Partition regularity of Diophantine equations

VUW Discrete Mathematics Seminar

Jordan Mitchell Barrett

Victoria University of Wellington

math@jmbarrett.nz
https://jmbarrett.nz/

29th April 2021

Ramsey theory

- Studies what kinds of regular configurations can be found in (finite partitions/colourings of) infinite/sufficiently large finite structures.
- First Ramsey-type result was proven by Hilbert in 1892[1]
  - Used this to prove Hilbert's irreducibility theorem
- Named after Ramsey's seminal 1930 theorem
  - Used it to prove decidability of an instance of SAT
  - Many different flavours (finite, infinite, sets, graphs, etc...)

Theorem (Ramsey, 1930, infinite combinatorial version)[2]

Fix $m, r \in \mathbb{N}$. Then, for every r-colouring of $\mathcal{P}(\mathbb{N})$, there exists some infinite $A \subseteq \mathbb{N}$ such that the family $\{B \subseteq A : |B| = m\}$ is monochromatic.

---

[1] D. Hilbert. Über die Irreduzibilität ganzer rationaler Funktionen mit ganzzahligen Koeffizienten. *J. Reine Angew. Math.* **110** (1892), pp. 104–129

[2] F. P. Ramsey. On a problem of formal logic. *Proceedings of the London Mathematical Society* **s2-30.1** (1930), pp. 264–286

Partition regularity

Notation

Let $\mathbf{x} = (x_1, \ldots, x_n)$ be a tuple, and $P(\mathbf{x}) \in \mathbb{Z}[\mathbf{x}]$ be a (multivariate) polynomial over $\mathbb{Z}$. We say that $P(\mathbf{x}) = 0$ is a *Diophantine equation*.

Definition (partition regularity)

We say that a Diophantine equation $P(\mathbf{x}) = 0$ is *partition regular* (abbreviated p.r.) if for any finite partition $\mathbb{N} = C_0 \sqcup \cdots \sqcup C_{k-1}$, there exists $i \in k$ and $\mathrm{m} = (m_1, \ldots, m_n) \in C_i^n$ such that $P(\mathrm{m}) = 0$.

Alternative definition

$P(\mathbf{x}) = 0$ is *partition regular* if for any finite colouring $c : \mathbb{N} \to k$, there exists $m_1, \ldots, m_n \in \mathbb{N}$ such that $c(m_1) = \cdots = c(m_n)$ and $P(\mathrm{m}) = 0$.

These two definitions are equivalent under $c(n) = j \iff n \in C_j$.

Early results

Example (Schur, 1917)[3]

The equation $x + y = z$ is partition regular.

Example (van der Waerden, 1927)[4]

Fix $m, r \in \mathbb{N}$. Then, for every r-colouring $c : \mathbb{N} \to r$, there exists a c-monochromatic arithmetic progression of length m.

Example (Rado, 1933)[5]

A linear Diophantine equation $\sum_{k=1}^{n} a_k x_k = 0$ is partition regular iff there exists a nonempty subset $I \subseteq \{1, \ldots, n\}$ such that $\sum_{i \in I} a_i = 0$.

---

[3] I. Schur. Über die Kongruenz $x^m + y^m \equiv z^m (\bmod p)$. *Jahresbericht der Deutschen Mathematiker-Vereinigung* **25** (1917), pp. 114–117

[4] B. L. van der Waerden. Beweis einer Baudetschen Vermutung. *Nieuw Archief voor Wiskunde* **15** (1927), pp. 212–216

[5] R. Rado. Studien zur Kombinatorik. *Math. Z.* **36.1** (1933), pp. 424–470

Nonlinear equations

- Linear homogeneous case totally settled by Rado
- Nonlinear case has proved much harder - progress has been sporadic

Example (multiplicative Rado's theorem)

The equation $\prod_{k=1}^{n} x_k^{a_k} = 1$ is p.r. iff "Rado's condition" holds: there exists a nonempty subset $I \subseteq \{1, \dots, n\}$ such that $\sum_{i \in I} a_i = 0$.

Example (Lefmann, 1991)[6]

The equation $\sum_{j=1}^{n} a_j x_j^{1/k} = 0$ is p.r. iff Rado's condition holds.

Example (Bergelson, 1996)[7]

If $P(z) \in \mathbb{Z}[z]$ has no constant term, then $x - y = P(z)$ is p.r..

