Rado numbers: SAT methods and connections to Nullstellensatz complexity

William (Jack) Wesley (joint with Yuan Chang and Jesús De Loera)

University of California, Davis

April 19, 2023

Outline of Talk

1. Arithmetic Ramsey theory
2. Rado numbers and SAT
3. Nullstellensatz certificates for Ramsey-type numbers

Introduction

Ramsey theory is the study of patterns that necessarily appear when a mathematical structure is sufficiently large: “total disorder is impossible”

Introduction

Ramsey theory is the study of patterns that necessarily appear when a mathematical structure is sufficiently large: "total disorder is impossible"

Theorem (Ramsey, 1930)

Given positive integers r and s, there exists an integer n such that every red/blue edge coloring of K_n contains either a red K_r or a blue K_s.

Introduction

Ramsey theory is the study of patterns that necessarily appear when a mathematical structure is sufficiently large: "total disorder is impossible"

Theorem (Ramsey, 1930)

Given positive integers r and s, there exists an integer n such that every red/blue edge coloring of K_n contains either a red K_r or a blue K_s.

But Ramsey theory came before Ramsey!

Introduction

Ramsey theory is the study of patterns that necessarily appear when a mathematical structure is sufficiently large: "total disorder is impossible"

Theorem (Ramsey, 1930)

Given positive integers r and s, there exists an integer n such that every red/blue edge coloring of K_n contains either a red K_r or a blue K_s.

But Ramsey theory came before Ramsey!

Origins in algebra and number theory

Origins of Ramsey Theory

Theorem (Hilbert's cube lemma, 1892)

For every k and d, there is an n such that every k-coloring of $\{1, \ldots, n\}$ produces a monochromatic solution to the system

$$x_0 + \sum_{i \in I} x_i = x_I, \quad I \subseteq \{1, \ldots, d\}, I \neq \emptyset.$$

Hilbert used this to prove results on irreducibility of rational functions.

Schur's Theorem

Theorem (Schur, 1916)

For every $k \geq 1$, there exists a number n such that every k-coloring of $\{1, 2, \ldots, n\}$ contains a monochromatic triple (x, y, z) satisfying

$$x + y = z.$$

Schur's Theorem

Theorem (Schur, 1916)

For every $k \geq 1$, there exists a number n such that every k-coloring of $\{1, 2, \ldots, n\}$ contains a monochromatic triple (x, y, z) satisfying

$$x + y = z.$$

- Proven while Schur was attacking Fermat's Last Theorem; used to prove existence of solutions to $x^m + y^m = z^m \pmod{p}$

Schur's Theorem

Theorem (Schur, 1916)

For every $k \geq 1$, there exists a number n such that every k-coloring of $\{1, 2, \ldots, n\}$ contains a monochromatic triple (x, y, z) satisfying

$$x + y = z.$$

- Proven while Schur was attacking Fermat's Last Theorem; used to prove existence of solutions to $x^m + y^m = z^m \pmod{p}$
- The Schur number $S(k)$ is the *smallest* such n

Schur numbers

- $S(2) = 5$

Schur numbers

- $S(2) = 5$
- We can 2-color [4] while avoiding monochromatic solutions to $x + y = z$:

1 2 3 4

Schur numbers

- $S(2) = 5$
- We can 2-color $[4]$ while avoiding monochromatic solutions to $x + y = z$:

1 2 3 4

- $S(3) = 14$:

Schur numbers

- $S(2) = 5$
- We can 2-color [4] while avoiding monochromatic solutions to $x + y = z$:

1 2 3 4

- $S(3) = 14$:
- We can 3-color [13] while avoiding monochromatic solutions to $x + y = z$:

1 2 3 4 5 6 7 8 9 10 11 12 13

Van der Waerden's Theorem

Theorem (van der Waerden, 1927)

For every $k, \ell \geq 1$, there exists a number n such that every k-coloring of $\{1, \ldots, n\}$ contains a monochromatic length ℓ arithmetic progression.

- Rephrased: there is a positive integer d such that there is a monochromatic solution to the system of equations

$$x_2 = x_1 + d,\ x_3 = x_2 + d, \ldots,\ x_\ell = x_{\ell-1} + d.$$

- Originally conjectured by Schur while studying quadratic residues.

Van der Waerden numbers

Definition

The van der Waerden number $w(k, \ell)$ is the smallest n such that every k-coloring of $\{1, \ldots, n\}$ contains a monochromatic ℓ-term arithmetic progression.

Van der Waerden numbers

Definition

The van der Waerden number $w(k, \ell)$ is the smallest n such that every k-coloring of $\{1, \ldots, n\}$ contains a monochromatic ℓ-term arithmetic progression.

Example: $w(2, 3) = 9$

1 2 3 4 5 6 7 8
1 2 3 4 5 6 7 8
1 2 3 4 5 6 7 8

Van der Waerden numbers

Best general bounds:

- $w(2, p+1) \geq p2^p$ (Berlekamp '68)
- $w(k, \ell) \leq 2^{2^{k^{2^{2^{\ell+9}}}}}$ (Gowers '01)

Van der Waerden numbers

Best general bounds:

- $w(2, p+1) \geq p2^p$ (Berlekamp '68)
- $w(k, \ell) \leq 2^{2^{k^{2^{2^{\ell+9}}}}}$ (Gowers '01)

All known exact values of $w(k, \ell)$:

ℓ \ k	2	3	4
3	9	27	76
4	35	293	
5	178		
6	1132		

Rado's theorem

Questions:

Questions:

- What about other (systems of) equations?

