Ultrafilters and nonstandard methods in combinatorics of numbers

Mauro Di Nasso

Università di Pisa

Models of PA / Set Theory seminars – CUNY Graduate Center
New York, June 18, 2015

Introduction

In combinatorics of numbers one finds deep and fruitful interactions among diverse *non-elementary* methods, namely:

- Ergodic theory.
- Fourier analysis.
- Discrete topological dynamics.
- Algebra $(\beta\mathbb{N}, \oplus)$ in the space of ultrafilters on $\mathbb{N}$.

Recently, also the methods of nonstandard analysis have been applied to prove both "Ramsey results" and "density results".

Nonstandard Analysis in one slide

Nonstandard analysis essentially consists of two properties:

1. Every set X is "extended" to an object ${}^*X$, called its hyper-extension or nonstandard extension.

2. ${}^*X$ is a sort of "weakly isomorphic" copy of X, in the sense that it satisfies the same "elementary properties" as X.

The fact that "elementary properties" are preserved under hyper-extensions is called transfer principle.

Transfer principle

If $P(x_1, \ldots, x_n)$ is any property expressed in "elementary terms" (first-order formula), then for all $A_1, \ldots, A_n$:

$$P(A_1, \ldots, A_n) \Longleftrightarrow P(^*A_1, \ldots, ^*A_n)$$

Caveat: Quantifiers must be used in the *bounded forms*:

$$\text{“}\forall x \in A \;\; P(x, \ldots)\text{”} \quad \text{and} \quad \text{“}\exists x \in A \;\; P(x, \ldots)\text{”}.$$

The complete language $\mathcal{L}_X$ over a set X is the language that contains one symbol for each constant, function and relation on X.

The complete structure over X is the $\mathcal{L}_X$-structure having X as a universe, and where symbols are interpreted in the obvious way.

The hyper-extension ${}^*X$ is a non-trivial *elementary extension* of the complete structure over X. (Symbols of $\mathcal{L}_X$ are interpreted in ${}^*X$ by the corresponding hyper-extensions.)

E.g., the hyperreal numbers ${}^*\mathbb{R}$ are an ordered field that properly extends the real line $\mathbb{R}$; and the hyperintegers ${}^*\mathbb{Z}$ are a *discretely ordered ring*.

$\mathbb{R}$ and ${}^*\mathbb{R}$ (and similarly $\mathbb{Z}$ and ${}^*\mathbb{Z}$) cannot be distinguished by any "elementary property".

The hyperreal numbers

As a proper extension of the real line, the hyperreal field ${}^*\mathbb{R}$ contains infinitesimal numbers $\varepsilon \neq 0$:

$$-\frac{1}{n} < \varepsilon < \frac{1}{n} \quad \text{for all } n \in \mathbb{N}$$

and infinite numbers Ω:

$$|\Omega| > n \quad \text{for all } n \in \mathbb{N}.$$

So, ${}^*\mathbb{R}$ is *not* Archimedean, and hence it is *not* complete (*e.g.*, the bounded set of infinitesimal numbers does not have a least upper bound).

Clearly, both the *Archimedean property* and the *completeness property* are not "elementary" properties of $\mathbb{R}$.

Standard Part

Every *finite* number $\xi \in {}^*\mathbb{R}$ has infinitesimal distance from a unique real number, called the standard part of ξ:

$$\xi \approx \mathrm{st}(\xi) \in \mathbb{R}$$

So ${}^*\mathbb{R}$ consists of infinite numbers and of numbers of the form $r + \varepsilon$ where $r \in \mathbb{R}$ and $\varepsilon \approx 0$ is infinitesimal.

The hypernatural numbers

The hyperintegers ${}^*\mathbb{Z}$ are a *discretely ordered ring* whose positive part are the hypernatural numbers ${}^*\mathbb{N}$, which are a very special model of PA.

$$^*\mathbb{N} \;=\; \{\underbrace{1,2,\ldots,n,\ldots}_{\text{finite numbers}}\quad \underbrace{\ldots,N-2,N-1,N,N+1,N+2,\ldots}_{\text{infinite numbers}}\}$$

- Every $\xi \in {}^*\mathbb{R}$ has an *integer part*, *i.e.* there exists a unique hyperinteger $\nu \in {}^*\mathbb{Z}$ such that $\nu \leq \xi < \nu + 1$.

- The order structure of $^*\mathbb{R}$ have been investigated by several researchers, including Zakon, Forti and Honsell, Keisler, Schmerl. An example:

Theorem (DN-Forti 2002)

There are sets of hyperreal numbers where "microcosm" and "macrocosm" are order-isomorphic:

$$\mu(0) = \{\varepsilon \in {}^*\mathbb{R} \mid \varepsilon \sim 0\} \cong {}^*\mathbb{R}$$

On the other hand, for every $\kappa > 2^{\aleph_0}$, there are sets of hyperreals where $cof(\mu(0)) = cof({}^*\mathbb{R}) = \kappa$ but $\mu(0) \not\cong {}^*\mathbb{R}$.

Why nonstandard analysis in combinatorics?

- Arguments of elementary finite combinatorics can be used in a hyperfinite setting to prove results about infinite sets of integers, also in the case of null asymptotic density.
- The nonstandard integers (or hyperintegers) ${}^*\mathbb{Z}$ may serve as a sort of "bridge" between the *discrete* and the *continuum*.
- Tools from *analysis* and *measure theory*, such as Birkhoff Ergodic Theorem and Lebesgue Density Theorem, can be used in ${}^*\mathbb{Z}$.

- Hypernatural numbers can play the role of ultrafilters on $\mathbb{N}$ and be used in *Ramsey theory* problems (partition regularity of diophantine equations).
- Nonstandard proofs for density-depending results usually work also in the more general setting of amenable groups.
- Additional model-theoretic tools are available, most notably saturation.

Syndeticity

Definition

A is thick if it contains arbitrarily long intervals, *i.e.* if for every k there exists x such that

$$[x+1, x+k] \subseteq A$$

Definition (Nonstandard)

A is thick if there exists an *infinite interval* $[\nu, \mu] \subseteq {}^*A$.

Definition

A is syndetic if there exists $k \in \mathbb{N}$ such that every interval $[x, x+k] \cap A \neq \emptyset$. (That is, if A^c is *not* thick.)
Equivalently, there exists a finite set F such that $A + F = \mathbb{Z}$.