---

[6] H. Lefmann. On p.r. systems of equations. *JCTA* **58.1** (1991), pp. 35–53

[7] V. Bergelson. Ergodic Ramsey theory – an update. *Ergodic Theory of $\mathbb{Z}^d$-actions, London Math. Soc. Lecture Note Series* **228** (1996), pp. 1–61

Nonstandard analysis

- Developed by Abraham Robinson in the 60s to rigorously formalise calculus/analysis in terms of infinitesimal numbers
- Recently has been used successfully in Ramsey theory[8]
- Assign to every object of discourse M a "nonstandard extension" ${}^*M$, satisfying nice properties
  - $A \subseteq B \implies {}^*A \subseteq {}^*B$
  - $f\colon A \to B \implies {}^*f\colon {}^*A \to {}^*B$ and ${}^*f$ extends f
  - ${}^*n = n$ for all $n \in \mathbb{N}$.
- ${}^*\mathbb{N}$ is the "hypernaturals": add "infinite elements" to $\mathbb{N}$
- Transfer: for "elementary properties"[9] $\varphi(x_1, \ldots, x_n)$,

$$\varphi(M_1, \ldots, M_n) \iff \varphi({}^*M_1, \ldots, {}^*M_n)$$

---

[8] M. Di Nasso, I. Goldbring & M. Lupini. *Nonstandard Methods in Ramsey Theory and Combinatorial Number Theory*. 1st ed. Springer, Cham (2019)

[9] All quantifiers are $\in$-bounded, i.e. of the form $Q\,x \in y$.

Ultrafilters

- Recall: an *ultrafilter on* $\mathbb{N}$ is a family of subsets $\mathcal{U} \subseteq \mathcal{P}(\mathbb{N})$ such that:
  - $\varnothing \notin \mathcal{U}$
  - $\mathbb{N} \in \mathcal{U}$
  - $A \in \mathcal{U}$, $B \supseteq A \implies B \in \mathcal{U}$
  - $A, B \in \mathcal{U} \implies A \cap B \in \mathcal{U}$
  - For every $A \subseteq \mathbb{N}$, either $A \in \mathcal{U}$ or $A^{\complement} \in \mathcal{U}$
- Ultrafilters define a notion of *largeness* for subsets of $\mathbb{N}$: $A \in \mathcal{U}$ means A is large according to $\mathcal{U}$.
  - Can also be characterised as finitely additive $\{0, 1\}$-valued measures
- Each hypernatural number $\alpha \in {}^*\mathbb{N}$ generates an ultrafilter on $\mathbb{N}$ in a natural way:

$$\alpha \mapsto \mathcal{U}_\alpha = \{A \subseteq \mathbb{N} : \alpha \in {}^*A\}$$

u-equivalence

- Each hypernatural number $\alpha \in {}^*\mathbb{N}$ generates an ultrafilter on $\mathbb{N}$ in a natural way:

$$\alpha \mapsto \mathcal{U}_\alpha = \{A \subseteq \mathbb{N} : \alpha \in {}^*A\}$$

- This map is surjective but **not** injective, thus:

Definition (u-equivalence)

We say two hypernatural numbers $\zeta, \xi \in {}^*\mathbb{N}$ are *u-equivalent*, sometimes denoted $\zeta \sim \xi$, if they generate the same ultrafilter $\mathcal{U}_\zeta = \mathcal{U}_\xi$.

Polynomial Bridge Theorem (Luperi Baglini, 2012)[10]

The equation $f(\mathbf{x}) = 0$ is partition regular if and only if there exist u-equivalent $\xi_1 \sim \cdots \sim \xi_n \in {}^*\mathbb{N}$ such that $f(\xi_1, \ldots, \xi_n) = 0$.

[10] L. Luperi Baglini. Hyperintegers and nonstandard techniques in combinatorics of numbers. *PhD thesis, University of Siena* (2012). https://arxiv.org/abs/1212.2049

Applications of u-equivalence

- u-equivalence is quite a strong property: $\zeta \sim \xi$ implies:
  - For any first-order formula $\varphi(x)$, $\varphi(\zeta)$ holds iff $\varphi(\xi)$ holds.
  - For any $A \subseteq \mathbb{N}$, $\zeta \in {}^*A$ if and only if $\xi \in {}^*A$.