Rado's theorem

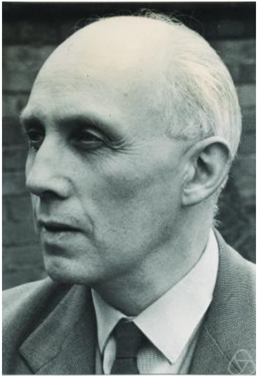
Questions:

- What about other (systems of) equations?
- Is there a way to unify the results of Hilbert, Schur, and van der Waerden?

Questions:

- What about other (systems of) equations?
- Is there a way to unify the results of Hilbert, Schur, and van der Waerden?

Answered by Rado in his PhD thesis with Schur.



Rado numbers

Definition (Rado number)

The ($k-$color) Rado number $R_k(\mathcal{E})$ of an equation $\mathcal{E}$ is the smallest number n such that every $k-$coloring of $\{1, \ldots, n\}$ contains a monochromatic solution to $\mathcal{E}$.

Rado numbers

Definition (Rado number)

The ($k-$color) Rado number $R_k(\mathcal{E})$ of an equation $\mathcal{E}$ is the smallest number n such that every $k-$coloring of $\{1, \ldots, n\}$ contains a monochromatic solution to $\mathcal{E}$.

- The Schur number $S(k)$ is $R_k(x + y = z)$.

Rado numbers

Definition (Rado number)

The ($k-$color) Rado number $R_k(\mathcal{E})$ of an equation $\mathcal{E}$ is the smallest number n such that every $k-$coloring of $\{1, \ldots, n\}$ contains a monochromatic solution to $\mathcal{E}$.

- The Schur number $S(k)$ is $R_k(x + y = z)$.
- Not all Rado numbers are finite: e.g., $R_2(2x + 2y = z) = 34$, $R_3(2x + 2y = z) = \infty$.

Rado's theorem

Definition

An equation $\mathcal{E}$ is regular if $R_k(\mathcal{E})$ exists (is finite) for all k.

Rado's theorem

Definition

An equation $\mathcal{E}$ is regular if $R_k(\mathcal{E})$ exists (is finite) for all k.

Rado's theorem generalizes Schur's theorem:

Theorem (Rado's Single Equation Theorem, 1933)

Let $m \geq 2$, and let $c_i \in \mathbb{Z} \setminus \{0\}$. Then the equation

$$\sum_{i=1}^{m} c_i x_i = 0$$

is regular if and only if there exists a nonempty subset of the coefficients that sums to 0.

Rado's theorem

Definition

An equation $\mathcal{E}$ is regular if $R_k(\mathcal{E})$ exists (is finite) for all k.

Rado's theorem generalizes Schur's theorem:

Theorem (Rado's Single Equation Theorem, 1933)

Let $m \geq 2$, and let $c_i \in \mathbb{Z} \setminus \{0\}$. Then the equation

$$\sum_{i=1}^{m} c_i x_i = 0$$

is regular if and only if there exists a nonempty subset of the coefficients that sums to 0.

- $4w - 2x + 3y - 7z = 0$ is regular.

Rado's theorem

Definition

An equation $\mathcal{E}$ is regular if $R_k(\mathcal{E})$ exists (is finite) for all k.

Rado's theorem generalizes Schur's theorem:

Theorem (Rado's Single Equation Theorem, 1933)

Let $m \geq 2$, *and let* $c_i \in \mathbb{Z} \setminus \{0\}$. *Then the equation*

$$\sum_{i=1}^{m} c_i x_i = 0$$

is regular if and only if there exists a nonempty subset of the coefficients that sums to 0.

- $4w - 2x + 3y - 7z = 0$ is regular.
- $2x - 5y + 6z = 0$ is NOT regular.

SAT successes in Ramsey theory

- $w(2,6) = 1132$ (Kouril-Paul 2008)

SAT successes in Ramsey theory

- $w(2,6) = 1132$ (Kouril-Paul 2008)
- Green-Tao numbers (Kullmann 2010)

SAT successes in Ramsey theory

- $w(2,6) = 1132$ (Kouril-Paul 2008)
- Green-Tao numbers (Kullmann 2010)
- $w(3,4) = 293$ (Kouril 2012)

SAT successes in Ramsey theory

- $w(2,6) = 1132$ (Kouril-Paul 2008)
- Green-Tao numbers (Kullmann 2010)
- $w(3,4) = 293$ (Kouril 2012)
- Generalized van der Waerden numbers (Ahmed-Kullmann-Snevily 2014)

SAT successes in Ramsey theory

- $w(2, 6) = 1132$ (Kouril-Paul 2008)
- Green-Tao numbers (Kullmann 2010)
- $w(3, 4) = 293$ (Kouril 2012)
- Generalized van der Waerden numbers (Ahmed-Kullmann-Snevily 2014)
- Various Rado numbers (Myers 2015)

SAT successes in Ramsey theory

- $w(2,6) = 1132$ (Kouril-Paul 2008)
- Green-Tao numbers (Kullmann 2010)
- $w(3,4) = 293$ (Kouril 2012)
- Generalized van der Waerden numbers (Ahmed-Kullmann-Snevily 2014)
- Various Rado numbers (Myers 2015)
- $R(3,3,4) = 30$ (Codish-Frank-Itzhakov-Miller 2016)

