Arithmetic Progressions and Symbolic Dynamical Systems

Satyadev Nandakumar

March 10, 2016

van der Waerden's Theorem

Suppose \mathbb{N} is partitioned into two sets S_1 and S_2 . Then either S_1 or S_2 has arbitrarily long arithmetic progressions — i.e. $\exists S_i$ such that for every $k \ge 2$, there are integers a and b such that have

$$a, a+2b, \ldots, a+(k-1)b \in S_i.$$

Suppose \mathbb{N} is partitioned into two sets S_1 and S_2 . Then either S_1 or S_2 has arbitrarily long arithmetic progressions — i.e. $\exists S_i$ such that for every $k \ge 2$, there are integers a and b such that have

$$a, a+2b, \ldots, a+(k-1)b \in S_i.$$

Proof due to Ron Graham, that within 325, you can find an arithmetic progression of length 3:

Suppose \mathbb{N} is partitioned into two sets S_1 and S_2 . Then either S_1 or S_2 has arbitrarily long arithmetic progressions — i.e. $\exists S_i$ such that for every $k \ge 2$, there are integers a and b such that have

$$a, a+2b, \ldots, a+(k-1)b \in S_i.$$

Proof due to Ron Graham, that within 325, you can find an arithmetic progression of length 3:

Divide 325 into 65 blocks, [1-5], [6-10], ..., [321-325]. Each number is colored either red or blue (say).

Suppose \mathbb{N} is partitioned into two sets S_1 and S_2 . Then either S_1 or S_2 has arbitrarily long arithmetic progressions — i.e. $\exists S_i$ such that for every $k \ge 2$, there are integers a and b such that have

$$a, a+2b, \ldots, a+(k-1)b \in S_i.$$

Proof due to Ron Graham, that within 325, you can find an arithmetic progression of length 3:

Divide 325 into 65 blocks, [1-5], [6-10], ..., [321-325]. Each number is colored either red or blue (say).

There are 32 possible block colorings. Pigeonhole \implies 2 blocks in the first 33 are colored the same.

Proof of vdW





Erdős' Conjecture

Definition

A set $S \subseteq \mathbb{Z}$ has positive upper Banach density if

$$\limsup_{N \to \infty} \frac{|S \cap [-N, N]|}{2N + 1} > 0.$$

Erdős' Conjecture

Definition

A set $S \subseteq \mathbb{Z}$ has positive upper Banach density if $\limsup_{N \to \infty} \frac{|S \cap [-N, N]|}{2N + 1} > 0.$

Erdős conjectured that if a set S of positive upper Banach density is partitioned into two, one of the partitions has arbitrarily long arithmetic progressions.

Erdős' Conjecture

Definition

A set $S \subseteq \mathbb{Z}$ has positive upper Banach density if $\limsup_{N \to \infty} \frac{|S \cap [-N, N]|}{2N + 1} > 0.$

Erdős conjectured that if a set S of positive upper Banach density is partitioned into two, one of the partitions has arbitrarily long arithmetic progressions.

Theorem: (Szemerédi 1975)

Erdős conjecture holds.

Proof uses his "regularity lemma".



Some highlights

- 1. Roth 1956 Erdős Conjecture holds for length 3 A.P.
- 2. Szemerédi's Theorem 1975
- 3. Furstenberg's ergodic theory proof 1978
- 4. Gowers' Fourier Analytic proof, 1996
- 5. Green-Tao A.P. in primes

Infinitude of Primes — A topological proof

Theorem

There are infinitely many prime numbers.

The following proof is by Hillel Furstenberg, 1955.

Proof. Consider the topology on \mathbb{Z} where U is open if and only if it is empty, or a union of arithmetic progressions of the form

$$A(a,b) = \{a+nb \mid n \in \mathbb{Z}\}.$$

Theorem

There are infinitely many prime numbers.

The following proof is by Hillel Furstenberg, 1955.