Definition (Nonstandard)

A is syndetic if ${}^*A$ has only *finite gaps*,
i.e. if ${}^*A \cap I \neq \emptyset$ for every infinite interval I.

Definition

A is piecewise syndetic if $A = B \cap C$ where B is *thick* and C is *syndetic*.
Equivalently, there exists a finite set F such that $A + F$ is thick.

Definition (Nonstandard)

A is piecewise syndetic if ${}^*A$ has only *finite gaps* on some *infinite interval*.

Asymptotic density

Definition

The upper asymptotic density of a set $A \subseteq \mathbb{N}$:

$$\overline{d}(A) \;=\; \limsup_{n\to\infty} \frac{|A \cap [1,n]|}{n}.$$

Definition (Nonstandard)

$\overline{d}(A) \geq \alpha$ if there exists an infinite $N \in {}^*\mathbb{N}$ such that

$$\frac{|{}^*A \cap [1,N]|}{N} \approx \alpha.$$

Definition

The (upper) Banach density of a set $A \subseteq \mathbb{Z}$:

$$\mathrm{BD}(A) = \lim_{n\to\infty}\left(\max_{k\in\mathbb{Z}} \frac{|A\cap[k+1,k+n]|}{n}\right)$$

Definition (Nonstandard)

$\mathrm{BD}(A) \geq \alpha$ if there exists an infinite interval I such that

$$\frac{|{}^*A\cap I|}{|I|} \approx \alpha.$$

- $\mathrm{BD}(A) \geq \overline{d}(A)$.
- There are sets with $\mathrm{BD}(A) = 1$ and $\overline{d}(A) = 0$.
- A is thick $\Leftrightarrow \mathrm{BD}(A) = 1$.
- A piecewise syndetic $\Rightarrow \mathrm{BD}(A) > 0$, but not conversely.

Partition regularity

The fundamental notion of structural “largeness” in Ramsey theory is the following “indestructibility” property under finite partitions.

Definition

A family $\mathcal{F}$ of sets of integers is partition regular if

$$A_1 \cup \ldots \cup A_n = A \in \mathcal{F} \implies \exists\, i \text{ s.t. } A_i \in \mathcal{F}$$

- $\{A \subseteq \mathbb{N} \mid A \text{ is infinite}\}$ is P.R.
- $\{A \subseteq \mathbb{N} \mid \overline{d}(A) > 0\}$ is P.R.
- $\{A \subseteq \mathbb{N} \mid \text{BD}(A) > 0\}$ is P.R.
- $\{A \subseteq \mathbb{N} \mid \sum_{a \in A} 1/a = \infty\}$ is P.R.
- $\{A \subseteq \mathbb{N} \mid A \text{ is thick}\}$ is not P.R.
- $\{A \subseteq \mathbb{N} \mid A \text{ is syndetic}\}$ is not P.R.
- $\{A \subseteq \mathbb{N} \mid A \text{ is piecewise syndetic}\}$ is P.R.

Theorem

The family of piecewise syndetic sets is partition regular.

Nonstandard proof. By induction, it is enough to check the property for 2-partitions $A = \text{BLUE} \cup \text{RED}$.

- Take hyper-extensions ${}^*A = {}^*\text{BLUE} \cup {}^*\text{RED}$, and pick an infinite interval I where ${}^*A$ has only finite gaps.
- If the *blue elements of ${}^*A$ have only finite gaps in I, then BLUE is piecewise syndetic.
- Otherwise, there exists an infinite interval $J \subseteq I$ that only contains *red elements of ${}^*A$. But then ${}^*\text{RED}$ has only finite gaps in J, and hence RED is piecewise syndetic.

Combinatorics of numbers

The two areas of combinatorics where nonstandard methods have been applied are the following:

- Ramsey theory $\longrightarrow$ partition regularity properties on sets of numbers.
- Additive combinatorics $\longrightarrow$ Density-dependent results for sets of integers.

A little history

In the early years of XX century, Issai Schur was working on *Fermat's last theorem* over finite fields.

Theorem (Schur 1916)

For every m, the equation $x^m + y^m = z^m$ has non-trivial solutions in $\mathbb{Z}/p\mathbb{Z}$ for all sufficiently large primes p.

The crucial combinatorial lemma used in the proof:

Theorem (Schur 1916 – Finite version)

For every r, there exists $N(r)$ such that for all $n \geq N(r)$, in every r-coloring $\{1, 2, \ldots, n\} = C_1 \cup \ldots \cup C_r$ there is a monochromatic Schur triple $a, b, a + b \in C_i$.

By compactness, the finite and infinite versions are equivalent:

Theorem (Schur – Infinite version)

In every finite coloring $\mathbb{N} = C_1 \cup \ldots \cup C_r$ there is a monochromatic Schur triple $a, b, a + b$.

Theorem (Schur 1916)

For every m, the equation $x^m + y^m = z^m$ has non-trivial solutions in $\mathbb{Z}/p\mathbb{Z}_p$ for all sufficiently large primes p.

Proof.

- Take the multiplicative subgroup $H = \{x^m \mid x \in \mathbb{Z}_p^*\}$ and say that $x, y \in \mathbb{Z}_p^*$ have the *same color* if $xH = yH$.
- The subgroup H has index $gcd(m, p-1) \leq m$, so the number of colors r is at most m for every p.
- By the Lemma, for every sufficiently large p, we can pick a *monochromatic triple* $a, b, a+b$. That is, $a, b, a+b \in \xi H$.
- Pick x, y, z such that $a = \xi x^m$, $b = \xi y^m$, $a+b = \xi z^m$. Then

$$\xi x^m + \xi y^m = \xi z^m \implies x^m + y^m = z^m.$$

A fundamental result in this area of combinatorics was proved by Bartel van der Waerden at the age of 23.

Theorem (van der Waerden 1926)

In every finite coloring $\mathbb{N} = C_1 \cup \ldots \cup C_r$ *there are arbitrarily long monochromatic arithmetic progressions.*

Ramsey theorem

At the end of the 20's years of the XX century, Frank Ramsey was working on the problem of decidibility of 1st order logic.