SAT successes in Ramsey theory

- $w(2, 6) = 1132$ (Kouril-Paul 2008)
- Green-Tao numbers (Kullmann 2010)
- $w(3, 4) = 293$ (Kouril 2012)
- Generalized van der Waerden numbers (Ahmed-Kullmann-Snevily 2014)
- Various Rado numbers (Myers 2015)
- $R(3, 3, 4) = 30$ (Codish-Frank-Itzhakov-Miller 2016)
- Pythagorean Triples (Heule-Kullmann-Marek 2016)

SAT successes in Ramsey theory

- $w(2,6) = 1132$ (Kouril-Paul 2008)
- Green-Tao numbers (Kullmann 2010)
- $w(3,4) = 293$ (Kouril 2012)
- Generalized van der Waerden numbers (Ahmed-Kullmann-Snevily 2014)
- Various Rado numbers (Myers 2015)
- $R(3,3,4) = 30$ (Codish-Frank-Itzhakov-Miller 2016)
- Pythagorean Triples (Heule-Kullmann-Marek 2016)
- $S(5) = 161$ (Heule 2018)

SAT successes in Ramsey theory

- $w(2,6) = 1132$ (Kouril-Paul 2008)
- Green-Tao numbers (Kullmann 2010)
- $w(3,4) = 293$ (Kouril 2012)
- Generalized van der Waerden numbers (Ahmed-Kullmann-Snevily 2014)
- Various Rado numbers (Myers 2015)
- $R(3,3,4) = 30$ (Codish-Frank-Itzhakov-Miller 2016)
- Pythagorean Triples (Heule-Kullmann-Marek 2016)
- $S(5) = 161$ (Heule 2018)
- Generalized 3-color Schur numbers (Boza-Marín-Revuelta-Sanz 2019)

Schur numbers

Table of all known Schur numbers:

k	$S(k)$	
1	2	
2	5	
3	14	
4	45	Golomb and Baumert '65
5	161	Heule '18

Schur numbers

Table of all known Schur numbers:

k	$S(k)$	
1	2	
2	5	
3	14	
4	45	Golomb and Baumert '65
5	161	Heule '18

- Showing $S(5) \leq 161$ was a massive SAT computation using cube and conquer

Schur numbers

Table of all known Schur numbers:

k	$S(k)$	
1	2	
2	5	
3	14	
4	45	Golomb and Baumert '65
5	161	Heule '18

- Showing $S(5) \leq 161$ was a massive SAT computation using cube and conquer
- 2-petabyte certificate

Schur numbers

Table of all known Schur numbers:

k	$S(k)$	
1	2	
2	5	
3	14	
4	45	Golomb and Baumert '65
5	161	Heule '18

- Showing $S(5) \leq 161$ was a massive SAT computation using cube and conquer
- 2-petabyte certificate
- Our goal: study Rado numbers using SAT solvers

Three-variable equations

- The equation $ax + by = cz$ gives bounds for other linear homogeneous equations

Three-variable equations

- The equation $ax + by = cz$ gives bounds for other linear homogeneous equations
- Two color numbers most popular, but no general formula for $R_2(ax + by = cz)$ known.

Three-variable equations

- The equation $ax + by = cz$ gives bounds for other linear homogeneous equations
- Two color numbers most popular, but no general formula for $R_2(ax + by = cz)$ known.
- Formulas for $R_2(ax - ay = bz)$ and $R_2(ax + ay = bz)$ (Harborth and Maasberg '97)

Three-variable equations

- The equation $ax + by = cz$ gives bounds for other linear homogeneous equations
- Two color numbers most popular, but no general formula for $R_2(ax + by = cz)$ known.
- Formulas for $R_2(ax - ay = bz)$ and $R_2(ax + ay = bz)$ (Harborth and Maasberg '97)
- Few values known for three or more colors

Three-variable equations

- The equation $ax + by = cz$ gives bounds for other linear homogeneous equations
- Two color numbers most popular, but no general formula for $R_2(ax + by = cz)$ known.
- Formulas for $R_2(ax - ay = bz)$ and $R_2(ax + ay = bz)$ (Harborth and Maasberg '97)
- Few values known for three or more colors

Theorem (Chang-De Loera-W '22)

1. $R_2(ax + by = cz)$ *for* $1 \leq a, b, c \leq 20$.
2. $R_3(a(x - y) = bz)$ *for* $1 \leq a, b \leq 15$.
3. $R_3(a(x + y) = bz)$ *for* $1 \leq a, b \leq 10$.
4. $R_3(ax + by = cz)$ *for* $1 \leq a, b, c \leq 6$.
5. $R_4(x - y = az)$ *for* $1 \leq a \leq 4$.
6. $R_4(a(x - y) = z)$ *for* $1 \leq a \leq 5$.

Patterns in $R_3(a(x-y)=bz)$

b \ a	1	2	3	4	5	6	7	8	9	10	11	12
1	14	14	27	64	125	216	343	512	729	1000	1331	1728
2	43	*14*	31	*14*	125	*27*	343	*64*	729	*125*	1331	*216*
3	94	61	*14*	73	125	*14*	343	512	*27*	1000	1331	*64*
4	173	*43*	109	*14*	141	*31*	343	*14*	729	*125*	1331	*27*
5	286	181	186	180	*14*	241	343	512	729	*14*	1331	1728
6	439	*94*	*43*	*61*	300	*14*	379	*73*	*31*	*125*	1331	*14*
7	638	428	442	456	470	462	*14*	561	729	1000	1331	1728
8	889	*173*	633	*43*	665	*109*	644	*14*	793	*141*	1331	*31*
9	1198	856	*94*	892	910	*61*	896	896	*14*	1081	1331	*73*
10	1571	*286*	1171	*181*	*43*	*186*	1190	*180*	1206	*14*	1431	*241*
11	2014	1508	1530	1552	1574	1596	1618	1584	1575	1580	*14*	1849
12	2533	*439*	*173*	*94*	2005	*43*	2053	*61*	*109*	*300*	2024	*14*

