{j=1}^t a_i y_i = a_0$ with a finite Rado number $R_k(\mathcal{E})$. Let $X_{n,\mathcal{E}} = \{(m_1, \ldots, m_t) : \sum_{j=1}^t a_j m_j = a_0,\ 1 \le m_j \le n\}$ be the set of solutions over $[n]$ to $\mathcal{E}$. Then for every n, the following system has no solution over $\overline{\mathbb{F}_2}$ if and only if $n \ge R_k(\mathcal{E})$.*

$$\begin{aligned}
\prod_{j=1}^{t} x_{i,m_j} &= 0 && \forall (m_1, \ldots, m_t) \in X_{n,\mathcal{E}},\ 1 \le i \le k,\\
1 + \sum_{i=1}^{k} x_{i,m} &= 0 && 1 \le m \le n,\\
x_{i,m} x_{j,m} &= 0 && 1 \le m \le n, 1 \le i < j \le k.
\end{aligned}$$

The degree of a minimal Nullstellensatz certificate for this system has degree at most $\tilde{R}_k(X_{n,\mathcal{E}}, \ldots, X_{n,\mathcal{E}}; [n]) - 1$.

As an example, let $\mathcal{E}$ denote the equation $x + 3y = 3z$, and let $X_{9,\mathcal{E}}$ be the solutions to $\mathcal{E}$ over $[9]$ as above. It is known that $R_2(\mathcal{E}) = 9$ [27]. However, Builder can select, in order, the integers 4,6,9,3, and 7 to win the Builder-Painter game in at most 5 turns: since $(6,4,6)$ is a solution, 4 and 6 must be different colors, and then since $(9,6,9)$ and $(3,3,4)$ are solutions, 4 and 9 must be one color and 3 and 6 are the other color. But then $(3,6,7)$ and $(9,4,7)$ are solutions, so there is a monochromatic solution no matter which color Painter selects for 7. Therefore $\tilde{R}_2(X_{9,\mathcal{E}}, X_{9,\mathcal{E}}; [9]) \le 5$, and the minimal degree of a Nullstellensatz certificate for the system of equations in Corollary 6 is at most 4. In fact, some computations show the minimal degree is 2.

Similarly, the encoding in Theorem 1 for the Schur number $S(2) = R_2(x + y = z)$ also gives an example of Nullstellensatz certificates that are smaller than the ones given by games. It is well-known that $S(2) = 5$, and from the encoding in Theorem 4, we have $S(2) \le 5$ if and only if the following system of equations has no solutions over $\overline{\mathbb{F}_2}$.

$$\begin{aligned}
&1 + x_{1,i} + x_{2,i} = 0, && 1 \le i \le 5,\\
&\left.\begin{aligned}
&x_{i,1}x_{i,2} = 0, \quad x_{i,2}x_{i,4} = 0,\\
&x_{i,1}x_{i,3}x_{i,4} = 0, \quad x_{i,1}x_{i,4}x_{i,5} = 0, \quad x_{i,2}x_{i,3}x_{i,5} = 0.
\end{aligned}\right\} && i = 1,2
\end{aligned}$$

A computer search shows that the number $\tilde{R}_2(X_{5,x+y=z}, X_{5,x+y=z}; [5]) = 5$, where $X_{5,x+y=z}$ is the set of positive integer solutions to $x + y = z$ in $[1, 5]$. We computed a degree 3 Nullstellensatz certificate for the above system of equations, which is an improvement on the bound in Theorem 4. We omit the certificate here for space considerations, but it can be found in [13]. Moreover, by Theorem 4 there are similar consequences for van der Waerden numbers, Hales–Jewett numbers, and essentially any other Ramsey-type quantity. We are unable to include them here due to space, but we invite readers to see more in [13].

Acknowledgements

The authors were supported by National Science Foundation grant DMS-1818969. We thank Susan Margulies for helpful discussions and assistance with computations.

References

[1] V. Angeltveit and B. McKay. "$R(5, 5) \leq 48$". *J. Graph Theory* **89**.1 (2018), pp. 5–13. DOI.

