Forcing as a tool to prove theorems

$$(\Vdash_{\mathbb{P}} \varphi) \Longrightarrow (V \models \varphi)$$

Mathematics Colloquium,
Bar-Ilan University
10-November-2013

Assaf Rinot
BIU

These slides are be available at:
http://www.assafrinot.com/talk/biu013

The Continuum Hypothesis

Theorem (Cantor, 1873)

$|\mathbb{N}| < |\mathbb{R}|$.

The Continuum Hypothesis

Theorem (Cantor, 1873)

$|\mathbb{N}| < |\mathbb{R}|$.

Cantor's Continuum Hypothesis

If $\mathbb{N} \subseteq A \subseteq \mathbb{R}$, then either $|A| = |\mathbb{N}|$ or $|A| = |\mathbb{R}|$.

The Continuum Hypothesis

Theorem (Cantor, 1873)

$|\mathbb{N}| < |\mathbb{R}|$.

Cantor's Continuum Hypothesis

If $\mathbb{N} \subseteq A \subseteq \mathbb{R}$, then either $|A| = |\mathbb{N}|$ or $|A| = |\mathbb{R}|$.

A question arises

Is CH true? Hilbert put this question on top of his famous 1900 list of major open problems.

The Continuum Hypothesis

Theorem (Cantor, 1873)

$|\mathbb{N}| < |\mathbb{R}|$.

Cantor's Continuum Hypothesis

If $\mathbb{N} \subseteq A \subseteq \mathbb{R}$, then either $|A| = |\mathbb{N}|$ or $|A| = |\mathbb{R}|$.

A question arises

Is CH true? Hilbert put this question on top of his famous 1900 list of major open problems.

A surprising answer (Cohen, 1963)

CH is independent of the usual axioms of set theory (ZFC).

The Continuum Hypothesis

Theorem (Cantor, 1873)

$|\mathbb{N}| < |\mathbb{R}|$.

Cantor's Continuum Hypothesis

If $\mathbb{N} \subseteq A \subseteq \mathbb{R}$, then either $|A| = |\mathbb{N}|$ or $|A| = |\mathbb{R}|$.

A question arises

Is CH true? Hilbert put this question on top of his famous 1900 list of major open problems.

A surprising answer (Cohen, 1963)

CH is independent of the usual axioms of set theory (ZFC).
To prove this, he invented the method of <u>forcing</u>.

Plan

The method of forcing proved itself very useful, leading to literally hundreds of independence results.

Plan

The method of forcing proved itself very useful, leading to literally hundreds of independence results.

The method turned out to be useful also in proving "standard" theorems (that is, implications).

Plan

The method of forcing proved itself very useful, leading to literally hundreds of independence results.

The method turned out to be useful also in proving "standard" theorems (that is, implications).

Today's talk will consist of two parts:

1. What is forcing?
   1.1 Recasting the theory of algebraic fields
   1.2 A (semi-)formal description of forcing
2. A sample of theorems proved using forcing

Part 1

Recasting field theory

A field is a collection F of *objects*, together with *binary operations* $+, \cdot$, and two distinguished elements $0, 1$, that interact as follows:

Recasting field theory

A field is a collection F of *objects*, together with *binary operations* $+, \cdot$, and two distinguished elements $0, 1$, that interact as follows:

- for every two objects a, b from F, the outcome $\cdot(a, b)$ is again in F.

Recasting field theory

A field is a collection F of *objects*, together with *binary operations* $+, \cdot$, and two distinguished elements $0, 1$, that interact as follows:

- for every two objects a, b from F, the outcome $\cdot(a, b)$ is again in F. Same goes to $+$;

Recasting field theory

A field is a collection F of *objects*, together with *binary operations* $+, \cdot$, and two distinguished elements $0, 1$, that interact as follows:

- for every two objects a, b from F, the outcome $\cdot(a, b)$ is again in F. Same goes to $+$;
- $\cdot(\cdot(a, b), c) = \cdot(a, \cdot(b, c))$ for all objects a, b, c in F.

Recasting field theory

A field is a collection F of *objects*, together with *binary operations* $+, \cdot$, and two distinguished elements $0, 1$, that interact as follows:

- for every two objects a, b from F, the outcome $\cdot(a, b)$ is again in F. Same goes to $+$;
- $\cdot(\cdot(a, b), c) = \cdot(a, \cdot(b, c))$ for all objects a, b, c in F. Also $+$;

Recasting field theory

A field is a collection F of *objects*, together with *binary operations* $+, \cdot$, and two distinguished elements $0, 1$, that interact as follows:

- for every two objects a, b from F, the outcome $\cdot(a, b)$ is again in F. Same goes to $+$;
- $\cdot(\cdot(a, b), c) = \cdot(a, \cdot(b, c))$ for all objects a, b, c in F. Also $+$;
- $\cdot(a, b) = \cdot(b, a)$ for all objects a, b in F. Same goes to $+$;

Recasting field theory

A field is a collection F of *objects*, together with *binary operations* $+, \cdot$, and two distinguished elements $0, 1$, that interact as follows:

- for every two objects a, b from F, the outcome $\cdot(a, b)$ is again in F. Same goes to $+$;
- $\cdot(\cdot(a, b), c) = \cdot(a, \cdot(b, c))$ for all objects a, b, c in F. Also $+$;
- $\cdot(a, b) = \cdot(b, a)$ for all objects a, b in F. Same goes to $+$;
- $+(a, 0) = a = \cdot(a, 1)$ for any object a in F;

Recasting field theory

A field is a collection F of *objects*, together with *binary operations* $+, \cdot$, and two distinguished elements $0, 1$, that interact as follows:

- for every two objects a, b from F, the outcome $\cdot(a, b)$ is again in F. Same goes to $+$;
- $\cdot(\cdot(a, b), c) = \cdot(a, \cdot(b, c))$ for all objects a, b, c in F. Also $+$;
- $\cdot(a, b) = \cdot(b, a)$ for all objects a, b in F. Same goes to $+$;
- $+(a, 0) = a = \cdot(a, 1)$ for any object a in F;
- for every a, there exists a' such that $+(a, a') = 0$;
- for every a distinct from 0, there is a'': $\cdot(a, a'') = 1$;

Recasting field theory

A field is a collection F of *objects*, together with *binary operations* $+, \cdot$, and two distinguished elements $0, 1$, that interact as follows:

- for every two objects a, b from F, the outcome $\cdot(a, b)$ is again in F. Same goes to $+$;
- $\cdot(\cdot(a, b), c) = \cdot(a, \cdot(b, c))$ for all objects a, b, c in F. Also $+$;
- $\cdot(a, b) = \cdot(b, a)$ for all objects a, b in F. Same goes to $+$;
- $+(a, 0) = a = \cdot(a, 1)$ for any object a in F;
- for every a, there exists a' such that $+(a, a') = 0$;
- for every a distinct from 0, there is a'': $\cdot(a, a'') = 1$;
- $\cdot(a, +(b, c)) = +(\cdot(a, b), \cdot(a, c))$ for all objects a, b, c in F.