Patterns in $R_3(a(x-y)=bz)$

b \ a	1	2	3	4	5	6	7	8	9	10	11	12
1	14	14	27	64	125	216	343	512	729	1000	1331	1728
2	43	*14*	31	*14*	125	*27*	343	*64*	729	*125*	1331	*216*
3	94	61	*14*	73	125	*14*	343	512	*27*	1000	1331	*64*
4	173	*43*	109	*14*	141	*31*	343	*14*	729	*125*	1331	*27*
5	286	181	186	180	*14*	241	343	512	729	*14*	1331	1728
6	439	*94*	*43*	*61*	300	*14*	379	*73*	*31*	*125*	1331	*14*
7	638	428	442	456	470	462	*14*	561	729	1000	1331	1728
8	889	*173*	633	*43*	665	*109*	644	*14*	793	*141*	1331	*31*
9	1198	856	*94*	892	910	*61*	896	896	*14*	1081	1331	*73*
10	1571	*286*	1171	*181*	*43*	*186*	1190	*180*	1206	*14*	1431	*241*
11	2014	1508	1530	1552	1574	1596	1618	1584	1575	1580	*14*	1849
12	2533	*439*	*173*	*94*	2005	*43*	2053	*61*	*109*	*300*	2024	*14*

- $R_3(a(x-y)=bz)=a^3$ for $a \geq b+2$, $\gcd(a,b)=1$
- $R_3(a(x-y)=(a-1)z)=a^3+(a-1)^2$
- $R_3(x-y=bz)=(b+2)^3-(b+2)^2-(b+2)-1$

Patterns in $R_3(a(x-y)=bz)$

Theorem (Chang-De Loera-W '22)

- $R_3(a(x-y)=bz)=a^3$ for $a \geq b+2$, $a \geq 3$, $\gcd(a,b)=1$,
- $R_3(a(x-y)=(a-1)z)=a^3+(a-1)^2$ for $a \geq 3$,
- $R_3(x-y=bz)=(b+2)^3-(b+2)^2-(b+2)-1$ for $b \geq 1$.

Patterns in $R_3(a(x-y)=bz)$

Theorem (Chang-De Loera-W '22)

- $R_3(a(x-y)=bz)=a^3$ *for* $a \geq b+2$, $a \geq 3$, $\gcd(a,b)=1$,
- $R_3(a(x-y)=(a-1)z)=a^3+(a-1)^2$ *for* $a \geq 3$,
- $R_3(x-y=bz)=(b+2)^3-(b+2)^2-(b+2)-1$ *for* $b \geq 1$.

This theorem implies that the following result, conjectured by Ahmed and Schaal in 2016, on the *generalized Schur numbers* $S(k,m) := R_k(x_1+\cdots+x_{m-1}=x_m)$ is true:

Theorem (Boza,Marín,Revuelta,Sanz '19)

$S(3,m)=m^3-m^2-m-1.$

SAT encoding

- Given an equation $\mathcal{E}$, we construct a formula $F_n^k(\mathcal{E})$ that is satisfiable if and only if $R_k(\mathcal{E}) > n$.

SAT encoding

- Given an equation $\mathcal{E}$, we construct a formula $F_n^k(\mathcal{E})$ that is satisfiable if and only if $R_k(\mathcal{E}) > n$.
- The variables of $F_n^k(\mathcal{E})$ are $\{v_i^c\}$, $1 \le i \le n$, $1 \le c \le k$. The variable v_i^c is set to true if and only if the integer i has color c.

SAT encoding

- Given an equation $\mathcal{E}$, we construct a formula $F_n^k(\mathcal{E})$ that is satisfiable if and only if $R_k(\mathcal{E}) > n$.
- The variables of $F_n^k(\mathcal{E})$ are $\{v_i^c\}$, $1 \leq i \leq n$, $1 \leq c \leq k$. The variable v_i^c is set to true if and only if the integer i has color c.
- $F_n^k(\mathcal{E})$ has three types of clauses: positive, negative, and optional

SAT encoding

- Positive clauses encode that each integer is assigned at least one color, and take the form

$$v_i^1 \vee v_i^2 \vee \cdots \vee v_i^k$$

for all i

SAT encoding

- Positive clauses encode that each integer is assigned at least one color, and take the form

$$v_i^1 \vee v_i^2 \vee \cdots \vee v_i^k$$

for all i

- Negative clauses encode that there are no monochromatic solutions to $\mathcal{E}$. For each solution (x, y, z) and color c, we have the negative clause

$$\bar{v}_x^c \vee \bar{v}_y^c \vee \bar{v}_z^c$$

SAT encoding

- Positive clauses encode that each integer is assigned at least one color, and take the form

$$v_i^1 \vee v_i^2 \vee \cdots \vee v_i^k$$

  for all i

- Negative clauses encode that there are no monochromatic solutions to $\mathcal{E}$. For each solution (x, y, z) and color c, we have the negative clause

$$\bar{v}_x^c \vee \bar{v}_y^c \vee \bar{v}_z^c$$

- Optional clauses encode that each integer is assigned at most one color, and take the form

$$\bar{v}_i^c \vee \bar{v}_i^{c'}$$

  for all i and all colors $1 \leq c < c' \leq k$.