Proposition (Di Nasso, 2015)[11]

1. If $\zeta \in {}^*\mathbb{N}$, $k \in \mathbb{N}$, then $\zeta \sim k \iff \zeta = k$.
2. For every $f : \mathbb{N} \to \mathbb{N}$, if $\zeta \sim \xi$, then ${}^*f(\zeta) \sim {}^*f(\xi)$.
3. For every $f : \mathbb{N} \to \mathbb{N}$, $\zeta \in {}^*\mathbb{N}$, ${}^*f(\zeta) \sim \zeta \implies {}^*f(\zeta) = \zeta$.

- In particular, $\zeta \sim \xi$ implies that:
  - $\zeta \equiv \xi \mod n$ for any $n \in \mathbb{N}$;
  - Fixing prime p and writing $\zeta = p^\alpha \zeta_0$, $\xi = p^\beta \xi_0$, we have that $\alpha \sim \beta$ and $\zeta_0 \sim \xi_0$;
  - If $\sigma, \tau \in {}^*\mathbb{N}$ are the largest s.t. $p^\sigma \leq \zeta$, $p^\tau \leq \xi$, then $\sigma \sim \tau$.

[11] M. Di Nasso. *Hypernatural numbers as ultrafilters*. *Nonstandard Analysis for the Working Mathematician. Springer, Dordrecht* (2015), pp. 443–474

A nonstandard proof of non-p.r.

Example (Di Nasso & Riggio, 2018)[12]

The equation $x^2 + y^2 = z$ is not partition regular.

Proof (Di Nasso, Goldbring & Lupini, 2019)[13]

Suppose, by contradiction, that it is partition regular, and fix $\alpha \sim \beta \sim \gamma \in {}^*\mathbb{N}$ such that $\alpha^2 + \beta^2 = \gamma$. Since $x^2 + y^2 = z$ doesn't admit constant solutions, we must have $\alpha, \beta, \gamma \in {}^*\mathbb{N} \setminus \mathbb{N}$. We can't have α, β, γ all odd, so they must all be even. Write

$$\alpha = 2^a \alpha_0, \quad \beta = 2^b \beta_0, \quad \gamma = 2^c \gamma_0$$

for **positive** $a \sim b \sim c$, and **odd** $\alpha_0 \sim \beta_0 \sim \gamma_0$.

---

[12] M. Di Nasso & M. Riggio. Fermat-like equations that are not partition regular. *Combinatorica* **38.5** (2018), pp. 1067–1078

[13] M. Di Nasso, I. Goldbring & M. Lupini. *Nonstandard Methods in Ramsey Theory and Combinatorial Number Theory*. 1st ed. Springer, Cham (2019)

A nonstandard proof of non-p.r. (cont.)

Example

The equation $x^2 + y^2 = z$ is not partition regular.

Proof (cont.)

We have **positive** $a \sim b \sim c$, **odd** $\alpha_0 \sim \beta_0 \sim \gamma_0$, and

$$2^{2a}\alpha_0^2 + 2^{2b}\beta_0^2 = 2^c\gamma_0$$

Case 1: $a < b$: then $2^{2a}(\alpha_0^2 + 2^{2b-2a}\beta_0^2) = 2^c\gamma_0$. Since γ_0 and $(\alpha_0^2 + 2^{2b-2a}\beta_0^2)$ are both odd, we must have $2a = c \sim a$, so $2a = a \implies a = 0 \implies$ contradiction.

Case 2: $a = b$: then $2^{2a}(\alpha_0^2 + \beta_0^2) = 2^c\gamma_0$. We have $\alpha_0^2 + \beta_0^2 \equiv 2 \bmod 4$, so $2^{2a+1}\zeta = 2^c\gamma_0$ for odd ζ. Then $2a + 1 = c \sim a$, so $2a + 1 = a \implies$ contradiction. $\square$

- This kind of argument only works for inhom. equations.

Results obtained

- Nonstandard approach useful for proving non-p.r. of equations

Example (Di Nasso & Riggio, 2018)[14]

Fix odd $m \in \mathbb{N}$. If $a_1, \ldots, a_m \in \mathbb{N}$ are all odd, and $n_1, \ldots, n_m \in \mathbb{N}$ are all distinct, then the equation $\sum_{i=1}^{m} a_i x_i^{n_i} = 0$ is not partition regular.

Example (Di Nasso & Riggio, 2018)[14]

If $k \notin \{n, m\}$, then the equation $x^n + y^m = z^k$ is not partition regular.