Recasting field theory

A field is a collection F of *objects*, together with *binary operations* $+, \cdot$, and two distinguished elements $0, 1$, that interact as follows:

- for every two objects a, b from F, the outcome $\cdot(a, b)$ is again in F. Same goes to $+$;
- $\cdot(\cdot(a, b), c) = \cdot(a, \cdot(b, c))$ for all objects a, b, c in F. Also $+$;
- $\cdot(a, b) = \cdot(b, a)$ for all objects a, b in F. Same goes to $+$;
- $+(a, 0) = a = \cdot(a, 1)$ for any object a in F;
- for every a, there exists a' such that $+(a, a') = 0$;
- for every a distinct from 0, there is a'': $\cdot(a, a'') = 1$;
- $\cdot(a, +(b, c)) = +(\cdot(a, b), \cdot(a, c))$ for all objects a, b, c in F.

A statement in the language of field theory is

A (well-formed) formula that uses symbols of first order-logic $(\wedge, \vee, \exists, \forall, =, \ldots)$ together with $+, \cdot, 0, 1$.

Recasting field theory

A <u>field</u> is a collection F of *objects*, together with *binary operations* $+, \cdot$, and two distinguished elements $0, 1$, that interact as follows:

- for every two objects a, b from F, the outcome $\cdot(a, b)$ is again in F. Same goes to $+$;
- $\cdot(\cdot(a, b), c) = \cdot(a, \cdot(b, c))$ for all objects a, b, c in F. Also $+$;
- $\cdot(a, b) = \cdot(b, a)$ for all objects a, b in F. Same goes to $+$;
- $+(a, 0) = a = \cdot(a, 1)$ for any object a in F;
- for every a, there exists a' such that $+(a, a') = 0$;
- for every a distinct from 0, there is a'': $\cdot(a, a'') = 1$;
- $\cdot(a, +(b, c)) = +(\cdot(a, b), \cdot(a, c))$ for all objects a, b, c in F.

A statement in the language of field theory is

said to be <u>valid</u>, if it is true in any field. For example:

$$(\forall a \forall b \forall c)((+(a, b) = +(a, c)) \to (b = c)).$$

Recasting field theory

A field is a collection F of *objects*, together with *binary operations* $+, \cdot$, and two distinguished elements $0, 1$, that interact as follows:

- for every two objects a, b from F, the outcome $\cdot(a, b)$ is again in F. Same goes to $+$;
- $\cdot(\cdot(a, b), c) = \cdot(a, \cdot(b, c))$ for all objects a, b, c in F. Also $+$;
- $\cdot(a, b) = \cdot(b, a)$ for all objects a, b in F. Same goes to $+$;
- $+(a, 0) = a = \cdot(a, 1)$ for any object a in F;
- for every a, there exists a' such that $+(a, a') = 0$;
- for every a distinct from 0, there is a'': $\cdot(a, a'') = 1$;
- $\cdot(a, +(b, c)) = +(\cdot(a, b), \cdot(a, c))$ for all objects a, b, c in F.

A statement in the language of field theory is

said to be consistent, if it is true in some field. For example:

$$(\forall a)(+(a, a) = 0).$$

Recasting field theory

A field is a collection F of *objects*, together with *binary operations* $+, \cdot$, and two distinguished elements $0, 1$, that interact as follows:

- for every two objects a, b from F, the outcome $\cdot(a, b)$ is again in F. Same goes to $+$;
- $\cdot(\cdot(a, b), c) = \cdot(a, \cdot(b, c))$ for all objects a, b, c in F. Also $+$;
- $\cdot(a, b) = \cdot(b, a)$ for all objects a, b in F. Same goes to $+$;
- $+(a, 0) = a = \cdot(a, 1)$ for any object a in F;
- for every a, there exists a' such that $+(a, a') = 0$;
- for every a distinct from 0, there is a'': $\cdot(a, a'') = 1$;
- $\cdot(a, +(b, c)) = +(\cdot(a, b), \cdot(a, c))$ for all objects a, b, c in F.

A statement in the language of field theory is

said to be independent, if both the statement and its negation are consistent. For example:

$$\exists x(\cdot(x, x) = +(1, 1))$$

Fields

Summary

For every statement φ in the language of field theory, exactly one of following holds:

- φ is valid;
- $\neg\varphi$ is valid;
- φ is independent. That is, both φ and $\neg\varphi$ are consistent.

Fields

Summary

For every statement φ in the language of field theory, exactly one of following holds:

- φ is valid;
- $\neg\varphi$ is valid;
- φ is independent. That is, both φ and $\neg\varphi$ are consistent.

The independence of a statement φ is sometime seen by passing to a subfield or to a field extension.

Passing to a subfield

Proposition

The statement $\exists x(+(\cdot(x, x), 1) = 0)$ is independent of the axioms of fields.

Passing to a subfield

Proposition

The statement $\exists x(+(\cdot(x,x),1)=0)$ is independent of the axioms of fields.

Proof.

Let $\mathbb{C}$ denote the field of complex numbers. We have

$$\mathbb{C} \models i^2+1=0.$$

Passing to a subfield

Proposition

The statement $\exists x(+(\cdot(x,x),1)=0)$ is independent of the axioms of fields.

Proof.

Let $\mathbb{C}$ denote the field of complex numbers. We have

$$\mathbb{C} \models i^2 + 1 = 0.$$

In particular, $\mathbb{C} \models \exists x(+(\cdot(x,x),1)=0)$.