Ramsey gave significant contributions to mathematics, economics and philosophy (by the way, he was Wittgenstein's supervisor). He died at the age of 26.

Theorem (Ramsey 1928)

The class of formulas whose prenex normal form have an $\exists\forall$ quantifier prefix and do not contain any function symbols, are a decidable fragment of 1st order logic formulas.

In the proof he needed a combinatorial property, namely Ramsey theorem, that eventually became the cornerstone of a whole field of research known as *Ramsey theory*.

Theorem (Ramsey 1928 – Infinite version)

Let $[X]^k = C_1 \cup \ldots \cup C_r$ be a finite coloring of the k-tuples of an infinite set X. Then there exists an infinite homogeneous set H, i.e. all k-tuples from H are monochromatic: $[H]^k \subseteq C_i$.

Theorem (Ramsey – Finite version)

For every k, m, r there exists $N = N(k, m, r)$ such that for every $n \geq N$ and for every r-coloring $[\{1, \ldots, n\}]^k = C_1 \cup \ldots \cup C_r$ there exists a homogeneous set $|H| \geq m$.

Usually, infinite versions are simpler to formulate, simpler to be proved, and equivalent to the finite versions!

A short nonstandard proof of Ramsey Theorem

We use iterated hyper-extensions. For simplicity, let $k = 2$.

Let a finite coloring $[^{**}\mathbb{N}]^2 = {}^{**}C_1 \cup \ldots \cup {}^{**}C_r$ be given.

Pick an infinite $\xi \in {}^*\mathbb{N}$. Then $\{\xi, {}^*\xi\} \in {}^{**}C_i$ for some i.

$\xi \in \{x \in {}^*\mathbb{N} \mid \{x, {}^*\xi\} \in {}^{**}C_i\} = {}^*\{x \in \mathbb{N} \mid \{x, \xi\} \in {}^*C_i\} = {}^*A$.

Pick $a_1 \in A$, so $\{a_1, \xi\} \in {}^*C_i$.

Then $\xi \in {}^*\{x \in \mathbb{N} \mid \{a_1, x\} \in C_i\} = {}^*B_1$.

$\xi \in {}^*A \cap {}^*B_1 \Rightarrow A \cap B_1$ is infinite: pick $a_2 \in A \cap B_1$ with $a_2 > a_1$.

$a_2 \in B_1 \Rightarrow \{a_1, a_2\} \in C_i$.

$a_2 \in A \Rightarrow \{a_2, \xi\} \in {}^*C_i \Rightarrow \xi \in {}^*\{x \in \mathbb{N} \mid \{a_2, x\} \in {}^*C_1\} = {}^*B_2$.

$\xi \in {}^*A \cap {}^*B_1 \cap {}^*B_2 \Rightarrow$ we can pick $a_3 \in A \cap B_1 \cap B_2$ with $a_3 > a_2$.

$a_3 \in B_1 \cap B_2 \Rightarrow \{a_1, a_3\}, \{a_2, a_3\} \in C_i$, and so forth.

The infinite set $H = \{a_n \mid n \in \mathbb{N}\}$ is such that $[H]^2 \subset C_i$.

As straight application of Ramsey Theorem:

Theorem (Schur – *Infinite version*)

In every finite coloring $\mathbb{N} = C_1 \cup \ldots \cup C_r$ there is a monochromatic Schur triple $a, b, a+b$.

Proof: Give any pair $\{x < y\} \in [\mathbb{N}]^2$ the same color as $y - x$. Pick an infinite homogeneous set H. Then for every $x < y < z$ in H, the following numbers form a monochromatic Schur triple:

$$a = y - x, \quad b = z - y, \quad a + b = z - x$$

Ultrafilters

Definition

A filter $\mathcal{U}$ on $\mathbb{N}$ is a nonempty family of subsets of $\mathbb{N}$ such that:

(a) $\mathbb{N} \in \mathcal{F}, \emptyset \notin \mathcal{F}$;

(b) $A \in \mathcal{F}, B \in \mathcal{F} \Rightarrow A \cap B \in \mathcal{F}$;

(c) $A \in \mathcal{F}, A \subseteq B \Rightarrow B \in \mathcal{F}$.

Example: The Frechet filter of cofinite subset:

$$\text{Fr}(\mathbb{N}) = \{A \subseteq \mathbb{N} \mid A^c \text{ is finite}\}$$

Definition

An ultrafilter is a filter $\mathcal{U}$ with the additional property:

- For every $A \subseteq \mathbb{N}$, if $A \notin \mathcal{U}$ then $A^c \in \mathcal{U}$

or, equivalently, the partition regularity:

- $A_1 \cup \ldots \cup A_n \in \mathcal{U} \ \Rightarrow \ A_i \in \mathcal{U}$ for some i.

Ultrafilters $=$ *Maximal* filters

Ultrafilters on a set I can be characterized as follows:

- The family of sets of measure 1 of a finitely-additive two-valued measure $\mu : \mathcal{P}(I) \to \{0, 1\}$.
- The family of zero-sets $Z(\varphi) = \{i \mid \varphi(i) = 0\}$ where φ ranges on the elements of a maximal ideal $\mathfrak{m} \subset \mathrm{Fun}(I, \mathbb{R})$.

Trivial examples are given the principal ultrafilters:

$$\mathfrak{U}_x = \{A \subseteq \mathbb{N} \mid x \in A\} \quad (x \in \mathbb{N})$$

The *non-principal* ultrafilters are precisely those ultrafilters that extend the *Frechet filter* (i.e., they do not contain any finite set).

- By *Zorn's lemma*, every filter can be extended to an ultrafilter

Ultrafilters in combinatorics of numbers

A fundamental result in combinatorics of numbers is the following strong generalization of Schur's theorem.

Theorem (Hindman 1974)

For every finite coloring of $\mathbb{N}$ there exists an infinite $X = \{x_i\}$ such that all finite sums $FS(X) = \{\sum_{i \in I} x_i \mid I \subset \mathbb{N} \text{ finite}\}$ are monochromatic.

The original proof consisted in really intricate combinatorial arguments.