Example (Di Nasso & Luperi Baglini, 2018)[15]

Fix $d \neq k$. If $P(y)$ is a polynomial of degree d with no constant term, and Rado's condition is not satisfied, then $\sum_{i=1}^{n} c_i x_i^k = P(y)$ is not p.r..

---

[14] M. Di Nasso & M. Riggio. Fermat-like equations that are not partition regular. *Combinatorica* **38.5** (2018), pp. 1067–1078

[15] M. Di Nasso & L. Luperi Baglini. Ramsey properties of nonlinear Diophantine equations. *Advances in Mathematics* **324** (2018), pp. 84–117

Our idea

Notation

A *multi-index* is a tuple $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}_0^n$. We then define $\mathbf{x}^\alpha := x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$. e.g. $\alpha = (3, 0, 2) \implies \mathbf{x}^\alpha = x^3 y^0 z^2 = x^3 z^2$.

Remark

Any polynomial $P(\mathbf{x}) \in \mathbb{Z}[\mathbf{x}]$ can be written as $P(\mathbf{x}) = \sum_\alpha c_\alpha \mathbf{x}^\alpha$.

Idea

Fix $\xi_1 \sim \cdots \sim \xi_n$ such that $P(\xi_1, \ldots, \xi_n) = 0$. Consider $\tau_i := \mathrm{Lg}_p(\xi_i)$, i.e. $\xi_i = p^{\tau_i} \sigma_i$, with $1 \leq \sigma_i < p$. As before, we have $\tau_1 \sim \cdots \sim \tau_n$ and $\sigma_1 \sim \cdots \sim \sigma_n$. Then:

$$P(\boldsymbol{\xi}) \;=\; \sum_\alpha c_\alpha \boldsymbol{\sigma}^\alpha p^{\boldsymbol{\tau} \cdot \alpha} \;\approx\; \sum_\alpha c_\alpha w^{|\alpha|} p^{\boldsymbol{\tau} \cdot \alpha}$$

Then we can *partition* the indices $\{\alpha\}$ based on their size $p^{\boldsymbol{\tau} \cdot \alpha}$.

Our contributions

Theorem (Barrett, Lupini & Moreira, 2019)[16]

If $P(\mathbf{x}) = 0$ is p.r., then it admits such a partition $J_0 > \cdots > J_\ell$. Furthermore, we can show that the polynomial

$$w \mapsto \sum_{i=0}^{m} p^{d_i} \sum_{\alpha \in J_i} c_\alpha w^{|\alpha|}$$

has a root in $[1, p]$, where $d_i = (\boldsymbol{\tau} \cdot J_i) - (\boldsymbol{\tau} \cdot J_0)$.

Example

The equations $x^2 - xy + ax + by + cz$ and $x^2 - y^2 + ax + by + cz$ both satisfy the above (*"maximal Rado condition"*) if $abc = 0$, or if $a + b + c = 0$.

[16] J. M. Barrett, M. Lupini & J. Moreira. On Rado conditions for nonlinear Diophantine equations. *European Journal of Combinatorics* **94C** (2021)

Our contributions II

- Write $\xi_i = p^{\nu_i}\zeta_i$ where $p \nmid \zeta_i$, partition indices $\{\alpha\}$ by $p^{\boldsymbol{\nu}\cdot\alpha}$.

Theorem (Barrett, Lupini & Moreira, 2019)[17]

If $P(\mathbf{x}) = 0$ is p.r.[18], then for every prime $p \in \mathbb{N}$, it admits such a partition $J_0 > \cdots > J_\ell$, and there exists $a \in \mathbb{Z}$ such that $P(a, \ldots, a) = 0$ and

$$w \;\mapsto\; \sum_{i=0}^{m} p^{d_i} \sum_{\alpha \in J_i} c_\alpha^a w^{|\alpha|}$$

has a solution $w \in {}^*\mathbb{N}$ with $w \not\equiv 0 \bmod p$. Here, c_α^a are the coefficients of $P^a(\mathbf{x}) = P(\mathbf{x} + a)$.

Example

$(x-y)^2 + (x-a)(y-b) = 0$ is not p.r. for any constants $a, b \in \mathbb{Z}$.

---

[18] J. M. Barrett, M. Lupini & J. Moreira. On Rado conditions for nonlinear Diophantine equations. *European Journal of Combinatorics* **94C** (2021)

[18] Also need $\tilde{P}(x) = P(x, \ldots, x) \neq 0$ and reducible to linear factors over $\mathbb{Z}$.