Passing to a subfield

Proposition

The statement $\exists x(+(\cdot(x,x),1)=0)$ is independent of the axioms of fields.

Proof.

Let $\mathbb{C}$ denote the field of complex numbers. We have

$$\mathbb{C} \models i^2 + 1 = 0.$$

In particular, $\mathbb{C} \models \exists x(+(\cdot(x,x),1)=0)$.
On the other hand, the subfield $\mathbb{R}$ of real numbers satisfies the negation: $\mathbb{R} \models \neg(\exists x(+(\cdot(x,x),1)=0))$. $\square$

Passing to a field extension

Recall..

If $\mathbb{F}$ is a field, then the objects of the polynomial ring $\mathbb{F}[X]$ are obtained via the following recursive process:

- $\mathbb{F}_0[X] = \{0\}$;
- $\mathbb{F}_{n+1}[X] := \{\alpha X^n + q \mid \alpha \in \mathbb{F}, q \in \mathbb{F}_n[X]\}$.

Passing to a field extension

Recall..

If $\mathbb{F}$ is a field, then the objects of the polynomial ring $\mathbb{F}[X]$ are obtained via the following recursive process:

- $\mathbb{F}_0[X] = \{0\}$;
- $\mathbb{F}_{n+1}[X] := \{(\alpha, q) \mid \alpha \in \mathbb{F}, q \in \mathbb{F}_n[X]\}$.

Passing to a field extension

Recall..

If $\mathbb{F}$ is a field, then the objects of the polynomial ring $\mathbb{F}[X]$ are obtained via the following recursive process:

- $\mathbb{F}_0[X] = \{0\}$;
- $\mathbb{F}_{n+1}[X] := \{(\alpha, q) \mid \alpha \in \mathbb{F}, q \in \mathbb{F}_n[X]\}$.

Fact

If $\mathbb{F}$ is a field, and $\mathfrak{I}$ is a maximal ideal in the polynomial ring $\mathbb{F}[X]$, then the quotient $\mathbb{F}[X]/\mathfrak{I}$ is a field extending $\mathbb{F}$.

Passing to a field extension, cont'

Application

The statement $\exists x(\cdot(x, x) = +(1, 1))$ is independent of the axioms of fields.

Passing to a field extension, cont'

Application

The statement $\exists x(\cdot(x,x) = +(1,1))$ is independent of the axioms of fields.

Proof.

The statement is not valid in the field of rational numbers $\mathbb{Q}$.

Passing to a field extension, cont'

Application

The statement $\exists x(\cdot(x, x) = +(1, 1))$ is independent of the axioms of fields.

Proof.

The statement is not valid in the field of rational numbers $\mathbb{Q}$.
In particular, the polynomial $X^2 - 2$ is irreducible in $\mathbb{Q}[X]$, and hence the generated ideal $(X^2 - 2)$ is maximal.
Consequently, $\mathbb{Q}[X]/(X^2 - 2)$ is a field (extending $\mathbb{Q}$).

Passing to a field extension, cont'

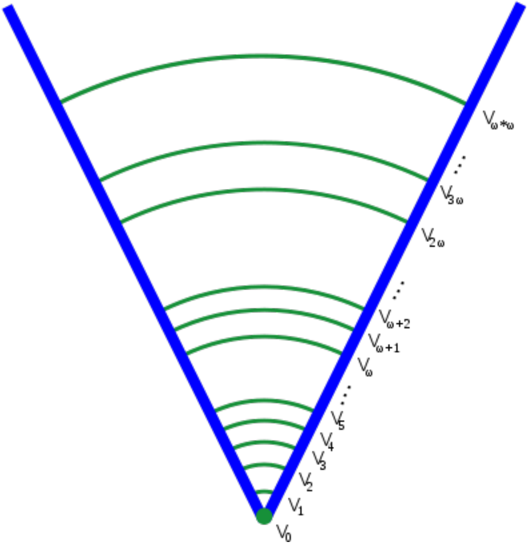
Application

The statement $\exists x(\cdot(x,x) = +(1,1))$ is independent of the axioms of fields.

Proof.

The statement is not valid in the field of rational numbers $\mathbb{Q}$.
In particular, the polynomial $X^2 - 2$ is irreducible in $\mathbb{Q}[X]$, and hence the generated ideal $(X^2 - 2)$ is maximal.
Consequently, $\mathbb{Q}[X]/(X^2 - 2)$ is a field (extending $\mathbb{Q}$).
Finally, note that $\exists x(\cdot(x,x) = +(1,1))$ is valid in $\mathbb{Q}[X]/(X^2 - 2)$, as witnessed by the residue class of X. $\square$

Set Theory


$V_{\omega*\omega}$
...
$V_{3\omega}$
$V_{2\omega}$
...
$V_{\omega+2}$
$V_{\omega+1}$
V_{ω}
...
V_5
V_4
V_3
V_2
V_1
V_0

Set Theory (à la ZFC)

A universe of set theory is a collection V of *objects*, together with a *binary relation* $\in$ that interact in the following way:

Set Theory (à la ZFC)

A universe of set theory is a collection V of *objects*, together with a *binary relation* $\in$ that interact in the following way:

(empty set) $\exists x \forall y \forall z (z \in x \to z \in y)$
(pairing) $\forall x \forall y \exists z (x \in z \wedge y \in z)$
(union) $\forall \mathcal{F} \exists u \forall Y \forall x ((x \in Y \wedge Y \in \mathcal{F}) \to x \in u)$
(power set) $\forall x \exists P \forall y ((\forall z ((z \in y) \to (z \in x))) \to z \in P)$
(extensionality) $\forall x \forall y (\forall z (z \in x \leftrightarrow z \in y) \to (x = y))$

Set Theory (à la ZFC)

A universe of set theory is a collection V of *objects*, together with a *binary relation* $\in$ that interact in the following way:

(empty set) $\exists x \forall y \forall z (z \in x \to z \in y)$
(pairing) $\forall x \forall y \exists z (x \in z \land y \in z)$
(union) $\forall \mathcal{F} \exists u \forall Y \forall x ((x \in Y \land Y \in \mathcal{F}) \to x \in u)$
(power set) $\forall x \exists P \forall y ((\forall z ((z \in y) \to (z \in x))) \to z \in P)$
(extensionality) $\forall x \forall y (\forall z (z \in x \leftrightarrow z \in y) \to (x = y))$
(infinity)
(foundation)
(replacement)
(choice)

Set Theory (à la ZFC)

A universe of set theory is a collection V of *objects*, together with a *binary relation* $\in$ that interact in the following way:

(empty set) $\exists x \forall y \forall z (z \in x \to z \in y)$
(pairing) $\forall x \forall y \exists z (x \in z \wedge y \in z)$
(union) $\forall \mathcal{F} \exists u \forall Y \forall x ((x \in Y \wedge Y \in \mathcal{F}) \to x \in u)$
(power set) $\forall x \exists P \forall y ((\forall z ((z \in y) \to (z \in x))) \to z \in P)$
(extensionality) $\forall x \forall y (\forall z (z \in x \leftrightarrow z \in y) \to (x = y))$
(infinity)
(foundation)
(replacement)
(choice)

A statement in the language of set theory is

A (well-formed) formula that uses symbols of first order-logic together with $\in$.

Hierarchies of sets: the well-founded hierarchy

Notation

Write $A \subseteq B$ whenever $\forall x(x \in A \to x \in B)$.
The power set $\mathcal{P}(B) := \{A \mid A \subseteq B\}$.

Hierarchies of sets: the well-founded hierarchy

Notation

Write $A \subseteq B$ whenever $\forall x(x \in A \to x \in B)$.
The power set $\mathcal{P}(B) := \{A \mid A \subseteq B\}$.

Fact

Suppose that $(V, \in) \models$ *ZFC.*
In V*, recursively define:*

- $V_0 := \emptyset$;
- $V_{\alpha+1} := \mathcal{P}(V_\alpha)$ *for every ordinal* α;
- $V_\delta := \bigcup_{\alpha<\delta} V_\alpha$ *for every nonzero limit ordinal* δ.

Then an object x *is in* V *iff* x *is in* V_α *for some ordinal* α.

Hierarchies of sets: the names hierarchy

Suppose that $(V, \in) \models$ ZFC, and $\mathbb{P} = \langle P, \leq \rangle$ is a poset in V.

Definition

The power set $\mathcal{P}(B) := \{A \mid A \subseteq B\}$.

The $\mathbb{P}$-power set $\mathbb{P}(B) := \{A \mid A \subseteq P \times B\}$.

Hierarchies of sets: the names hierarchy

Suppose that $(V, \in) \models$ ZFC, and $\mathbb{P} = \langle P, \leq \rangle$ is a poset in V.

Definition

The power set $\mathcal{P}(B) := \{A \mid A \subseteq B\}$.

The $\mathbb{P}$-power set $\mathbb{P}(B) := \{A \mid A \subseteq P \times B\}$.

Definition

In V, recursively define:

- $V_0^{\mathbb{P}} := \emptyset$;
- $V_{\alpha+1}^{\mathbb{P}} := \mathbb{P}(V_\alpha)$ for every ordinal α;
- $V_\delta^{\mathbb{P}} := \bigcup_{\alpha<\delta} V_\alpha^{\mathbb{P}}$ for every nonzero limit ordinal δ.

Say that x is a $\underline{\mathbb{P}\text{-name}}$ iff x is in $V_\alpha^{\mathbb{P}}$ for some ordinal α.

Hierarchies of sets: the names hierarchy

Suppose that $(V, \in) \models \mathsf{ZFC}$, and $\mathbb{P} = \langle P, \leq \rangle$ is a poset in V.

Definition

Let $V^{\mathbb{P}}$ denote the collection of all $\mathbb{P}$-names. Given a subset $G \subseteq P$, define for every $\mathbb{P}$-name x, the interpretation x/G by recursion on the least α with $x \in V^{\mathbb{P}}_\alpha$:

$$x/G = \{y/G \mid \exists p \in G \ (p, y) \in x\}.$$

Definition

In V, recursively define:

- $V^{\mathbb{P}}_0 := \emptyset$;
- $V^{\mathbb{P}}_{\alpha+1} := \mathbb{P}(V_\alpha)$ for every ordinal α;
- $V^{\mathbb{P}}_\delta := \bigcup_{\alpha<\delta} V^{\mathbb{P}}_\alpha$ for every nonzero limit ordinal δ.

Say that x is a $\underline{\mathbb{P}\text{-name}}$ iff x is in $V^{\mathbb{P}}_\alpha$ for some ordinal α.

Hierarchies of sets: the names hierarchy

Suppose that $(V, \in) \models \mathrm{ZFC}$, and $\mathbb{P} = \langle P, \leq \rangle$ is a poset in V.

Definition

Let $V^{\mathbb{P}}$ denote the collection of all $\mathbb{P}$-names. Given a subset $G \subseteq P$, we let:

$$V[G] := V^{\mathbb{P}}/G = \{x/G \mid x \text{ is a } \mathbb{P}\text{-name}\}.$$

Hierarchies of sets: the names hierarchy

Suppose that $(V, \in) \models$ ZFC, and $\mathbb{P} = \langle P, \leq \rangle$ is a poset in V.

Definition

Let $V^{\mathbb{P}}$ denote the collection of all $\mathbb{P}$-names. Given a subset $G \subseteq P$, we let:

$$V[G] := V^{\mathbb{P}}/G = \{x/G \mid x \text{ is a } \mathbb{P}\text{-name}\}.$$

Theorem (Cohen, 1963)

If $G \subseteq P$ is a particular form of a maximal ideal (called "generic"), then:

1. $(V[G], \in) \models$ZFC;
2. $V \subseteq V[G]$, and $G \in V[G]$;
3. V and $V[G]$ have the same ordinals.

Hierarchies of sets: the names hierarchy

Suppose that $(V, \in) \models$ ZFC, and $\mathbb{P} = \langle P, \leq \rangle$ is a poset in V.