Proof. Consider the topology on \mathbb{Z} where U is open if and only if it is empty, or a union of arithmetic progressions of the form

$$A(a,b) = \{a+nb \mid n \in \mathbb{Z}\}.$$

The basis sets A(a, b) are clopen.

Theorem

There are infinitely many prime numbers.

The following proof is by Hillel Furstenberg, 1955.

Proof. Consider the topology on \mathbb{Z} where U is open if and only if it is empty, or a union of arithmetic progressions of the form

$$A(a,b) = \{a+nb \mid n \in \mathbb{Z}\}.$$

The basis sets A(a, b) are clopen.

A finite set cannot be open. Equivalently, the complement of a finite set cannot be closed.

Theorem

There are infinitely many prime numbers.

The following proof is by Hillel Furstenberg, 1955.

Proof. Consider the topology on \mathbb{Z} where U is open if and only if it is empty, or a union of arithmetic progressions of the form

$$A(a,b) = \{a+nb \mid n \in \mathbb{Z}\}.$$

The basis sets A(a, b) are clopen.

A finite set cannot be open. Equivalently, the complement of a finite set cannot be closed.

 $\{-1,+1\}^c = \cup_{p \text{ prime}} A(p,0).$

Theorem

There are infinitely many prime numbers.

The following proof is by Hillel Furstenberg, 1955.

Proof. Consider the topology on \mathbb{Z} where U is open if and only if it is empty, or a union of arithmetic progressions of the form

$$A(a,b) = \{a+nb \mid n \in \mathbb{Z}\}.$$

The basis sets A(a, b) are clopen.

A finite set cannot be open. Equivalently, the complement of a finite set cannot be closed.

 $\{-1,+1\}^c = \cup_{p \text{ prime}} A(p,0).$

 $\{-1,1\}^c$ cannot be closed. Each A(p,0) is closed. If the number of primes were finite, then the RHS would be closed!

Topological Dynamics

Further connections between topological dynamics and integer sets.

Definition

If X is a compact space and $T: X \to X$ is a continuous map, then (X,T) is said to be a *dynamical system*.

Topological Dynamics

Further connections between topological dynamics and integer sets.

Definition

If X is a compact space and $T: X \to X$ is a continuous map, then (X,T) is said to be a *dynamical system*.

We are typically interested in the behavior of the orbit of a point or a set — e.g. $\{T^n x \mid x \in X, n \in \mathbb{Z}\}$ or

Topological Dynamics

Further connections between topological dynamics and integer sets.

Definition

If X is a compact space and $T: X \to X$ is a continuous map, then (X,T) is said to be a *dynamical system*.

We are typically interested in the behavior of the orbit of a point or a set — e.g. $\{T^n x \mid x \in X, n \in \mathbb{Z}\}$ or $\{T^n U \mid U \subset X, n \in \mathbb{Z}\}$. Pigeonhole principle and Recurrence in Open Covers

Theorem: The infinite pigeonhole principle

If $\ensuremath{\mathbb{Z}}$ is colored using finitely many colours, then at least one color appears i.o.

Theorem: The infinite pigeonhole principle

If $\mathbb Z$ is colored using finitely many colours, then at least one color appears i.o.

Theorem: Recurrence in Open Covers

Let (X,T) be a toplogical dynamical system, and $(U_{\alpha})_{\alpha\in\Omega}$ be an open cover of X. Then there is a U_{α} in the cover for which for infinitely many n, $U_{\alpha} \cap T^{n}U_{\alpha} \neq \emptyset$.

Pigeonhole Principle implies BROC

X is compact. Hence some finite subcover U_1, \ldots, U_n covers X.

Pick $x \in X$. Consider its orbit

 $\ldots, T^{-1}x, x, Tx, \ldots$

Pigeonhole Principle implies BROC

X is compact. Hence some finite subcover U_1, \ldots, U_n covers X.

Pick $x \in X$. Consider its orbit

 $\ldots, T^{-1}x, x, Tx, \ldots$

Pigeonhole Principle \Rightarrow there is some U_i , $1 \le i \le n$ such that for infinitely many n, $T^n x \in U_i$.