"Anyone with a very masochistic bent is invited to wade through the original combinatorial proof." (Neil Hindman)

Before Hindman's proof, Glazer noticed that the "finite sum property" would follow from the existence of ultrafilters $\mathcal{U} = \mathcal{U} \oplus \mathcal{U}$ that are idempotent with respect to a "pseudo-sum" operation:

$$A \in \mathcal{U} \oplus \mathcal{V} \iff \{n \mid A - n \in \mathcal{V}\} \in \mathcal{U}$$

where $A - n = \{m \mid m + n \in A\}$.

After first attemps to prove the existence of idempotent ultrafilters failed, Hindman found his intricate combinatorial proof. The very next year, Galvin showed that idempotent ultrafilters exist as a consequence of general result on topological semigroups, namely Ellis' Lemma.

Galvin-Glazer proof of Hindman's thoerem opened a new area of research. Since then, many relevant applications of ultrafilters in combinatorial number theory have been found. As yet, several of them do not have any elementary proof.

- N. Hindman e D. Strauss, *Algebra in the Stone-Čech compactification*, 2nd edition, De Gruyter, 2012.

1. Let $\mathcal{U} = \mathcal{U} \oplus \mathcal{U}$ be an *idempotent* ultrafilter. Then every $A \in \mathcal{U}$ includes a set of sums $FS(X)$ for some infinite X.
2. Let $\mathcal{U}$ be a *uniformly recurrent* point in the topological dynamics $(\beta\mathbb{N}, S)$ where $S : \mathcal{U} \mapsto \mathfrak{U}_1 \oplus \mathcal{U}$ is the "shift". Then every $A \in \mathcal{U}$ contains arbitrarily long arithmetic progressions.

(1) $\Rightarrow$ Hindman theorem.

(2) $\Rightarrow$ van der Waerden theorem.

Density-depending results

Relationships between "largeness" in terms of density, and "combinatorial richness".

Density versions of Ramsey results are usually much harder to prove.

A weak density version of van der Waerden Theorem is the following:

Theorem (Roth 1952)

If $\overline{d}(A) > 0$, then A contains arithmetic progressions of length 3.

Szemerédi Theorem

In the 70's, by *"a masterpiece of combinatorial reasoning"*, Endre Szemerédi proved the density version of van der Waerden's theorem, that was conjectured by Erdoš and Turán in 1936. (In 2012, he was awarded the Abel Prize.)

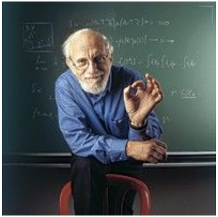
Theorem (Szemerédi 1975)

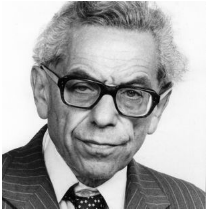
If $\overline{d}(A) > 0$, then A contains arbitrarily long arithmetic progressions.

Other proofs of Szemerédi Theorem have been found by Hillel Fürstenberg using ergodic theory (1977) and by Timothy Gowers using Fourier analysis (2001).
Fürstenberg developed a whole area of research by introducing the use of ergodic theory in combinatorial number theory.

Theorem (Sarközy-Fürstenberg 1978)

If $\overline{d}(A) > 0$ then there exists distinct $a, a' \in A$ such that $a - a' = n^2$ is a square.





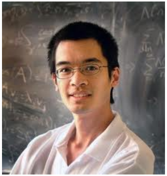
Erdös' Conjecture (1936)

If A is a set of natural numbers with $\sum_{a \in A} 1/a = \infty$ then it contains arbitrarily long arithmetic progressions.

This conjecture is still open even for arithmetic progressions of length 3.

Theorem (Green-Tao 2004)

The sequence of prime numbers contains arbitrarily long arithmetic progressions.



Recently, Tao showed interest in *nonstandard analysis* as a convenient tool in certain aspecets of additive combinatorics.

Jin's Theorem

Theorem

If $BD(A) > 0$, then $(A - A) \cap (B - B) \neq \emptyset$ for every infinite B.

The proof consists of a *pigeonhole principle* argument.
Let $\alpha = \mathrm{BD}(A)$ and take distinct elements $b_1, \ldots, b_N \in B$ with $N > 1/\alpha$. The shifts $A + b_i$ are not pairwise disjoint, as otherwise

$$\mathrm{BD}\left(\bigcup_{i=1}^{N}(A + b_i)\right) = \sum_{i=1}^{N} \mathrm{BD}(A + b_i) = N \cdot \alpha > 1$$

Finally, note that if $(A + b) \cap (A + b') \neq \emptyset$ for some $b \neq b'$, then $(A - A) \cap (B - B) \neq \emptyset$.

Corollary

If $BD(A) > 0$ then $A - A$ is syndetic.

Proof. If $A - A$ was not syndetic, then $T = (A - A)^c$ would be thick, and one could find an infinite set B with $B - B \subseteq T$, a contradiction.

Remark

$\mathrm{BD}(A), \mathrm{BD}(B) > 0 \not\Longrightarrow A - B$ syndetic.

E.g., it is not difficult to find thick sets A, B, C such that their complements A^c, B^c, C^c are thick as well, and $A - B \subset C$.

In a series of papers appeared at the end of the 80's, Steven Leth developed a framework for use of hyperintegers of nonstandard analysis in combinatorial number theory. Most notably, he established connections between properties of sequences of natural numbers, and topological properties in a nonstandard setting.

In a paper of 1991, Jerry Keisler and Steven Leth investigated various topological properties of the hyperfinite time line, namely an initial hyperfinite interval of hyperintegers.

A question left open was the following:

- Let $\nu \in {}^*\mathbb{N}$ be infinite. If $A, B \subseteq [1, \nu]$ are hyperfinite sets with positive *Loeb measure*, is it true that the sumset $A + B$ is somewhere dense in the so-called $\mathbb{N}$-*topology*?

Leth pointed out that the standard counterpart of the topological property of being somewhere dense in the $\mathbb{N}$-topology, is piecewise syndeticity.

About 15 years ago, Renling Jin eventually proved the desired nonstandard topological property of sumsets, and obtained the following result as a corollary:

Theorem (Jin 2000)

If $BD(A), BD(B) > 0$ then $A + B$ is piecewise syndetic.

A number of other interesting results in additive number theory have been also obtained by Jin using nonstandard analysis.