Definition

Let $V^{\mathbb{P}}$ denote the collection of all $\mathbb{P}$-names. Given a subset $G \subseteq P$, we let:

$$V[G] := V^{\mathbb{P}}/G = \{x/G \mid x \text{ is a } \mathbb{P}\text{-name}\}.$$

Theorem (Cohen, 1963)

If $G \subseteq P$ is a particular form of a maximal ideal (called "generic"), then:

1. $(V[G], \in) \models$ZFC;
2. $V \subseteq V[G]$, and $G \in V[G]$;
3. V and $V[G]$ have the same cardinals, provided that $\mathbb{P}$ does not have uncountable antichains.

Forcing

Summary

Starting with a model V of ZFC, and a partial order $\mathbb{P}$ from V, the method of forcing allows to pass to a $\mathbb{P}$-generic extension $V[G]$, which is again a model of ZFC.
The statements which are valid in $V[G]$ are tightly related to the combinatorial properties of the ground model V, and the chosen poset $\mathbb{P}$.

Exercise

Definition

- $D \subseteq P$ is said to be dominating if for all $p \in P$, there exists $d \in D$ with $p \leq d$.
- $I \subseteq P$ is an ideal over $\mathbb{P}$ if:
  1. for every $p, q \in I$, there exists $r \in I$ with $p \leq r$ and $q \leq r$;
  2. for every $p \in I$ and $q \leq p$, we have $q \in I$;
- the ideal $I \subseteq P$ is generic, if $I \cap D \neq \emptyset$ for each dominating D.

Prove!

Suppose that V is a model of ZFC. In V, define $\mathbb{P} := (P, \subseteq)$, where P is the set of all functions of the form $f : x \to 2$, for finite subsets x of ω_2.
Let $V[G]$ denote the $\mathbb{P}$-generic extension of V; then

$$V[G] \models \mathrm{ZFC} + \neg\text{Continuum hypothesis}.$$

Hierarchies of sets: the constructible hierarchy

Definition

The definable power set $\mathcal{D}(B) := \{A \mid A \text{ is definable over } (B, \in)\}$.

Hierarchies of sets: the constructible hierarchy

Definition

Say that A is <u>definable</u> over $(B, \in)$ if there exists a formula φ in the language of set theory and parameters $b_1, \ldots, b_n$ in B such that

$$A = \{z \in B \mid (B, \in) \models \varphi[z, b_1, \ldots, b_n]\}.$$

The definable power set $\mathcal{D}(B) := \{A \mid A \text{ is definable over } (B, \in)\}$.

Hierarchies of sets: the constructible hierarchy

Definition

Say that A is definable over $(B, \in)$ if there exists a formula φ in the language of set theory and parameters $b_1, \ldots, b_n$ in B such that

$$A = \{z \in B \mid (B, \in) \models \varphi[z, b_1, \ldots, b_n]\}.$$

The definable power set $\mathcal{D}(B) := \{A \mid A \text{ is definable over } (B, \in)\}$.

Definition

Suppose that $(V, \in) \models \mathrm{ZFC}$.
In V, recursively define:

- $L_0 := \emptyset$;
- $L_{\alpha+1} := \mathcal{D}(L_\alpha)$ for every ordinal α;
- $L_\delta := \bigcup_{\alpha<\delta} L_\alpha$ for every nonzero limit ordinal δ.

Say that x is a constructible set iff x is in L_α for some ordinal α.

Hierarchies of sets: the constructible hierarchy

Theorem (Gödel, 1936)

Suppose that $(V, \in) \models$ *ZFC.*
Let L *denote the (sub)collection of all constructible sets.*
Then $(L, \in) \models$*ZFC+GCH.*

Definition

Suppose that $(V, \in) \models$ ZFC.
In V, recursively define:

- $L_0 := \emptyset$;
- $L_{\alpha+1} := \mathcal{D}(L_\alpha)$ for every ordinal α;
- $L_\delta := \bigcup_{\alpha<\delta} L_\alpha$ for every nonzero limit ordinal δ.

Say that x is a constructible set iff x is in L_α for some ordinal α.

Hierarchies of sets: the constructible hierarchy

Theorem (Gödel, 1936)

Suppose that $(V, \in) \models ZFC$.
Let L denote the (sub)collection of all constructible sets.
Then $(L, \in) \models ZFC+GCH$.

Application of passing to an inner model

If ZFC is consistent, then so is ZFC + Continuum Hypothesis.

Hierarchies of sets: the constructible hierarchy

Theorem (Gödel, 1936)

Suppose that $(V, \in) \models ZFC$.
Let L *denote the (sub)collection of all constructible sets.*
Then $(L, \in) \models ZFC + GCH$.

> *Given a conjecture, the best thing is to prove it. The second best thing is to disprove it. The third best thing is to prove that it is not possible to disprove it, since it will tell you not to waste your time trying to disprove it. That's what Gödel did for the Continuum Hypothesis.*
>
> Saharon Shelah

Part 2: theorems proved via forcing

Ramsey-type theorems

Theorem (Ramsey, 1929)

For every coloring $c : [\mathbb{N}]^2 \to \{0, 1\}$, *there exists an infinite* $A \subseteq \mathbb{N}$, *such that* $c \restriction [A]^2$ *is constant.*

Ramsey-type theorems

Theorem (Sierpinski, 1933)

There exists a coloring $c : [\omega_1]^2 \to \{0, 1\}$ *such that* $c \restriction [A]^2$ *is non-constant for all uncountable* $A \subseteq \omega_1$.

Ramsey-type theorems

Theorem (Sierpinski, 1933)

There exists a coloring $c : [\omega_1]^2 \to \{0,1\}$ *such that* $c \restriction [A]^2$ *is non-constant for all uncountable* $A \subseteq \omega_1$.

Theorem (Baumgartner-Hajnal, 1973)

For every coloring $c : [\omega_1]^2 \to \{0,1\}$, *end every ordinal* $\alpha < \omega_1$, *there exists a subset* $A \subseteq \omega_1$ *of order-type* α *such that* $c \restriction [A]^2$ *is constant.*

Ramsey-type theorems

Theorem (Sierpinski, 1933)

There exists a coloring $c : [\omega_1]^2 \to \{0, 1\}$ *such that* $c \restriction [A]^2$ *is non-constant for all uncountable* $A \subseteq \omega_1$.