[2] R. Bayardo. "Relsat". `https://github.com/roberto-bayardo/relsat`.

[3] D. Bayer. "The Division Algorithm and the Hilbert Scheme". PhD thesis. Harvard University, 1982.

[4] S. A. Burr. "On the computational complexity of Ramsey-type problems". *Mathematics of Ramsey theory*. Vol. 5. Algorithms Combin. Springer, Berlin, 1990, pp. 46–52. DOI.

[5] S. Buss and T. Pitassi. "Good degree bounds on Nullstellensatz refutations of the induction principle". Vol. 57. 2. Complexity 96—The Eleventh Annual IEEE Conference on Computational Complexity (Philadelphia, PA). 1998, pp. 162–171. DOI.

[6] Y. Chang, J. A. De Loera, and W. J. Wesley. "Rado Numbers and SAT Computations". *Proceedings of the 2022 International Symposium on Symbolic and Algebraic Computation*. ISSAC '22. Association for Computing Machinery, 2022, 333–342. DOI.

[7] M. Codish, M. Frank, A. Itzhakov, and A. Miller. "Computing the Ramsey number $R(4, 3, 3)$ using abstraction and symmetry breaking". *Constraints* **21**.3 (2016), pp. 375–393.

[8] D. Conlon, J. Fox, A. Grinshpun, and X. He. "Online Ramsey Numbers and the Subgraph Query Problem". *Building Bridges II*. Ed. by I. Bárány, G. O. H. Katona, and A. Sali. Springer, 2019, pp. 159–194.

[9] D. A. Cox, J. Little, and D. O'Shea. *Ideals, varieties, and algorithms*. Fourth. Undergraduate Texts in Mathematics. An introduction to computational algebraic geometry and commutative algebra. Springer, Cham, 2015, pp. xvi+646. DOI.

[10] J. A. De Loera, J. Lee, P. N. Malkin, and S. Margulies. "Hilbert's Nullstellensatz and an algorithm for proving combinatorial infeasibility". *Proceedings of the Twenty-first International Symposium on Symbolic and Algebraic Computation* (2008), pp. 197–206.

[11] J. A. De Loera, J. Lee, S. Margulies, and J. Miller. "Weak orientability of matroids and polynomial equations". *European J. Combin.* **50** (2015), pp. 56–71. DOI.

[12] J. A. De Loera, J. Lee, S. Margulies, and S. Onn. "Expressing Combinatorial Problems by Systems of Polynomial Equations and Hilbert's Nullstellensatz". *Combinatorics, Probability and Computing* **18**.4 (2009), 551–582. DOI.

[13] J. A. De Loera and W. J. Wesley. "Ramsey Numbers through the Lenses of Polynomial Ideals and Nullstellensätze". 2022. arXiv:2209.13859.

[14] J. A. De Loera. "Gröbner bases and graph colorings". *Beiträge Algebra Geom.* **36**.1 (1995), pp. 89–96.

[15] J. A. De Loera, J. Lee, P. N. Malkin, and S. Margulies. "Computing infeasibility certificates for combinatorial problems through Hilbert's Nullstellensatz". *J. Symbolic Comput.* **46**.11 (2011), pp. 1260–1283. DOI.

[16] J. A. De Loera, S. Margulies, M. Pernpeintner, E. Riedl, D. Rolnick, G. Spencer, D. Stasi, and J. Swenson. "Graph-coloring ideals: Nullstellensatz certificates, Gröbner bases for chordal graphs, and hardness of Gröbner bases". *ISSAC'15—Proceedings of the 2015 ACM International Symposium on Symbolic and Algebraic Computation*. ACM, New York, 2015.

[17] G. Exoo. "A lower bound for $R(5,5)$". *J. Graph Theory* **13**.1 (1989), pp. 97–98. DOI.

[18] D. Gonzalez, X. He, and H. Zheng. "An upper bound for the restricted online Ramsey number". *Discrete Math.* **342**.9 (2019), pp. 2564–2569. DOI.