Pick $x \in X$. Consider its orbit

 $\ldots, T^{-1}x, x, Tx, \ldots$

Pigeonhole Principle \Rightarrow there is some U_i , $1 \le i \le n$ such that for infinitely many n, $T^n x \in U_i$.

Consider $O = \{n \in \mathbb{Z} \mid T^n x \in U_i\}$. Pick some $n_0 \in O$.

Pick $x \in X$. Consider its orbit

 $\ldots, T^{-1}x, x, Tx, \ldots$

Pigeonhole Principle \Rightarrow there is some U_i , $1 \le i \le n$ such that for infinitely many n, $T^n x \in U_i$.

Consider $O = \{n \in \mathbb{Z} \mid T^n x \in U_i\}$. Pick some $n_0 \in O$.

 $\forall n \in O, \quad T^{n_0}x = T^{n_0-n}T^nx.$ Hence $T^{n_0}x \in U_i \cap T^{n_0-n}U_i.$

Pick $x \in X$. Consider its orbit

 $\ldots, T^{-1}x, x, Tx, \ldots$

Pigeonhole Principle \Rightarrow there is some U_i , $1 \le i \le n$ such that for infinitely many n, $T^n x \in U_i$.

Consider $O = \{n \in \mathbb{Z} \mid T^n x \in U_i\}$. Pick some $n_0 \in O$.

 $\forall n \in O, \quad T^{n_0}x = T^{n_0-n}T^nx.$ Hence $T^{n_0}x \in U_i \cap T^{n_0-n}U_i.$

Hence for infinitely many n, $U_i \cap T^{n_0-n}U_i \neq \emptyset$.

Let Ω be the finite set of colors. Let A be a coloring of \mathbb{Z} . Consider the tds $(\Omega^{\mathbb{Z}}, T)$, where T is the right-shift. Represent A by $a \in \Omega^{\mathbb{Z}}$.

Let Ω be the finite set of colors. Let A be a coloring of \mathbb{Z} . Consider the tds $(\Omega^{\mathbb{Z}}, T)$, where T is the right-shift. Represent A by $a \in \Omega^{\mathbb{Z}}$. Define

$$X_a = \overline{\{T^n a \mid n \in Z\}}.$$

Let Ω be the finite set of colors. Let A be a coloring of \mathbb{Z} . Consider the tds $(\Omega^{\mathbb{Z}}, T)$, where T is the right-shift. Represent A by $a \in \Omega^{\mathbb{Z}}$. Define

$$X_a = \overline{\{T^n a \mid n \in Z\}}.$$

Consider the cover $(U_c)_{c\in\Omega}$ where U_c are the points in X_a with 0 colored c.

Let Ω be the finite set of colors. Let A be a coloring of \mathbb{Z} . Consider the tds $(\Omega^{\mathbb{Z}}, T)$, where T is the right-shift. Represent A by $a \in \Omega^{\mathbb{Z}}$. Define

$$X_a = \overline{\{T^n a \mid n \in Z\}}.$$

Consider the cover $(U_c)_{c\in\Omega}$ where U_c are the points in X_a with 0 colored c.

By recurrence in open covers,

 $\exists c \in \Omega \ \exists^{\infty} n \ U_c \cap T^n U_c \neq \emptyset.$

(1)

Let Ω be the finite set of colors. Let A be a coloring of \mathbb{Z} . Consider the tds $(\Omega^{\mathbb{Z}}, T)$, where T is the right-shift. Represent A by $a \in \Omega^{\mathbb{Z}}$. Define

$$X_a = \overline{\{T^n a \mid n \in Z\}}.$$

Consider the cover $(U_c)_{c\in\Omega}$ where U_c are the points in X_a with 0 colored c.

By recurrence in open covers,

 $\exists c \in \Omega \ \exists^{\infty} n \ U_c \cap T^n U_c \neq \emptyset.$ ⁽¹⁾

Since X_a is the orbit closure of a, there is a $k \in \mathbb{Z}$ such that $T^k a \in U_c \cap T^n U_c$. That is, $a_{-k} = c$ and $a_{-k+n} = c$. This is true for all n in (1).

van der Waerden's Theorem and Multiple Recurrence in Open Covers The version of recurrence in tds which is equivalent to Van der Waerden's theorem is the following.