Theorem (Baumgartner-Hajnal, 1973)

For every coloring $c : [\omega_1]^2 \to \{0, 1\}$, *end every ordinal* $\alpha < \omega_1$, *there exists a subset* $A \subseteq \omega_1$ *of order-type* α *such that* $c \restriction [A]^2$ *is constant.*

They prove that the monochromatic set of order-type α exists in a forcing extension $V[G]$, and then pull (a copy of) it back to V, using absoluteness reasoning.

Ramsey-type theorems

Theorem (Sierpinski, 1933)

There exists a coloring $c : [\omega_1]^2 \to \{0,1\}$ *such that* $c \restriction [A]^2$ *is non-constant for all uncountable* $A \subseteq \omega_1$.

Theorem (Baumgartner-Hajnal, 1973)

For every coloring $c : [\omega_1]^2 \to \{0,1\}$, *end every ordinal* $\alpha < \omega_1$, *there exists a subset* $A \subseteq \omega_1$ *of order-type* α *such that* $c \restriction [A]^2$ *is constant.*

Shortly afterwards, Galvin found a direct combinatorial proof.

Cardinal Arithmetic

Theorem (Silver, 1975)

If $2^{\aleph_\alpha} = \aleph_{\alpha+1}$ *for all* $\alpha < \aleph_{\omega_1}$, *then* $2^{\aleph_{\omega_1}} = \aleph_{\omega_1+1}$.

Cardinal Arithmetic

Theorem (Silver, 1975)

If $2^{\aleph_\alpha} = \aleph_{\alpha+1}$ *for all* $\alpha < \aleph_{\omega_1}$, *then* $2^{\aleph_{\omega_1}} = \aleph_{\omega_1+1}$.

Silver's proof used the forcing machinery ("non-wellfounded generic ultrapowers").

Cardinal Arithmetic

Theorem (Silver, 1975)

If $2^{\aleph_\alpha} = \aleph_{\alpha+1}$ *for all* $\alpha < \aleph_{\omega_1}$, *then* $2^{\aleph_{\omega_1}} = \aleph_{\omega_1+1}$.

Silver's proof used the forcing machinery ("non-wellfounded generic ultrapowers").

Afterwards, Baumgartner and Prikry carefully analyzed Silver's arguments, and devised a direct, forcing-free proof.

Covering the plane

Identify a function $f : \mathbb{R} \to \mathbb{R}$ with its graph $\{(x, f(x)) \mid x \in \mathbb{R}\}$.
Denote $f^{-1} := \{(f(x), x) \mid x \in \mathbb{R}\}$.

Covering the plane

Identify a function $f : \mathbb{R} \to \mathbb{R}$ with its graph $\{(x, f(x)) \mid x \in \mathbb{R}\}$.
Denote $f^{-1} := \{(f(x), x) \mid x \in \mathbb{R}\}$.

Theorem (Sierpinski, 1919)

For every $\aleph_1$-sized sets of reals X, there exists a countable collection of functions $\{f_n : \mathbb{R} \to \mathbb{R} \mid n < \omega\}$ such that $\bigcup_{n<\omega}(f_n \cup f_n^{-1})$ covers X^2.

Covering the plane

Identify a function $f : \mathbb{R} \to \mathbb{R}$ with its graph $\{(x, f(x)) \mid x \in \mathbb{R}\}$.
Denote $f^{-1} := \{(f(x), x) \mid x \in \mathbb{R}\}$.

Theorem (Sierpinski, 1919)

For every $\aleph_1$-sized sets of reals X, there exists a countable collection of functions $\{f_n : \mathbb{R} \to \mathbb{R} \mid n < \omega\}$ such that $\bigcup_{n<\omega}(f_n \cup f_n^{-1})$ covers X^2.

Theorem (Kubiś-Vejnar, 2012)

There exists a countable collection of continuous functions $\{f_n : \mathbb{R} \to \mathbb{R} \mid n < \omega\}$ such that $\bigcup_{n<\omega}(f_n \cup f_n^{-1})$ covers X^2, for some uncountable set $X \subseteq \mathbb{R}$.

Covering the plane

They introduced the functions by forcing, and then appealed to the work of Keisler on the logic $L^\omega(Q)$, to obtain the functions in the ground model.

Theorem (Kubiś-Vejnar, 2012)

There exists a countable collection of continuous functions $\{f_n : \mathbb{R} \to \mathbb{R} \mid n < \omega\}$ such that $\bigcup_{n<\omega}(f_n \cup f_n^{-1})$ covers X^2, for some uncountable set $X \subseteq \mathbb{R}$.

Covering the plane

Kunen found a forcing-free proof, of an even stronger statement.

Theorem (Kunen, 2012)

There exists a countable collection of C^∞ functions $\{f_n : \mathbb{R} \to \mathbb{R} \mid n < \omega\}$ such that $\bigcup_{n<\omega}(f_n \cup f_n^{-1})$ covers X^2, for some uncountable set $X \subseteq \mathbb{R}$.

Theorem (Kubiś-Vejnar, 2012)

There exists a countable collection of continuous functions $\{f_n : \mathbb{R} \to \mathbb{R} \mid n < \omega\}$ such that $\bigcup_{n<\omega}(f_n \cup f_n^{-1})$ covers X^2, for some uncountable set $X \subseteq \mathbb{R}$.

Rational distances

Theorem (Komjáth, 1994)

$\mathbb{R}^n$ is the union of countably many sets, none containing two points a rational distance apart.

Rational distances

Theorem (Komjáth, 1994)

$\mathbb{R}^n$ is the union of countably many sets, none containing two points a rational distance apart.

That is, letting $E^n := \{\{\bar{x}, \bar{y}\} \in [\mathbb{R}^n]^2 \mid |\bar{x} - \bar{y}| \in \mathbb{Q}\}$, the graph $(\mathbb{R}^n, E^n)$ is countably chromatic!

Rational distances

Theorem (Komjáth, 1994)

$\mathbb{R}^n$ is the union of countably many sets, none containing two points a rational distance apart.

Theorem (Kumar, 2012)

For any set $X \subseteq \mathbb{R}$, there is a subset $Y \subseteq X$ such X and Y have the same Lebesgue outer measure, and the distance between any two distinct points in Y is irrational.