The clauses in the formula $F_4^3(x+y=z)$ are:
Positive clauses:

$$(v_1^1 \vee v_1^2 \vee v_1^3) \wedge (v_2^1 \vee v_2^2 \vee v_2^3) \wedge (v_3^1 \vee v_3^2 \vee v_3^3) \wedge (v_4^1 \vee v_4^2 \vee v_4^3)$$

Negative clauses:

$$(\overline{v}_1^1 \vee \overline{v}_1^1 \vee \overline{v}_2^1) \wedge (\overline{v}_2^1 \vee \overline{v}_1^1 \vee \overline{v}_3^1) \wedge (\overline{v}_3^1 \vee \overline{v}_1^1 \vee \overline{v}_4^1) \wedge$$
$$(\overline{v}_1^1 \vee \overline{v}_2^1 \vee \overline{v}_3^1) \wedge (\overline{v}_2^1 \vee \overline{v}_2^1 \vee \overline{v}_4^1) \wedge (\overline{v}_1^1 \vee \overline{v}_3^1 \vee \overline{v}_4^1) \wedge$$
$$(\overline{v}_1^2 \vee \overline{v}_1^2 \vee \overline{v}_2^2) \wedge (\overline{v}_2^2 \vee \overline{v}_1^2 \vee \overline{v}_3^2) \wedge (\overline{v}_3^2 \vee \overline{v}_1^2 \vee \overline{v}_4^2) \wedge$$
$$(\overline{v}_1^2 \vee \overline{v}_2^2 \vee \overline{v}_3^2) \wedge (\overline{v}_2^2 \vee \overline{v}_2^2 \vee \overline{v}_4^2) \wedge (\overline{v}_1^2 \vee \overline{v}_3^2 \vee \overline{v}_4^2) \wedge$$
$$(\overline{v}_1^3 \vee \overline{v}_1^3 \vee \overline{v}_2^3) \wedge (\overline{v}_2^3 \vee \overline{v}_1^3 \vee \overline{v}_3^3) \wedge (\overline{v}_3^3 \vee \overline{v}_1^3 \vee \overline{v}_4^3) \wedge$$
$$(\overline{v}_1^3 \vee \overline{v}_2^3 \vee \overline{v}_3^3) \wedge (\overline{v}_2^3 \vee \overline{v}_2^3 \vee \overline{v}_4^3) \wedge (\overline{v}_1^3 \vee \overline{v}_3^3 \vee \overline{v}_4^3)$$

Optional clauses:

$$(\overline{v}_1^1 \vee \overline{v}_1^2) \wedge (\overline{v}_1^1 \vee \overline{v}_1^3) \wedge (\overline{v}_1^2 \vee \overline{v}_1^3) \wedge (\overline{v}_2^1 \vee \overline{v}_2^2) \wedge (\overline{v}_2^1 \vee \overline{v}_2^3) \wedge (\overline{v}_2^2 \vee \overline{v}_2^3) \wedge$$
$$(\overline{v}_3^1 \vee \overline{v}_3^2) \wedge (\overline{v}_3^1 \vee \overline{v}_3^3) \wedge (\overline{v}_3^2 \vee \overline{v}_3^3) \wedge (\overline{v}_4^1 \vee \overline{v}_4^2) \wedge (\overline{v}_4^1 \vee \overline{v}_4^3) \wedge (\overline{v}_4^2 \vee \overline{v}_4^3)$$

SAT solving

- For each equation $\mathcal{E}$ we produced the satisfiable formula $F^k_{n-1}(\mathcal{E})$ and unsatisfiable formula $F^k_n(\mathcal{E})$ to prove $R_k(\mathcal{E}) = n$

SAT solving

- For each equation $\mathcal{E}$ we produced the satisfiable formula $F_{n-1}^{k}(\mathcal{E})$ and unsatisfiable formula $F_{n}^{k}(\mathcal{E})$ to prove $R_k(\mathcal{E}) = n$
- Guess lower and upper bounds for n, then use binary search to determine n

SAT solving

- For each equation $\mathcal{E}$ we produced the satisfiable formula $F_{n-1}^k(\mathcal{E})$ and unsatisfiable formula $F_n^k(\mathcal{E})$ to prove $R_k(\mathcal{E}) = n$
- Guess lower and upper bounds for n, then use binary search to determine n
- Solving is relatively fast for two or three colors (≤ 1 min for most formulas)

SAT solving

- For each equation $\mathcal{E}$ we produced the satisfiable formula $F^k_{n-1}(\mathcal{E})$ and unsatisfiable formula $F^k_n(\mathcal{E})$ to prove $R_k(\mathcal{E}) = n$
- Guess lower and upper bounds for n, then use binary search to determine n
- Solving is relatively fast for two or three colors (≤ 1 min for most formulas)
- Four color formulas require symmetry breaking and more time

SAT solving

- For each equation $\mathcal{E}$ we produced the satisfiable formula $F^k_{n-1}(\mathcal{E})$ and unsatisfiable formula $F^k_n(\mathcal{E})$ to prove $R_k(\mathcal{E}) = n$
- Guess lower and upper bounds for n, then use binary search to determine n
- Solving is relatively fast for two or three colors (≤ 1 min for most formulas)
- Four color formulas require symmetry breaking and more time
- Modified encoding to compute **infinitely** many values with a single formula

SAT solving

Example: $R_2(x+3y=3z)=9$.

SAT solving

Example: $R_2(x + 3y = 3z) = 9$.

- Don't need *all* the integers 1 to 9:

Example: $R_2(x + 3y = 3z) = 9$.