- Jin's result raised the attention of researchers in the area, but they did not understand his nonstandard proof.
  (In fact, his proof used "difficult" nonstandard arguments).
- Jin's himself then published a "standard" proof, which was a direct translation of the original *nonstandard* arguments. Unfortunately, in this way "certain degree of intuition and motivation are lost".
- In 2006, by using ergodic theory, Bergelson, Furstenberg and Weiss re-proved Jin's theorem in strengthened form, by showing that $A + B$ is *piecewise Bohr*.

- In 2009, again by ergodic theory, Griesmer extended BFW's result to special cases where one of the two sets has zero Banach density.
- In 2010, Beiglböck found a nice proof of Jin's theorem by using ultrafilters and some measure theory.

In early versions of his paper, Jin asked whether one can estimate the number k needed for $A + B + [0, k]$ to be thick, in terms of BD(A) and BD(B). He later proved that such a k *does not* directly depend on $BD(A)$ and $BD(B)$. In fact:

For any $\alpha + \beta < 1$ and for every $k \in \mathbb{N}$, there exist sets A, B s.t.

1. $BD(A) > \alpha$
2. $BD(B) > \beta$
3. $A + B + [0, k]$ is <u>not</u> thick.

However, if one takes *arbitrary* finite sets F in place of initial segments $[0, k]$, a bound can be given.

Theorem (DN 2012)

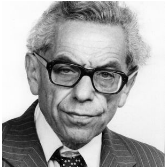
Let $BD(A) = \alpha > 0$ and $BD(B) = \beta > 0$. Then there exists a finite set $|F| \leq 1/\alpha\beta$ such that $A + B + F$ is thick. So, $A + B$ is piecewise syndetic.

The nonstandard arguments used in the proofs can be (almost) directly applied to more general settings.

A form of Jin's theorem with a bound, also holds for all amenable groups (*joint work with M. Lupini*).

Erdös' $B + C$ conjecture

In analogy to *Szemerédi theorem* w.r.t. *van der Waerden's theorem*, in 1975 Paul Erdős conjectured a density property inspired by *Hindman's theorem*.



Erdös' $B + C$ conjecture (1979)

If $A \subseteq \mathbb{N}$ has positive lower density, then there exist infinite sets B, C such that $B + C \subseteq A$.

A partial result was soon obtained by Melvin Nathanson.

Theorem (Nathanson 1980)

If $\overline{d}(A) > 0$ then there exist an infinite set B and an arbitrarily large finite set C such that $B + C \subset A$.

No progress have been made on the conjecture until recent times.

The following result was proved during the "AIM SQuaRE" research program "Nonstandard analysis in combinatorics":

Theorem (DN-Goldbring-Jin-Leth-Lupini-Mahlburg - 2014)

If $BD(A) > 0$, then there exist infinite sets B, C and $k \in \mathbb{N}$ such that $B + C \subseteq A \cup (A + k)$.

We also have a proof for the full Erdös' conjecture when $\mathrm{BD}(A) > 1/2$ (these results are also extended to countable amenable groups.)

These results also holds for all countable amenable groups.

An example of nonstandard reasoning

- Suppose $\mathrm{BD}(A) > 0$.
- Take an infinite interval $I = [\Omega + 1, \Omega + N]$ of ${}^*\mathbb{N}$ such that the relative density $|{}^*A \cap I|/N \approx \mathrm{BD}(A)$.
- Take the Loeb measure μ on I, that extends the "counting measure": for all *internal* $X \subseteq I$, it is $\mu(X) = \mathrm{st}(|X \cap I|/N)$.
- Consider the shift operator $T : \xi \mapsto \xi + 1$ $(T(\Omega + N) = \Omega + 1)$.

- Apply Birkhoff Ergodic Theorem: For almost all $\xi \in I$ the following limit exists:

$$\lim_{n\to\infty} \frac{1}{n} \sum_{i=1}^{n} \chi_A(T^i(\xi))$$

- By the definition of Banach density, it follows that such limits equal $\mathrm{BD}(A)$ for almost all $\xi \in I$:

$$\lim_{n\to\infty} \frac{1}{n} \sum_{i=1}^{n} \chi_A(T^i(\xi)) = \lim_{n\to\infty} \frac{|{}^*A \cap [\xi+1, \xi+n]|}{n} = \mathrm{BD}(A).$$

Let $A_\xi = ({}^*A - \xi) \cap \mathbb{N} = \{i \in \mathbb{N} \mid \xi + i \in {}^*A\}$. We have proved that for almost all ξ, the density $d(A_\xi) = \mathrm{BD}(A)$. What does it mean?

Definition

$B \leq_{fe} A$: B is finitely embeddable in A if for every n, there exists a shift $x + (B \cap [1, n]) = A \cap [x + 1, x + n]$.

Finite embeddability preserves all finite configurations (*e.g.*, the existence of arbitrarily long arithmetic progressions).

- Fact: $B \leq_{fe} A$ if and only if there exists $\xi \in {}^*\mathbb{N}$ with $B = A_\xi$.

Theorem

Let $BD(A) = \alpha$. Then there exists a set $B \leq_{fe} A$ with asymptotic density $d(B) = \alpha$. (Actually, much more holds; e.g., one can assume Schnirelmann density $\sigma(B) = \alpha$.)

Partition regularity of diophantine equations

Definition

An equation $F(x_1, \ldots, x_n) = 0$ is [injectively] partition regular (PR) on $\mathbb{N}$ if for every finite coloring of $\mathbb{N}$ there exist [distinct] monochromatic elements $a_1, \ldots, a_n$ such that $F(a_1, \ldots, a_n) = 0$.

- By *Schur's Lemma*, the equation $X + Y = Z$ is partition regular.
- By *van der Waerden's theorem*, the equation $X + Y = 2Z$ is partition regular. (Solutions are the 3-term arithmetic progressions.)
- However, the equation $X + Y = 3Z$ is *not* partition regular!

The problem of partition regularity of linear diophantine equations was completely solved by Richard Rado.

Theorem (Rado 1933)

The diophantine equation $c_1X_1 + \ldots + c_nX_n = 0$ *is PR if and only if* $\sum_{i\in I} c_i = 0$ *for some (nonempty)* $I \subseteq \{1, \ldots, k\}$.