Rational distances

Theorem (Komjáth, 1994)

$\mathbb{R}^n$ is the union of countably many sets, none containing two points a rational distance apart.

Theorem (Kumar, 2012)

For any set $X \subseteq \mathbb{R}$, there is a subset $Y \subseteq X$ such X and Y have the same Lebesgue outer measure, and the distance between any two distinct points in Y is irrational.

Kumar's proof relies on a theorem of Gitik and Shelah that was obtained indirectly by means of forcing.

Rational distances

Theorem (Komjáth, 1994)

$\mathbb{R}^n$ is the union of countably many sets, none containing two points a rational distance apart.

Theorem (Kumar, 2012)

For any set $X \subseteq \mathbb{R}$, there is a subset $Y \subseteq X$ such X and Y have the same Lebesgue outer measure, and the distance between any two distinct points in Y is irrational.

Kumar's proof relies on a theorem of Gitik and Shelah that was obtained indirectly by means of forcing.
A Forcing-free proof of the Gitik-Shelah theorem was given by Burke and Fremlin.

Compact subsets of the first Baire class

Suppose that X is a Polish space. Let $B_1(X)$ denote the space of all Baire class-1 real-valued functions on X, endowed with the topology of pointwise convergence.

Compact subsets of the first Baire class

Suppose that X is a Polish space. Let $B_1(X)$ denote the space of all Baire class-1 real-valued functions on X, endowed with the topology of pointwise convergence.

Theorem (Bourgain, 1978)

Every compact subset of $B_1(X)$ contains a dense set of G_δ-points.

Compact subsets of the first Baire class

Suppose that X is a Polish space. Let $B_1(X)$ denote the space of all Baire class-1 real-valued functions on X, endowed with the topology of pointwise convergence.

Theorem (Bourgain, 1978)

Every compact subset of $B_1(X)$ contains a dense set of G_δ-points.

Theorem (Todorčević, 1999)

Every compact subset of $B_1(X)$ contains a dense metrizable subspace.

Compact subsets of the first Baire class

Suppose that X is a Polish space. Let $B_1(X)$ denote the space of all Baire class-1 real-valued functions on X, endowed with the topology of pointwise convergence.

Theorem (Bourgain, 1978)

Every compact subset of $B_1(X)$ contains a dense set of G_δ-points.

Theorem (Todorčević, 1999)

Every compact subset of $B_1(X)$ contains a dense metrizable subspace.

Todorčević's proof is involved and uses the forcing machinery in a deep way. A forcing-free proof is unknown.

Uniformization

Definition

Suppose that $\varphi(\bar{x}, \bar{y})$ is a formula for which $\forall \bar{x} \exists \bar{y}(\varphi(\bar{x}, \bar{y}))$ is valid. A formula $\psi(\bar{x}, \bar{y})$ is a <u>uniformization</u> of $\varphi(\bar{x}, \bar{y})$ provided that:

- $\forall \bar{x} \forall \bar{y}(\psi(\bar{x}, \bar{y}) \to \varphi(\bar{x}, \bar{y}))$;
- $\forall \bar{x} \exists ! y(\psi(\bar{x}, \bar{y}))$.

(here, $\exists !$ stands for "exists a unique")

Uniformization

Definition

Suppose that $\varphi(\bar{x}, \bar{y})$ is a formula for which $\forall \bar{x} \exists \bar{y} (\varphi(\bar{x}, \bar{y}))$ is valid. A formula $\psi(\bar{x}, \bar{y})$ is a uniformization of $\varphi(\bar{x}, \bar{y})$ provided that:

- $\forall \bar{x} \forall \bar{y} (\psi(\bar{x}, \bar{y}) \to \varphi(\bar{x}, \bar{y}))$;
- $\forall \bar{x} \exists ! y (\psi(\bar{x}, \bar{y}))$.

(here, $\exists !$ stands for "exists a unique")

Theorem (Gurevich-Shelah, 1983)

There exists a formula $\varphi(\bar{x}, \bar{y})$ in monadic second-order logic on the infinite binary tree, that does not admit a uniformization.

Uniformization

Definition

Suppose that $\varphi(\bar{x}, \bar{y})$ is a formula for which $\forall \bar{x} \exists \bar{y}(\varphi(\bar{x}, \bar{y}))$ is valid. A formula $\psi(\bar{x}, \bar{y})$ is a uniformization of $\varphi(\bar{x}, \bar{y})$ provided that:

- $\forall \bar{x} \forall \bar{y}(\psi(\bar{x}, \bar{y}) \rightarrow \varphi(\bar{x}, \bar{y}))$;
- $\forall \bar{x} \exists ! y(\psi(\bar{x}, \bar{y}))$.

(here, $\exists !$ stands for "exists a unique")

Theorem (Gurevich-Shelah, 1983)

There exists a formula $\varphi(\bar{x}, \bar{y})$ in monadic second-order logic on the infinite binary tree, that does not admit a uniformization.

The proof uses a forcing argument, and then appeals to an absolute decision procedure for the monadic second-order theory of the full binary tree T, due to Rabin.

Uniformization

Definition

Suppose that $\varphi(\bar{x}, \bar{y})$ is a formula for which $\forall \bar{x} \exists \bar{y}(\varphi(\bar{x}, \bar{y}))$ is valid. A formula $\psi(\bar{x}, \bar{y})$ is a uniformization of $\varphi(\bar{x}, \bar{y})$ provided that:

- $\forall \bar{x} \forall \bar{y}(\psi(\bar{x}, \bar{y}) \rightarrow \varphi(\bar{x}, \bar{y}))$;
- $\forall \bar{x} \exists! y(\psi(\bar{x}, \bar{y}))$.

(here, $\exists!$ stands for "exists a unique")

Theorem (Gurevich-Shelah, 1983)

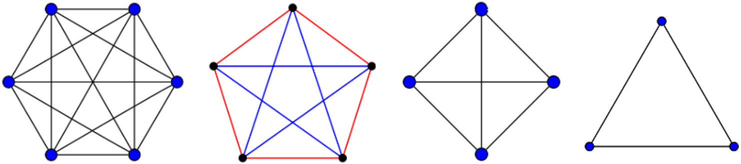
There exists a formula $\varphi(\bar{x}, \bar{y})$ in monadic second-order logic on the infinite binary tree, that does not admit a uniformization.