- Don't need *all* the integers 1 to 9:
- Suppose 4 is red. Then since $(6, 4, 6)$ is a solution, 6 must be blue.

SAT solving

Example: $R_2(x + 3y = 3z) = 9$.

- Don't need *all* the integers 1 to 9:
- Suppose 4 is red. Then since $(6, 4, 6)$ is a solution, 6 must be blue.
- (9,6,9) and (3,3,4) are solutions, so 9 must be red and 3 must be blue.

Example: $R_2(x+3y=3z)=9$.

- Don't need *all* the integers 1 to 9:
- Suppose 4 is red. Then since $(6,4,6)$ is a solution, 6 must be blue.
- (9,6,9) and (3,3,4) are solutions, so 9 must be red and 3 must be blue.
- But (3,6,7) and (9,4,7) are solutions, so 7 can't be either color.

SAT solving

Example: $R_2(x + 3y = 3z) = 9$.

- Don't need *all* the integers 1 to 9:
- Suppose 4 is red. Then since $(6, 4, 6)$ is a solution, 6 must be blue.
- (9,6,9) and (3,3,4) are solutions, so 9 must be red and 3 must be blue.
- But (3,6,7) and (9,4,7) are solutions, so 7 can't be either color.
- Only needed to use the numbers in $S = \{3, 4, 6, 7, 9\}$

SAT solving

Example: $R_2(x + 3y = 3z) = 9$.

- Don't need *all* the integers 1 to 9:
- Suppose 4 is red. Then since $(6, 4, 6)$ is a solution, 6 must be blue.
- (9,6,9) and (3,3,4) are solutions, so 9 must be red and 3 must be blue.
- But (3,6,7) and (9,4,7) are solutions, so 7 can't be either color.
- Only needed to use the numbers in $S = \{3, 4, 6, 7, 9\}$
- Want to describe sets S that work for an *entire family* of equations

2-color Generalized Schur Numbers

Example: $R_2(x + (a-2)y = z) = a^2 - a - 1$ for all $a \geq 3$.

Example: $R_2(x + (a-2)y = z) = a^2 - a - 1$ for all $a \geq 3$.

- Let $S = \{1, a-1, a, a^2 - 2a + 1, a^2 - a - 1\}$

2-color Generalized Schur Numbers

Example: $R_2(x + (a-2)y = z) = a^2 - a - 1$ for all $a \geq 3$.

- Let $S = \{1, a-1, a, a^2 - 2a + 1, a^2 - a - 1\}$
- Suppose 1 is red.

2-color Generalized Schur Numbers

Example: $R_2(x + (a-2)y = z) = a^2 - a - 1$ for all $a \geq 3$.

- Let $S = \{1, a-1, a, a^2-2a+1, a^2-a-1\}$
- Suppose 1 is red.
- $(1, 1, a-1)$ is a solution, so $a-1$ is blue.

2-color Generalized Schur Numbers

Example: $R_2(x + (a-2)y = z) = a^2 - a - 1$ for all $a \geq 3$.

- Let $S = \{1, a-1, a, a^2 - 2a + 1, a^2 - a - 1\}$
- Suppose 1 is red.
- $(1, 1, a-1)$ is a solution, so $a - 1$ is blue.
- $(a-1, a-1, a^2 - 2a + 1)$ is a solution, so $a^2 - 2a + 1$ is red.

2-color Generalized Schur Numbers

Example: $R_2(x + (a-2)y = z) = a^2 - a - 1$ for all $a \geq 3$.

- Let $S = \{1, a-1, a, a^2 - 2a + 1, a^2 - a - 1\}$
- Suppose 1 is red.
- $(1, 1, a-1)$ is a solution, so $a - 1$ is blue.
- $(a-1, a-1, a^2 - 2a + 1)$ is a solution, so $a^2 - 2a + 1$ is red.
- $(a^2 - 2a + 1, 1, a^2 - a - 1)$ is a solution, so $a^2 - a - 1$ is blue.

2-color Generalized Schur Numbers

Example: $R_2(x+(a-2)y=z)=a^2-a-1$ for all $a\geq 3$.

- Let $S=\{1,a-1,a,a^2-2a+1,a^2-a-1\}$
- Suppose 1 is red.
- $(1,1,a-1)$ is a solution, so $a-1$ is blue.
- $(a-1,a-1,a^2-2a+1)$ is a solution, so a^2-2a+1 is red.
- $(a^2-2a+1,1,a^2-a-1)$ is a solution, so a^2-a-1 is blue.
- $(1,a,a^2-2a+1)$ and $(a-1,a,a^2-a-1)$ are solutions, so a cannot be either color.

Upper bounds: Variables indexed by polynomials

- Can prove upper bounds by generating a formula in the same way: negative clauses look like

$$\overline{v_1}^1 \vee \overline{v_a}^1 \vee \overline{v}^1_{a^2-2a+1}.$$

- Set S describes an unsatisfiable core for an equation

Upper bounds: Variables indexed by polynomials

- Can prove upper bounds by generating a formula in the same way: negative clauses look like

$$\overline{v_1}^1 \vee \overline{v_a}^1 \vee \overline{v}^1_{a^2-2a+1}.$$

- Set S describes an unsatisfiable core for an equation
- Found suitable S for our Rado number families:

$\mathcal{E}$	$R_3(\mathcal{E})$	$\lvert S \rvert$
$x - y = (b-2)z$	$b^3 - b^2 - b - 1$	685
$a(x-y) = (a-1)z$	$a^3 + (a-1)^2$	1365
$a(x-y) = bz$	a^3	40645

Current work

- Conjecture: $R_4(x_1 + \cdots + x_{m-1} = x_m) = m^4 - m^3 - m^2 - m - 1$ for $m \geq 4$

Current work

- Conjecture: $R_4(x_1 + \cdots + x_{m-1} = x_m) = m^4 - m^3 - m^2 - m - 1$ for $m \geq 4$
- Refine methods to find unsatisfiable cores for Rado numbers

Current work

- Conjecture: $R_4(x_1 + \cdots + x_{m-1} = x_m) = m^4 - m^3 - m^2 - m - 1$ for $m \geq 4$
- Refine methods to find unsatisfiable cores for Rado numbers
- Application to other families of Rado numbers (nonhomogeneous, nonlinear, etc.)