Hypernatural numbers as ultrafilters

In a nonstandard setting, every hypernatural number $\xi \in {}^*\mathbb{N}$ generates a (standard) ultrafilter:

$$\mathfrak{U}_\xi = \{A \subseteq \mathbb{N} \mid \xi \in {}^*A\}$$

If ${}^*\mathbb{N}$ is $\mathfrak{c}^+$-saturated, then every ultrafilter is generated by some number $\xi \in {}^*\mathbb{N}$ (actually, by at least $\mathfrak{c}^+$-many).

In some sense, in a nonstandard setting, every ultrafilter is a *principal* ultrafilter!

Question

What one can say about the map $\xi \mapsto \mathfrak{U}_\xi$?

- The map $\xi \mapsto \mathfrak{U}_\xi$ is never a bijection.
- There exists an injective map $\xi \mapsto \mathfrak{U}_\xi$ if and only there exists an ultrafilter $\mathcal{U}$ such that for every $f, g : \mathbb{N} \to \mathbb{N}$:

$$f(\mathcal{U}) = g(\mathcal{U}) \implies \{n \mid f(n) = g(n)\} \in \mathcal{U}$$

[Recall that $A \in f(\mathcal{U}) \Leftrightarrow f^{-1}(A) \in \mathcal{U}$.]

Ultrafilters with the above property are named Hausdorff ultrafilter, Hausdorff ultrafilters have been investigated by their own sake:

Theorem (DN-Forti 2006)

Regular Hausdorff ultrafilters cannot exists on cardinals that are larger than $2^{\aleph_0}$. (Indeed, they cannot exist on the cardinal invariant $\mathfrak{u}$.)

Hausdorff ultrafilter are proved to exist under the *continuum hypothesis*. (Indeed, every selective ultrafilter is Hausdorff.) However, the following question is still open:

OPEN QUESTION

Can one prove in ZFC the existence of Hausdorff ultrafilters?

u-equivalence

Definition

For $\xi, \zeta \in {}^*\mathbb{N}$, we say that $\xi \underset{u}{\sim} \zeta$ are *u*-equivalent if for every $A \subseteq \mathbb{N}$ one has that either $\xi, \zeta \in {}^*A$ or $\xi, \zeta \notin {}^*A$.

So, $\xi \underset{u}{\sim} \zeta$ means that ξ and ζ are "indiscernible", in the sense that cannot be distinguished by any hyper-extension (they satisfy the same "definable" properties).

The name *u*-equivalence is because $\xi \underset{u}{\sim} \zeta$ generate the same ultrafilter on $\mathbb{N}$:

$$\mathfrak{U}_\xi = \{A \subseteq \mathbb{N} \mid \xi \in {}^*A\} = \{A \subseteq \mathbb{N} \mid \zeta \in {}^*A\} = \mathfrak{U}_\zeta.$$

Notice that the following properties are equivalent:

- There exists a nonstandard model ${}^*\mathbb{N}$ where $\xi \underset{u}{\sim} \zeta \Rightarrow \xi = \zeta$.
- There exists a nonstandard model ${}^*\mathbb{N}$ where different points have different 1-types.
- There exists a Hausdorff ultrafilter on $\mathbb{N}$.

Definition

An equation $F(x_1, \ldots, x_n) = 0$ is [injectively] partition regular (PR) on $\mathbb{N}$ if for every finite coloring of $\mathbb{N}$ there exist [distinct] monochromatic elements $a_1, \ldots, a_n$ such that $F(a_1, \ldots, a_n) = 0$.

Theorem (Nonstandard characterization)

An equation $F(x_1, \ldots, x_n) = 0$ is [injectively] PR on $\mathbb{N}$ if and only if there exist [distinct] numbers $\xi_1 \underset{u}{\sim} \ldots \underset{u}{\sim} \xi_n \in {}^*\mathbb{N}$ such that ${}^*F(\xi_1, \ldots, \xi_n) = 0$.

Idempotent ultrafilters and hyper-hypernatural numbers

Hyper-hypernatural numbers ${}^{**}\mathbb{N}$ can be used to give a nice characterization of idempotent ultrafilters.

- The natural numbers are an initial segment of the hyper-natural numbers: $\mathbb{N} < {}^*\mathbb{N} \setminus \mathbb{N}$

Then by *transfer*: ${}^*\mathbb{N} < {}^{**}\mathbb{N} \setminus {}^*\mathbb{N}$

Also numbers $\Xi \in {}^{**}\mathbb{N}$ generate ultrafilters:

$$\mathfrak{U}_{\Xi} \;=\; \{A \subseteq \mathbb{N} \mid \Xi \in {}^{**}A\}$$

Nonstandard characterization

An ultrafilter $\mathcal{U}$ is *idempotent* if and only if there exists $\nu \in {}^*\mathbb{N}$ such that

$$\mathcal{U} \;=\; \mathfrak{U}_\nu \;=\; \mathfrak{U}_{\nu + {}^*\nu}$$

This characterization makes it easier to handle idempotent ultrafilters and their combinations.

Let us start with a simple example.

Theorem (Bergelson-Hindman 1990)

Let $\mathcal{U}$ be an idempotent ultrafilter. Then every $A \in 2\mathcal{U} \oplus \mathcal{U}$ contains an arithmetic progression of length 3.

There is a really simple proof in a nonstandard setting.

If ν is such that $\mathcal{U} = \mathfrak{U}_\nu = \mathfrak{U}_{\nu + {}^*\nu}$ then

- $\xi = 2\nu + {}^{**}\nu$
- $\zeta = 2\nu + {}^*\nu + {}^{**}\nu$
- $\vartheta = 2\nu + 2{}^*\nu + {}^{**}\nu$

form an arithmetic progression of length 3 in ${}^{***}\mathbb{N}$, and

$$\mathfrak{U}_\xi = \mathfrak{U}_\zeta = \mathfrak{U}_\vartheta = 2\mathcal{U} \oplus \mathcal{U}$$

Then for every $A \in 2\mathcal{U} \oplus \mathcal{U}$, the numbers $\xi, \zeta, \vartheta \in {}^{***}A$ and so, by *transfer*, there exist 3 elements in A in arithmetic progression.

Ultrafilter version of Rado's Theorem

The previous argument can be generalize to prove the following ultrafilter version of Rado's theorem.