In a paper from 2010, Löding, Niwiński, and Walukiwicz provide a simpler forcing-free proof that only uses basic tools from automata theory.

Partition relations for graphs

For every coloring $c : [6]^2 \to \{0, 1\}$, there exists a monochromatic triangle Δ. That is, $|\Delta| = 3$ such that $c \restriction [\Delta]^2$ is constant. One cannot replace 6 with 5.

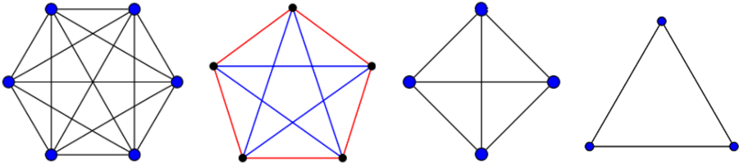
Erdös and Hajnal asked: could there be a graph (G, E) that does not embed a copy of $[4]^2$, yet for any coloring $c : E \to \{0, 1\}$, there would be a monochromatic triangle?



Partition relations for graphs

Theorem (Shelah, 1987)

There exists a K_4-free graph (G, E), such that for every coloring $c : E \to \{0, 1\}$, there exists a monochromatic triangle $\Delta \subseteq G$. That is, $|\Delta| = 3$, $[\Delta]^2 \subseteq E$ and $c \restriction [\Delta]^2$ is constant.



Partition relations for graphs

Theorem (Shelah, 1987)

There exists a K_4-free graph (G, E), such that for every coloring $c : E \to \{0, 1\}$, there exists a monochromatic triangle $\Delta \subseteq G$. That is, $|\Delta| = 3$, $[\Delta]^2 \subseteq E$ and $c \restriction [\Delta]^2$ is constant.

Shelah constructs a forcing extension which adds a graph $\mathcal{H}$ with the same partition property, even for $\aleph_0$ colors. In particular, $\mathcal{H}$ has the edge-coloring property for 2 colors. By compactness of first-order logic, $\mathcal{H}$ must contain a finite subgraph $\mathcal{G}$ with the same property. As forcing cannot create new finite graphs, $\mathcal{G}$ is already present in the ground model!

The tensor product of graphs

Conjecture (Hedetniemi, 1966)

For every graphs $\mathcal{G}, \mathcal{H}$:

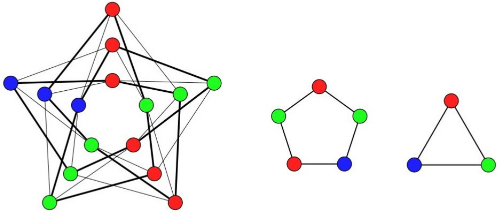
$$\mathsf{Chr}(\mathcal{G} \times \mathcal{H}) = \min\{\mathsf{Chr}(\mathcal{G}), \mathsf{Chr}(\mathcal{H})\}.$$

The tensor product of graphs

Conjecture (Hedetniemi, 1966)

For every graphs $\mathcal{G}, \mathcal{H}$:

$$\mathsf{Chr}(\mathcal{G} \times \mathcal{H}) = \min\{\mathsf{Chr}(\mathcal{G}), \mathsf{Chr}(\mathcal{H})\}.$$



The tensor product of graphs

Conjecture (Hedetniemi, 1966)

For every graphs $\mathcal{G}, \mathcal{H}$:

$$\mathrm{Chr}(\mathcal{G} \times \mathcal{H}) = \min\{\mathrm{Chr}(\mathcal{G}), \mathrm{Chr}(\mathcal{H})\}.$$

Theorem (Hajnal, 1985)

For every infinite cardinal κ, there exist graphs $\mathcal{G}, \mathcal{H}$ such that:

1. $\mathrm{Chr}(\mathcal{G}) = \mathrm{Chr}(\mathcal{H}) = \kappa^+$;
2. $\mathrm{Chr}(\mathcal{G} \times \mathcal{H}) = \kappa$.

Theorem (Soukup, 1988)

If ZFC is consistent, then so is ZFC+GCH+there exist graphs $\mathcal{G}, \mathcal{H}$ of size $\aleph_2$ such that:

1. $\mathrm{Chr}(\mathcal{G}) = \mathrm{Chr}(\mathcal{H}) = \aleph_2$;
2. $\mathrm{Chr}(\mathcal{G} \times \mathcal{H}) = \aleph_0$.

The tensor product of graphs

Conjecture (Hedetniemi, 1966)

For every graphs $\mathcal{G}, \mathcal{H}$:

$$\mathsf{Chr}(\mathcal{G} \times \mathcal{H}) = \min\{\mathsf{Chr}(\mathcal{G}), \mathsf{Chr}(\mathcal{H})\}.$$

Theorem (2013)

In the constructible universe, for every infinite cardinal κ, there exist graphs $\mathcal{G}, \mathcal{H}$ of size κ^+ such that:

1. $\mathsf{Chr}(\mathcal{G}) = \mathsf{Chr}(\mathcal{H}) = \kappa^+$;
2. $\mathsf{Chr}(\mathcal{G} \times \mathcal{H}) = \aleph_0$.

The tensor product of graphs

Conjecture (Hedetniemi, 1966)

For every graphs $\mathcal{G}, \mathcal{H}$:

$$\mathrm{Chr}(\mathcal{G} \times \mathcal{H}) = \min\{\mathrm{Chr}(\mathcal{G}), \mathrm{Chr}(\mathcal{H})\}.$$

Theorem (2013)

In the constructible universe, for every infinite cardinal κ, there exist graphs $\mathcal{G}, \mathcal{H}$ of size κ^+ such that:

1. $\mathrm{Chr}(\mathcal{G}) = \mathrm{Chr}(\mathcal{H}) = \kappa^+$;
2. $\mathrm{Chr}(\mathcal{G} \times \mathcal{H}) = \aleph_0$.

Aspects of forcing are built into the very definition of the graphs, and items (1),(2) above are established through an inspection of $\mathcal{G}, \mathcal{H}$ in different forcing extensions. Forcing seems crucial here, and I do not know of a forcing-free proof.