Theorem: Multiple Recurrence in Open Covers

Let (X,T) be a topological dynamical system and $(U_{\alpha})_{\alpha\in\Omega}$ be an open cover of X. Then there is a U_{α} in the cover such that

 $\forall k \ge 2 \ \exists n > 0 \qquad U_{\alpha} \cap T^{n} U_{\alpha} \cap \dots \cap T^{(k-1)n} U_{\alpha} \neq \emptyset.$

Szemerédi's Theorem

Dynamical Systems view of Szemerédi's Theorem

For Szemerédi's theorem, we now have to consider *measure* as well. **Definition**

A measure-preserving topological dynamical system is a quadruple (X, \mathcal{X}, μ, T) is a space where

- X is a compact topological space,
- \mathcal{X} is a σ -algebra on X,
- μ a probability measure on $\mathcal X$ and
- $T: X \to X$ is a measure-preserving homeomorphism.

Fursteneberg Multiple Recurrence Theorem

Theorem: Multiple Recurrence Theorem

Let (X, \mathcal{X}, μ, T) be a mtds. Then for any $E \in \mathcal{X}$ with $\mu(E) > 0$, we have

 $\mu(E \cap T^n E \cap \dots \cap T^{(k-1)n} E) > 0.$

Furstenberg Correspondence Principle

Lemma

Let (X, \mathcal{X}, μ, T) be as in the FMRT, and *E* have positive measure. Then there is an *F*, $\mu(F) > 0$ such that for every *x* in *F*,

$$\{n \in \mathbb{Z} \mid T^n x \in E\}$$

has positive upper density.

Proof.

- Define $\delta_N(x)$ to be the frequency with which $T^{-N}x$, ..., T^Nx visits *E*. Then the expected value of δ_N is $\mu(E)$.
- By an Egorov-style argument, show that the probability of

$$\left\{ x \in X \mid \delta_N(x) \ge \frac{1}{2}\mu(E) \right\}$$

is at least $1/2\mu(E)$.

• Then F is the set $\bigcap_N \bigcup_{m>N} A_m$.

Let AP_k denote the set of k-length arithmetic progressions in \mathbb{Z} . For each $\alpha = (a_1, \ldots, a_k)$ which is an A.P., define

$$B_{\alpha} = \{ x \in X \mid T^{a_1}x, \dots, T^{a_k}x \in E \}.$$

Let AP_k denote the set of k-length arithmetic progressions in \mathbb{Z} . For each $\alpha = (a_1, \ldots, a_k)$ which is an A.P., define

$$B_{\alpha} = \{ x \in X \mid T^{a_1}x, \dots, T^{a_k}x \in E \}.$$

Pick $F \subseteq X$ as in the previous lemma. Then for every $x \in F$, the set $\{n \in \mathbb{Z} \mid T^n x \in E\}$ has positive upper density.

Let AP_k denote the set of k-length arithmetic progressions in \mathbb{Z} . For each $\alpha = (a_1, \ldots, a_k)$ which is an A.P., define

$$B_{\alpha} = \{ x \in X \mid T^{a_1}x, \dots, T^{a_k}x \in E \}.$$

Pick $F \subseteq X$ as in the previous lemma. Then for every $x \in F$, the set $\{n \in \mathbb{Z} \mid T^n x \in E\}$ has positive upper density.

By Szemerédi's theorem, the visit time set has a *k*-term arithmetic progression β such that $\mu(B_{\beta}) > 0$.

Let AP_k denote the set of k-length arithmetic progressions in \mathbb{Z} . For each $\alpha = (a_1, \ldots, a_k)$ which is an A.P., define

$$B_{\alpha} = \{ x \in X \mid T^{a_1}x, \dots, T^{a_k}x \in E \}.$$

Pick $F \subseteq X$ as in the previous lemma. Then for every $x \in F$, the set $\{n \in \mathbb{Z} \mid T^n x \in E\}$ has positive upper density.