Theorem (DN 2014)

Let $c_1X_1 + \ldots + c_nX_n = 0$ be a diophantine equation with $n \geq 3$. If $c_1 + \ldots + c_n = 0$ then there exist $a_1, \ldots, a_{n-1} \in \mathbb{N}$ such that for every idempotent $\mathcal{U}$, the ultrafilter

$$\mathcal{V} = a_1\mathcal{U} \oplus \ldots \oplus a_{n-1}\mathcal{U}$$

witnesses that the equation is injectively PR, i.e. for every $A \in \mathcal{V}$ there exist distinct $x_1, \ldots, x_n \in A$ with $c_1x_1 + \ldots + c_kx_k = 0$.

Let $\mathcal{U} = \mathfrak{U}_\xi$ be any idempotent ultrafilter.

For simplicity, denote by $u_1 = \xi$, $u_2 = {}^*\xi$, $u_3 = {}^{**}\xi$, *etc.*

Let $a_1, \ldots, a_{n-1}$ be arbitrary integers, and consider the following elements in ${}^{n*}\mathbb{N}$:

$$
\begin{array}{lllllllllllllllll}
\zeta_1 & = & a_1 u_1 & + & a_1 u_2 & + & a_2 u_3 & + & a_3 u_4 & + & \ldots & & & + & a_{n-2} u_{n-1} & + & a_{n-1} u_n \\
\zeta_2 & = & a_1 u_1 & + & 0 & + & a_2 u_3 & + & a_3 u_4 & + & \ldots & & & + & a_{n-2} u_{n-1} & + & a_{n-1} u_n \\
\zeta_3 & = & a_1 u_1 & + & a_2 u_2 & + & 0 & + & a_3 u_4 & + & \ldots & & & + & a_{n-2} u_{n-1} & + & a_{n-1} u_n \\
\vdots & & \vdots & & \vdots & & \vdots & & \vdots & & \vdots & & & & \vdots & & \vdots \\
\zeta_{n-1} & = & a_1 u_1 & + & a_2 u_2 & + & a_3 u_3 & + & \ldots & + & a_{n-2} u_{n-2} & & & + & 0 & + & a_{n-1} u_n \\
\zeta_n & = & a_1 u_1 & + & a_2 u_2 & + & a_3 u_3 & + & \ldots & + & a_{n-2} u_{n-2} & & & + & a_{n-1} u_{n-1} & + & a_{n-1} u_n
\end{array}
$$

$\zeta_1 \underset{u}{\sim} \zeta_2 \underset{u}{\sim} \ldots \underset{u}{\sim} \zeta_n$ generate the same ultrafilter, namely:

$$\mathcal{V} \;=\; a_1\mathcal{U} \oplus a_2\mathcal{U} \oplus \ldots \oplus a_{n-1}\mathcal{U}$$

Now, $c_1\zeta_1 + \ldots + c_n\zeta_n = 0$ if and only if the coefficients a_i fulfill the following conditions:

$$\begin{cases} (c_1 + c_2 + \ldots + c_n) \cdot a_1 = 0 \\ c_1 \cdot a_1 + (c_3 + \ldots + c_n) \cdot a_2 = 0 \\ (c_1 + c_2) \cdot a_2 + (c_4 + \ldots + c_n) \cdot a_3 = 0 \\ \qquad\qquad \vdots \\ (c_1 + c_2 + \ldots + c_{n-3}) \cdot a_{n-3} + (c_{n-1} + c_n) \cdot a_{n-2} = 0 \\ (c_1 + c_2 + \ldots + c_{n-2}) \cdot a_{n-2} + c_n \cdot a_{n-1} = 0 \\ (c_1 + c_2 + \ldots + c_n) \cdot a_{n-1} = 0 \end{cases}$$

The first and the last equations are trivially satisfied because of the hypothesis $c_1 + c_2 + \ldots + c_n = 0$.

The remaining $n - 2$ equations are satisfied by (infinitely many) suitable $a_1, \ldots, a_{n-1} \in \mathbb{N}$, that can be explicitly given in terms of the c_i.

Since all the $a_i \neq 0$, the numbers ζ_is are mutually distinct and we can apply the nonstandard characterization of injective PR.

Non-linear diophantine equations

Rado completely solved the partition regularity problem of linear diophantine equations, but not much has been proved so far about *non-linear* diophantine equations.

Theorem (Hindman 2011)

The following equation is partition regular:

$$X_1 + X_2 + \ldots + X_n = Y_1 \cdot Y_2 \cdot \cdots \cdot Y_m$$

The nonstandard formalism used to prove the ultrafilter version of Rado's Theorem can be developed to also study the *non-linear* case.

By combining additive and multiplicative idempotent ultrafilters in a nonstandard setting, the following was recently proved:

Theorem (Luperi 2013)

Let $a_1X_1 + \ldots + a_nX_n = 0$ be partition regular. Then for every choice of finite sets $F_1, \ldots, F_n$, the following polynomial equation is partition regular: (Variables X_i and Y_j must be distinct.)

$$a_1X_1 \prod_{j\in F_1} Y_j + a_2X_2 \prod_{j\in F_2} Y_j + \ldots + a_nX_n \prod_{j\in F_n} Y_j = 0.$$

Notice that the above *Hindman's theorem* follows by considering the equation $X_1 + X_2 + \ldots + X_n - Y_1 = 0$, and finite sets $F_1 = F_2 = \ldots = F_n = \emptyset$, $F_{n+1} = \{2, \ldots, m\}$.

u-equivalence is especially useful in the non-linear case.
E.g., one can give a short proof of the following negative result:

Theorem (Csikvari-Gyarmati-Sarkozy 2012)

$X + Y = Z^2$ is not partition regular on $\mathbb{N}$ (except for $X = Y = Z = 2$).

An essential use is made of the following non-trivial property:

- ${}^*f(\alpha) \underset{u}{\sim} \alpha \ \Rightarrow \ {}^*f(\alpha) = \alpha$.

It corresponds to the ultrafilter property that if $f(\mathcal{U}) = \mathcal{U}$ then $\{n \mid f(n) = n\} \in \mathcal{U}$.

Nonstandard proof.