Current work

- Conjecture: $R_4(x_1 + \cdots + x_{m-1} = x_m) = m^4 - m^3 - m^2 - m - 1$ for $m \geq 4$
- Refine methods to find unsatisfiable cores for Rado numbers
- Application to other families of Rado numbers (nonhomogeneous, nonlinear, etc.)
- General formula for $R_2(ax + by = cz)$

Current work

- The largest k for which $R_k(\mathcal{E})$ is finite (k-regular) is called the degree of regularity of $\mathcal{E}$.

Current work

- The largest k for which $R_k(\mathcal{E})$ is finite (k-regular) is called the degree of regularity of $\mathcal{E}$.

Theorem (Chang-De Loera-W '22)

The degree of regularity for the equation $ax + by + cz = 0$ *is known for* $1 \leq |a|, |b|, |c| \leq 5$.

Current work

- The largest k for which $R_k(\mathcal{E})$ is finite (k-regular) is called the degree of regularity of $\mathcal{E}$.

Theorem (Chang-De Loera-W '22)

The degree of regularity for the equation $ax + by + cz = 0$ is known for $1 \leq |a|, |b|, |c| \leq 5$.

Conjecture (Rado's Boundedness Conjecture)

For all linear homogeneous equations $\mathcal{E}$ in m variables, there is a value $\Delta = \Delta(m)$ such that if $\mathcal{E}$ is Δ-regular, then $\mathcal{E}$ is regular.

- Fox and Kleitman proved $\Delta = 24$ suffices for $m = 3$, but unknown if this can be improved

Current work

- The largest k for which $R_k(\mathcal{E})$ is finite (k-regular) is called the degree of regularity of $\mathcal{E}$.

Theorem (Chang-De Loera-W '22)

The degree of regularity for the equation $ax + by + cz = 0$ is known for $1 \leq |a|, |b|, |c| \leq 5$.

Conjecture (Rado's Boundedness Conjecture)

For all linear homogeneous equations $\mathcal{E}$ in m variables, there is a value $\Delta = \Delta(m)$ such that if $\mathcal{E}$ is Δ-regular, then $\mathcal{E}$ is regular.

- Fox and Kleitman proved $\Delta = 24$ suffices for $m = 3$, but unknown if this can be improved
- Is there an equation $\mathcal{E}$ of the form $ax + by + cz = 0$ with degree of regularity 4?

Polynomial encodings

Given an equation $\mathcal{E}$ and number of colors k, let S_n be the set of solutions to $\mathcal{E}$ where each variable is in $\{1, \ldots, n\}$.
The following system of equations has no solution over $\overline{\mathbb{F}_2}$ if and only if $R_k(\mathcal{E}) \leq n$:

$$
\begin{aligned}
\prod_{s \in S_n} x_{s,c} &= 0 && 1 \leq c \leq k, \\
1 + \sum_{c=1}^{k} x_{i,c} &= 0 && 1 \leq i \leq n, \\
x_{i,c} x_{i,c'} &= 0 && 1 \leq c < c' \leq k.
\end{aligned}
$$

Polynomial encodings

The following system of equations has no solution over $\overline{\mathbb{F}_2}$ if and only if $R_2(x + y = z) \leq 5$:

$$
\begin{aligned}
x_1x_2 &= 0, & y_1y_2 &= 0,\\
x_2x_4 &= 0, & y_2y_4 &= 0,\\
x_1x_2x_3 &= 0, & y_1y_2y_3 &= 0,\\
x_1x_3x_4 &= 0, & y_1y_3y_4 &= 0,\\
x_1x_4x_5 &= 0, & y_1y_4y_5 &= 0,\\
x_2x_3x_5 &= 0, & y_2y_3y_5 &= 0,\\
1 + x_i + y_i &= 0, & 1 \leq i &\leq 5.
\end{aligned}
$$

Hilbert's Nullstellensatz

Theorem (Hilbert, 1893)

Let K be an algebraically closed field, and let $f_1, \dots, f_m \in K[x_1, \dots, x_n]$. Then there is no solution to the system $f_1 = \cdots = f_m = 0$ if and only if there exist polynomials $\beta_1, \dots, \beta_m$ such that $\sum_{i=1}^{m} \beta_i f_i = 1$.

Hilbert's Nullstellensatz

Theorem (Hilbert, 1893)

Let K be an algebraically closed field, and let $f_1, \ldots, f_m \in K[x_1, \ldots, x_n]$. Then there is no solution to the system $f_1 = \cdots = f_m = 0$ if and only if there exist polynomials $\beta_1, \ldots, \beta_m$ such that $\sum_{i=1}^{m} \beta_i f_i = 1$.

The identity $\sum_{i=1}^{m} \beta_i f_i = 1$ is called a *Nullstellensatz certificate*.