Partition regularity of configurations

- Instead of Diophantine equations, we will now look at *configurations*, i.e. collections of functions $\{f_i : \mathbb{N}^d \to \mathbb{N}\}$

Definition (p.r. of configurations)

A configuration $\{f_1, \ldots, f_k\}$ is *partition regular* if for any finite partition $\mathbb{N} = C_1 \sqcup \cdots \sqcup C_r$, there exists $\mathbf{m} \in \mathbb{N}^d$ such that $\{f_1(\mathbf{m}), \ldots, f_k(\mathbf{m})\} \subseteq C_i$.

- Configurations $\to$ equations by *parametrising solutions*

Example

The equation $x + y = z$ can be parametrised by

$$\begin{cases} x = r \\ y = s \\ z = r + s \end{cases}$$

So, **Schur's theorem** says the *configuration* $\{r, s, r + s\}$ is p.r..

Topological dynamics and Moreira's work

- Furstenberg and Weiss[19] first developed a correspondence between *multiple recurrence of a topological dynamical system* and van der Waerden's theorem
- Moreira used a similar, but more general principle:
  - $\mathbb{N} \iff$ a certain compact Hausdorff space X
  - Semigroup of affine maps $\mathbb{N} \to \mathbb{N}$, $x \mapsto ax + b$ acts on X
  - Partition of $\mathbb{N} = C_1 \sqcup \cdots \sqcup C_r \iff$ open cover of $X = \bigcup_{i=1}^{r} U_i$

Theorem (Moreira, 2017)[20]

Let $f_1, \ldots, f_n \in \mathbb{Z}[x]$ have $f_i(0) = 0$. Then $\{x, xy, x + f_i(y)\}$ is p.r..

Corollary ($n = 1$, $f_1 = \mathrm{id}$)

The configuration $\{x, xy, x + y\}$ is partition regular.

---

[19] H. Furstenberg & B. Weiss. Topological dynamics and combinatorial number theory. *Journal d'Analyse Mathématique* **34** (1978), pp. 61–85

[20] J. Moreira. Monochromatic sums and products in $\mathbb{N}$. *Annals of Mathematics* **185.3** (2017), pp. 1069–1090

Our contributions III

- With a slight modification to Moreira's original argument:

Theorem (Barrett, Lupini & Moreira, 2019)[21]

Let $f_1, \ldots, f_n \in \mathbb{Z}[x]$ have $f_i(\mathbf{1}) = 0$. Then $\{x, xy, x + f_i(y)\}$ is p.r..

Corollary

Let $p(x, z) = \sum_{i=0}^{d} a_i x^{d-i} z^i$ be homogeneous of degree d in x and z. Then, $x^d(x - y) + p(x, z) = 0$ is p.r. if $a_0 = 0$, or if $\sum_{i=0}^{d} a_i = 0$.

Proof.

It is parametrised by $\{x = r;\ y = r + p(1, s);\ z = rs\}$.
Note $p(1, 0) = a_0$, so if $a_0 = 0$, the result follows by [JM17].
Note $p(1, 1) = \sum_{i=0}^{d} a_i$, so if $\sum_{i=0}^{d} a_i = 0$, apply [BLM19]. $\square$

[21] J. M. Barrett, M. Lupini & J. Moreira. On Rado conditions for nonlinear Diophantine equations. *European Journal of Combinatorics* **94C** (2021)

Further questions

- What other equations are p.r. / not p.r.?
- Density results - for which equations can we find a solution in any set of positive density?
- In light of Hilbert's tenth problem[22], is there a general algorithm to decide whether a given Diophantine equation is p.r.?
- What about equations in other structures (e.g. $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{F}_p$, general semigroups, etc...)?
  - Plenty of work has been done in finite fields $\mathbb{F}_p$: Csikvári, Gyarmati & Sárközy[23]; Green & Sanders[24]

---

[22] Y. Matiyasevich. c.e. sets are Diophantine. *Doklady Akademii Nauk* **191.2** (1970)

[23] P. Csikvári, K. Gyarmati & A. Sárközy. Density and Ramsey-type results on algebraic equations with restricted solution sets. *Combinatorica* **32.4** (2012), p. 425

[24] B. Green & T. Sanders. Monochromatic sums and products. *Discr. Analysis* (2016)