[19] R. Graham, B. Rothschild, and J. Spencer. *Ramsey Theory*. 2nd. Wiley, 1980.

[20] B. Green and T. Tao. "The distribution of polynomials over finite fields, with applications to the Gowers norms". *Contrib. Discrete Math.* **4**.2 (2009), pp. 1–36.

[21] R. Greenwood and A. Gleason. "Combinatorial relations and chromatic graphs". *Canadian J. Math.* **7** (1955), pp. 1–7. DOI.

[22] H. Haanpää. "Computational Methods for Ramsey Numbers". Research Report A65, Helsinki University of Technology Laboratory for Theoretical Computer Science, 2000.

[23] M. Heule. "Schur Number Five". *Proceedings of AAAI-18* (2018), pp. 6598–6606.

[24] C. J. Hillar and T. Windfeldt. "Algebraic characterization of uniquely vertex colorable graphs". *J. Combin. Theory Ser. B* **98**.2 (2008), pp. 400–414. DOI.

[25] C. Ikenmeyer and I. Pak. "What is in #P and what is not?" *CoRR* (2022). arXiv:2204.13149.

[26] J. Kollár. "Sharp Effective Nullstellensatz". *Journal of the AMS* **1**.4 (1988), pp. 963–975.

[27] B. M. Landman and A. Robertson. *Ramsey theory on the integers*. Second. Vol. 73. Student Mathematical Library. American Mathematical Society, Providence, RI, 2014. DOI.

[28] D. Lazard. "Algèbre linéaire sur $K[X_1, \cdots, X_n]$, et élimination". *Bull. Soc. Math. France* **105**.2 (1977), pp. 165–190. Link.

[29] B. Li, B. Lowenstein, and M. Omar. "Low degree Nullstellensatz certificates for 3-colorability". *Electron. J. Combin.* **23**.1 (2016), Paper 1.6, 12. DOI.

[30] L. Lovász. "Stable sets and polynomials". Vol. 124. 1-3. Graphs and combinatorics (Qawra, 1990). 1994, pp. 137–153. DOI.

[31] S. Margulies. "Computer Algebra, Combinatorics, and Complexity: Hilbert's Nullstellensatz and NP-complete Problems". PhD thesis. 2008.

[32] S. Margulies, S. Onn, and D. V. Pasechnik. "On the complexity of Hilbert refutations for partition". *J. Symbolic Comput.* **66** (2015), pp. 70–83. DOI.

[33] B. McKay. "Ramsey Graphs". `https://users.cecs.anu.edu.au/~bdm/data/ramsey.html`.

[34] G. Moshkovitz and J. Yu. "Sharp effective finite-field Nullstellensatz". preprint, arXiv, https://arxiv.org/abs/2111.09305. 2022.

[35] I. Pak. "What is a combinatorial interpretation?" 2022. arXiv:2209.06142.pdf.

[36] I. Pak. "Complexity problems in enumerative combinatorics". *Proceedings of the International Congress of Mathematicians—Rio de Janeiro 2018. Vol. IV. Invited lectures*. World Sci. Publ., Hackensack, NJ, 2018, pp. 3153–3180.

[37] S. Radziszowski. "Small Ramsey Numbers". *Electronic Journal of Combinatorics* (2021).

[38] F. Ramsey. "On a problem of formal logic". *Proceedings of the London Mathematical Society* **30** (1930), pp. 264–286.

[39] A. Sah. "Diagonal Ramsey via effective quasirandomness". 2020. arXiv:2005.09251.

[40] M. Schaefer. "Graph Ramsey theory and the polynomial hierarchy (extended abstract)". *Annual ACM Symposium on Theory of Computing (Atlanta, GA, 1999)*. ACM, New York, 1999, pp. 592–601. DOI.

[41] J. Spencer. "Ramsey's theorem—a new lower bound". *J. Combinatorial Theory Ser. A* **18** (1975), pp. 108–115. DOI.