By Szemerédi's theorem, the visit time set has a *k*-term arithmetic progression β such that $\mu(B_{\beta}) > 0$.

Thus some $b, n \in \mathbb{Z}$ exist such that $T^b B_a \subseteq E \cap T^n E \cap \cdots \cap T^{(k-1)n} E$, and $\mu(T^b B_a) > 0$. [A.P. starting with 0]

Let A have positive upper density, represented as $a \in 2^{\mathbb{Z}}$. Consider the system $(2^Z, T)$, where TB = B + 1 is the right shift.

Let A have positive upper density, represented as $a \in 2^{\mathbb{Z}}$. Consider the system $(2^Z, T)$, where TB = B + 1 is the right shift.

Take X_a to be the orbit closure of a. Let E be the sequences in X_a with their 0^{th} co-ordinate 1.

Let A have positive upper density, represented as $a \in 2^{\mathbb{Z}}$. Consider the system $(2^Z, T)$, where TB = B + 1 is the right shift.

Take X_a to be the orbit closure of a. Let E be the sequences in X_a with their 0^{th} co-ordinate 1.

If we can find an invariant measure μ with $\mu(E) > 0$, then by FMRT, we can conclude Szemerédi's theorem.

Let A have positive upper density, represented as $a \in 2^{\mathbb{Z}}$. Consider the system $(2^Z, T)$, where TB = B + 1 is the right shift.

Take X_a to be the orbit closure of a. Let E be the sequences in X_a with their 0^{th} co-ordinate 1.

If we can find an invariant measure μ with $\mu(E) > 0$, then by FMRT, we can conclude Szemerédi's theorem.

The invariant measure is constructed using the Banach-Alaoglu theorem.

Furstenberg Multiple Recurrence - the "random" case

Consider $B = (2^{\mathbb{Z}}, \mathcal{B}, T, \mu)$ where T is the right-shift and μ the product measure specified by $\mu(0)$ and $\mu(1)$.

Theorem. *B* has multiple recurrence.

Consider $B = (2^{\mathbb{Z}}, \mathcal{B}, T, \mu)$ where T is the right-shift and μ the product measure specified by $\mu(0)$ and $\mu(1)$.

Theorem. *B* has multiple recurrence.

Proof. It suffices to verify MR for cylinders.

Weak Mixing Systems - Bernoulli Systems

Consider $B = (2^{\mathbb{Z}}, \mathcal{B}, T, \mu)$ where T is the right-shift and μ the product measure specified by $\mu(0)$ and $\mu(1)$.

Theorem. *B* has multiple recurrence.

Proof. It suffices to verify MR for cylinders.

Let $E = (X_{i_1} = a_1, \dots, X_{i_k} = a_k)$.

Weak Mixing Systems - Bernoulli Systems

Consider $B = (2^{\mathbb{Z}}, \mathcal{B}, T, \mu)$ where T is the right-shift and μ the product measure specified by $\mu(0)$ and $\mu(1)$.

Theorem. *B* has multiple recurrence.

Proof. It suffices to verify MR for cylinders.

Let
$$E = (X_{i_1} = a_1, \dots, X_{i_k} = a_k)$$
.

Then for large n, the sets E, $T^n E$, ..., $T^{(k-1)n}E$ depend on disjoint sets of indices.

Consider $B = (2^{\mathbb{Z}}, \mathcal{B}, T, \mu)$ where T is the right-shift and μ the product measure specified by $\mu(0)$ and $\mu(1)$.

Theorem. *B* has multiple recurrence.

Proof. It suffices to verify MR for cylinders.

Let
$$E = (X_{i_1} = a_1, \dots, X_{i_k} = a_k)$$
.

Then for large n, the sets E, $T^n E$, ..., $T^{(k-1)n}E$ depend on disjoint sets of indices.