Hilbert's Nullstellensatz

Theorem (Hilbert, 1893)

Let K be an algebraically closed field, and let $f_1, \ldots, f_m \in K[x_1, \ldots, x_n]$. Then there is no solution to the system $f_1 = \cdots = f_m = 0$ if and only if there exist polynomials $\beta_1, \ldots, \beta_m$ such that $\sum_{i=1}^{m} \beta_i f_i = 1$.

The identity $\sum_{i=1}^{m} \beta_i f_i = 1$ is called a *Nullstellensatz certificate*.

The *degree* of the certificate is the maximum degree of the β_i.

Hilbert's Nullstellensatz

Theorem (Hilbert, 1893)

Let K be an algebraically closed field, and let $f_1, \ldots, f_m \in K[x_1, \ldots, x_n]$. Then there is no solution to the system $f_1 = \cdots = f_m = 0$ if and only if there exist polynomials $\beta_1, \ldots, \beta_m$ such that $\sum_{i=1}^{m} \beta_i f_i = 1$.

The identity $\sum_{i=1}^{m} \beta_i f_i = 1$ is called a *Nullstellensatz certificate*.

The *degree* of the certificate is the maximum degree of the β_i.

Goal: describe Nullstellensatz certificates for Rado numbers

Online Ramsey numbers

Consider the following game between the two players **Builder** and **Painter**:

- Fix an equation $\mathcal{E}$ and positive integers k and n.

Online Ramsey numbers

Consider the following game between the two players **Builder** and **Painter**:

- Fix an equation $\mathcal{E}$ and positive integers k and n.
- Builder and Painter take turns where Builder selects an integer in $\{1, \ldots, n\}$ and Painter assigns it one of k colors.

Online Ramsey numbers

Consider the following game between the two players **Builder** and **Painter**:

- Fix an equation $\mathcal{E}$ and positive integers k and n.
- Builder and Painter take turns where Builder selects an integer in $\{1, \ldots, n\}$ and Painter assigns it one of k colors.
- Builder wins when there is a monochromatic solution to $\mathcal{E}$.

Online Ramsey numbers

Consider the following game between the two players **Builder** and **Painter**:

- Fix an equation $\mathcal{E}$ and positive integers k and n.
- Builder and Painter take turns where Builder selects an integer in $\{1, \ldots, n\}$ and Painter assigns it one of k colors.
- Builder wins when there is a monochromatic solution to $\mathcal{E}$.
- The number $\tilde{R}_k(\mathcal{E}; n)$ is the smallest number of turns for which Builder is guaranteed victory.

Online Ramsey numbers

Consider the following game between the two players **Builder** and **Painter**:

- Fix an equation $\mathcal{E}$ and positive integers k and n.
- Builder and Painter take turns where Builder selects an integer in $\{1, \ldots, n\}$ and Painter assigns it one of k colors.
- Builder wins when there is a monochromatic solution to $\mathcal{E}$.
- The number $\tilde{R}_k(\mathcal{E}; n)$ is the smallest number of turns for which Builder is guaranteed victory.
- Builder always wins if $n \geq R_k(\mathcal{E})$.

Online Ramsey numbers

Consider the following game between the two players **Builder** and **Painter**:

- Fix an equation $\mathcal{E}$ and positive integers k and n.
- Builder and Painter take turns where Builder selects an integer in $\{1, \ldots, n\}$ and Painter assigns it one of k colors.
- Builder wins when there is a monochromatic solution to $\mathcal{E}$.
- The number $\tilde{R}_k(\mathcal{E}; n)$ is the smallest number of turns for which Builder is guaranteed victory.
- Builder always wins if $n \geq R_k(\mathcal{E})$.
- Example: $\tilde{R}_2(x + 3y = 3z; 9) \leq 5$ (Builder can choose from $\{3, 4, 6, 7, 9\}$ and win)

Online Ramsey numbers

Theorem (De Loera-W)

Using the previous encoding, there exists a Nullstellensatz certificate of degree at most $\tilde{R}_k(\mathcal{E}; n)$ *for* $n = R_k(\mathcal{E})$.

Online Ramsey numbers

Theorem (De Loera-W)

Using the previous encoding, there exists a Nullstellensatz certificate of degree at most $\tilde{R}_k(\mathcal{E}; n)$ for $n = R_k(\mathcal{E})$.

This theorem and encoding generalize!

- Ramsey numbers (multicolor, arbitrary graphs)
- Schur and Rado numbers
- van der Waerden numbers
- Hales-Jewett numbers

Future work

- Find lower bounds for the degrees of Nullstellensatz certificates in this encoding. Are online Ramsey-type numbers good bounds?
- The inequalities

  min Nullstellensatz degree $\leq$ online Rado number $\leq$ Rado number

  are strict in general

Future work

- Find lower bounds for the degrees of Nullstellensatz certificates in this encoding. Are online Ramsey-type numbers good bounds?
- The inequalities

  min Nullstellensatz degree $\leq$ online Rado number $\leq$ Rado number

  are strict in general
- Investigate the analogous Builder-Painter game for other problems (Schur numbers, van der Waerden numbers, Ramsey numbers for other graphs)

Thank you!

References:

- (with Yuan Chang and Jesús De Loera) **Rado Numbers and SAT Computations**, Proceedings of the International Symposium on Symbolic and Algebraic Computation, ISSAC, 2022, pp. 333–342, https://dl.acm.org/doi/10.1145/3476446.3535494
- (with Jesús De Loera) **Ramsey Numbers through the Lenses of Polynomial Ideals and Nullstellensätze** https://arxiv.org/abs/2209.13859