By contradiction, let $\alpha \underset{u}{\sim} \beta \underset{u}{\sim} \gamma$ be such that $\alpha + \beta = \gamma^2$.
By u-equivalence, $\alpha \equiv \beta \equiv \gamma \equiv i \mod 5$ with $0 \leq i \leq 4$, so

$$\alpha = 5^a \cdot \alpha_1 + i\,; \quad \beta = 5^b \cdot \beta_1 + i\,; \quad \gamma = 5^c \cdot \gamma_1 + i$$

where $a, b, c > 0$ and $\alpha_1, \beta_1, \gamma_1$ are not divisible by 5.
$\alpha \underset{u}{\sim} \beta \underset{u}{\sim} \gamma$ implies that $\alpha_1 \underset{u}{\sim} \beta_1 \underset{u}{\sim} \gamma_1$, and therefore
$\alpha_1 \equiv \beta_1 \equiv \gamma_1 \equiv j \not\equiv 0 \mod 5$.
The equality $\alpha + \beta = \gamma^2$ implies that either $i = 0$ or $i = 2$.
Assume first that $i = 0$. In this case $\gamma^2 = 5^{2c}\gamma_1^2$ where $\gamma_1^2 \equiv j^2 \not\equiv 0 \mod 5$. If $a < b$ then $\alpha + \beta = 5^a(\alpha_1 + 5^{b-a}\beta_1)$ where $\alpha_1 + 5^{b-a}\beta_1 \equiv j \not\equiv 0 \mod 5$. It follows that $2c = a \underset{u}{\sim} c$, and hence $2c = c$, a contradiction. If $a > b$ the proof is similar.

If $a = b$ then $\alpha + \beta = 5^a(\alpha_1 + \beta_1)$ where $\alpha_1 + \beta_1 \equiv 2j \not\equiv 0 \mod 5$, and also in this case we would have $2c = a \underset{u}{\sim} c$, a contradiction.

If $i = 2$ then $\gamma^2 - 4 = 5^c(5^c\gamma_1^2 + 4\gamma_1)$ where $5^c\gamma_1^2 + 4\gamma_1 \equiv 4j \not\equiv 0 \mod 5$. Now, in case $a < b$, one has that $\alpha + \beta - 4 = 5^a(\alpha_1 + 5^{b-a}\beta_1)$ where $\alpha_1 + 5^{b-a}\beta_1 \equiv j \not\equiv 0 \mod 5$, and so it would follow that $5^c\gamma_1^2 + 4\gamma_1 = \alpha_1 + 5^{b-a}\beta_1$. But then we would have $4j \equiv j$, which is not possible because $j \not\equiv 0$. The case $a > b$ is similar. Finally, if $a = b$ then $\alpha + \beta - 4 = 5^a(\alpha_1 + \beta_1)$ where $\alpha_1 + \beta_1 \equiv 2j \not\equiv 0 \mod 5$, and it would follow that $4j \equiv 2j$, again reaching the contradiction $j \equiv 0$.

Two examples of recent results aimed at generalizing Rado's theorem. On the positive side:

Theorem (DN - Luperi 2015)

Let us consider the diophantine equation

$$a_1X_1 + \ldots + a_nX_n = P(Y_1, \ldots, Y_k)$$

where the polynomial P is such that $P(0, \ldots, 0) = 0$.
If Rado's condition holds, i.e. if $\sum_{i \in I} c_i = 0$ for some (nonempty) $I \subseteq \{1, \ldots, k\}$, then the equation is PR.

E.g., let us consider the equation $X_1 - 2X_2 + X_3 = Y^3$. In every finite coloring of the natural numbers one finds monochromatic triples of the form $\{a, b, c, 2a - b + c^3\}$, *etc.*

On the negative side:

Theorem (DN - Luperi 2015)

Consider the diophantine equation

$$c_1X_1 + \ldots + c_nX_n = Y^k \quad (k \geq 2)$$

where Rado's condition fails. If at least one of the following holds:

- $\sum_{i=1}^{k} c_i$ *is not a* $(k-1)$*-th power,*
- $(k-1) \cdot \sum_{i \in I} c_i + k \cdot \sum_{i \notin I} c_i \neq 0$ *for every* $I \subseteq \{1, \ldots, n\}$*,*

then the equation is not PR.

OPEN QUESTION

Is the Pythagorean equation partition regular?

$$X^2 + Y^2 = Z^2$$

- $X + Y = Z$ is partition regular (Schur's Theorem).
- $X + Y = Z^2$ is *not* partition regular (Csikvari-Gyarmati-Sarkozy 2012).
- $X^2 + Y = Z$ is partition regular (consequence of Sarkozy-Fürstenberg theorem).
- $X^2 + Y^2 = Z$ is *not* partition regular (DN).
- $X_1X_2 + Y^2 = Z$ is partition regular (DN-Luperi).
- $X_1X_2 + Y^2 = Z_1Z_2$ is partition regular (DN-Luperi).
- $X^3 + Y^3 = Z^3$ has no solutions (Fermat's Theorem!).

Recent papers

- High density piecewise syndeticity of sumsets (with Goldbring, Jin, Leth, Lupini, Mahlburg), *Adv. in Math.*, 2015.
- A taste of nonstandard methods in combinatorics of numbers, in *Geometry, Structure and Randomness in Combinatorics* (Matoušek, Nešetřil and Pellegrini, eds.), 2015.
- Ultrafilters as hypernatural numbers, in *Nonstandard Analysis for the Working Mathematician* (Loeb and Wolff, eds.), Springer, 2015.
- Iterated hyper-extensions and an idempotent ultrafilter proof of Rado's theorem, *Proc. Amer. Math. Soc.*, 2015.
- Intersections of shifted sets, *Electron. J. Combin.*, 2015.
- Some applications of numerosities in measure theory (with Benci and Bottazzi), *Rend. Lincei Mat. Appl.*, 2015.
- Progress on a sumset conjecture by Erdös (with Goldbring, Jin, Leth, Lupini, Mahlburg), *Canad. J. Math.* 2014.
- Nonstandard analysis and the sumset phenomenon in amenable groups (with Lupini), *Illinois J. Math.*, 2014.
- An elementary proof of Jin's Theorem with a bound, *Electron. J. Combin.*, 2014.
- Embeddability properties of difference sets, *Integers*, 2014.


The End