Hence $\mu(E \cap T^n E \cap \cdots \cap T^{(k-1)n} E) = \mu(E)^k$ by independence and the measure preservation of T. $\mu(E)^k > 0$.

Furstenberg Multiple Recurrence - the "structured" case

Consider $X = (\mathbb{R}/\mathbb{Z}, T_{\alpha})$ where $T_{\alpha}(x) = (x + \alpha) \mod 1$. This is an *almost-periodic* system —

 $\forall \varepsilon > 0 \quad \forall x \in \mathbb{R}/\mathbb{Z} \quad \exists N \forall n \qquad ||T_{\alpha}^{n} x - T_{\alpha}^{n+N} x|| < \varepsilon.$

Theorem. *X* has multiple recurrence.

Consider $X = (\mathbb{R}/\mathbb{Z}, T_{\alpha})$ where $T_{\alpha}(x) = (x + \alpha) \mod 1$. This is an *almost-periodic* system —

 $\forall \varepsilon > 0 \quad \forall x \in \mathbb{R}/\mathbb{Z} \quad \exists N \forall n \qquad ||T_{\alpha}^{n} x - T_{\alpha}^{n+N} x|| < \varepsilon.$

Theorem. *X* has multiple recurrence.

Proof. Let $k \ge 3$. Fix $\varepsilon > 0$ and let $(x - \varepsilon, x + \varepsilon) \subseteq V$.

Consider $X = (\mathbb{R}/\mathbb{Z}, T_{\alpha})$ where $T_{\alpha}(x) = (x + \alpha) \mod 1$. This is an *almost-periodic* system —

 $\forall \varepsilon > 0 \quad \forall x \in \mathbb{R}/\mathbb{Z} \quad \exists N \forall n \qquad ||T_{\alpha}^{n} x - T_{\alpha}^{n+N} x|| < \varepsilon.$

Theorem. *X* has multiple recurrence.

Proof. Let $k \ge 3$. Fix $\varepsilon > 0$ and let $(x - \varepsilon, x + \varepsilon) \subseteq V$.

Using continued fractions, $\exists P, Q \in \mathbb{Z} |Q\alpha - P| < \varepsilon/k$.

Consider $X = (\mathbb{R}/\mathbb{Z}, T_{\alpha})$ where $T_{\alpha}(x) = (x + \alpha) \mod 1$. This is an *almost-periodic* system —

 $\forall \varepsilon > 0 \quad \forall x \in \mathbb{R}/\mathbb{Z} \quad \exists N \forall n \qquad ||T_{\alpha}^{n} x - T_{\alpha}^{n+N} x|| < \varepsilon.$

Theorem. *X* has multiple recurrence.

Proof. Let $k \ge 3$. Fix $\varepsilon > 0$ and let $(x - \varepsilon, x + \varepsilon) \subseteq V$.

Using continued fractions, $\exists P, Q \in \mathbb{Z} |Q\alpha - P| < \varepsilon/k$.

For any n, $|(x + n\alpha) \mod 1 - (x + (n + Q)\alpha) \mod 1| < \varepsilon/k$.

i.e. $\forall 0 \leq j \leq k-1$, $|x - T_{\alpha}^{jQ}x| \leq j\varepsilon/k \leq \varepsilon$. Hence $T^{jQ}x \in V$.

Further...

Decompose the system into a weak mixing and an almost periodic part if possible, and prove multiple recurrence for these part separately. Decompose the system into a weak mixing and an almost periodic part if possible, and prove multiple recurrence for these part separately.

General systems: build a tower of maps $X \to K_{\alpha} \to \cdots \to K_1$ where in each map $A \to B$, B is a Kronecker factor of A.

Decompose the system into a weak mixing and an almost periodic part if possible, and prove multiple recurrence for these part separately.

General systems: build a tower of maps $X \to K_{\alpha} \to \cdots \to K_1$ where in each map $A \to B$, *B* is a Kronecker factor of *A*.

Lift multiple recurrence from the bottommost system all the way to X.

Effective Versions