From Curry-Howard to Forcing

Laura Fontanella

Institut de mathématiques de Marseille
Université Aix-Marseille

January 1, 2015

Realizability

Establishes a correspondence between formulas provable in a logical system and programs interpreted in a model of computation. Then uses tools from computer science to extract information about proofs in the logical system.

A short history

Kleene 1945

Correspondence between formulas of Heyting arithmetic and (sets of indexes of) recursive functions.

Curry Howard 1958

Isomorphism between proofs in intuitionistic logic and simply typed lambda-terms.

Griffin 1990

Correspondence between classical logic and lambda-terms plus control operators. Peirce's law (excluded middle) is realized by *call/cc*.

Krivine 2000-2004

The programs-formulas correspondence is extended to any formula provable in ZF+DC. Krivine's technique generalizes Forcing: forcing models are special cases of realizability models.

Forcing

Forcing is a technique for building models of set theory, hence proving consistency and independent results.

It was introduced by Cohen in 1963 to prove the independence of the Axiom of Choice and the Continuum Hypothesis from ZF.

The intuition behind Forcing

In order to build our model we assign to each sentence in the language of set theory a certain value that corresponds to the 'degree' to which the sentence is true in the model.

- $\| \varphi \| = 1$ means 'φ is definitely true'
- $\| \varphi \| = 0$ means 'φ is definitely false'
- otherwise $\| \varphi \|$ takes some 'intermediate' value between 0 and 1

We pick a suitable *Boolean algebra* $\mathbb{B} = \langle 0, 1, \wedge, \vee, \neg \rangle$ and assign to each sentence φ an element of $\mathbb{B}$ that we denote $\| \varphi \|$. The elements of $\mathbb{B}$ are called 'conditions'

The intuition behind Forcing

In order to build our model we assign to each sentence in the language of set theory a certain value that corresponds to the 'degree' to which the sentence is true in the model.

- $\| \varphi \| = 1$ means 'φ is definitely true'
- $\| \varphi \| = 0$ means 'φ is definitely false'
- otherwise $\| \varphi \|$ takes some 'intermediate' value between 0 and 1

We pick a suitable *Boolean algebra* $\mathbb{B} = \langle 0, 1, \wedge, \vee, \neg \rangle$ and assign to each sentence φ an element of $\mathbb{B}$ that we denote $\| \varphi \|$. The elements of $\mathbb{B}$ are called 'conditions'

The intuition behind Forcing

In order to build our model we assign to each sentence in the language of set theory a certain value that corresponds to the 'degree' to which the sentence is true in the model.

- $\| \varphi \| = 1$ means 'φ is definitely true'
- $\| \varphi \| = 0$ means 'φ is definitely false'
- otherwise $\| \varphi \|$ takes some 'intermediate' value between 0 and 1

We pick a suitable *Boolean algebra* $\mathbb{B} = \langle 0, 1, \wedge, \vee, \neg \rangle$ and assign to each sentence φ an element of $\mathbb{B}$ that we denote $\| \varphi \|$. The elements of $\mathbb{B}$ are called 'conditions'

The function $\varphi \mapsto \llbracket \varphi \rrbracket$ must satisfy certain properties...

- $\llbracket \neg\varphi \rrbracket = \neg \llbracket \varphi \rrbracket$
- $\llbracket \varphi \wedge \psi \rrbracket = \llbracket \varphi \rrbracket \wedge \llbracket \psi \rrbracket$
- $\llbracket \varphi \vee \psi \rrbracket = \llbracket \varphi \rrbracket \vee \llbracket \psi \rrbracket$
- $\llbracket \forall x\, \varphi(x) \rrbracket = \bigwedge_{a} \llbracket \varphi(a) \rrbracket$

... then $\mathbb{B}$ must be a *complete Boolean algebra*, i.e. arbitrary subsets of $\mathbb{B}$ must have a greatest lower bound.

The function $\varphi \mapsto \| \varphi \|$ must satisfy certain properties...

- $\| \neg\varphi \| = \neg \| \varphi \|$
- $\| \varphi \wedge \psi \| = \| \varphi \| \wedge \| \psi \|$
- $\| \varphi \vee \psi \| = \| \varphi \| \vee \| \psi \|$
- $\| \forall x\, \varphi(x) \| = \bigwedge_a \| \varphi(a) \|$

... then $\mathbb{B}$ must be a *complete Boolean algebra*, i.e. arbitrary subsets of $\mathbb{B}$ must have a greatest lower bound.

The function $\varphi \mapsto \| \varphi \|$ must satisfy certain properties...

- $\| \neg\varphi \| = \neg \| \varphi \|$
- $\| \varphi \wedge \psi \| = \| \varphi \| \wedge \| \psi \|$
- $\| \varphi \vee \psi \| = \| \varphi \| \vee \| \psi \|$
- $\| \forall x\, \varphi(x) \| = \bigwedge_a \| \varphi(a) \|$

... then $\mathbb{B}$ must be a *complete Boolean algebra*, i.e. arbitrary subsets of $\mathbb{B}$ must have a greatest lower bound.

The function $\varphi \mapsto \| \varphi \|$ must satisfy certain properties...

- $\| \neg\varphi \| = \neg \| \varphi \|$
- $\| \varphi \wedge \psi \| = \| \varphi \| \wedge \| \psi \|$
- $\| \varphi \vee \psi \| = \| \varphi \| \vee \| \psi \|$
- $\| \forall x\, \varphi(x) \| = \bigwedge_a \| \varphi(a) \|$

... then $\mathbb{B}$ must be a *complete Boolean algebra*, i.e. arbitrary subsets of $\mathbb{B}$ must have a greatest lower bound.

The function $\varphi \mapsto [\![\varphi]\!]$ must satisfy certain properties...

- $[\![\neg\varphi]\!] = \neg [\![\varphi]\!]$
- $[\![\varphi \wedge \psi]\!] = [\![\varphi]\!] \wedge [\![\psi]\!]$
- $[\![\varphi \vee \psi]\!] = [\![\varphi]\!] \vee [\![\psi]\!]$
- $[\![\forall x \, \varphi(x)]\!] = \bigwedge_a [\![\varphi(a)]\!]$

... then $\mathbb{B}$ must be a *complete Boolean algebra*, i.e. arbitrary subsets of $\mathbb{B}$ must have a greatest lower bound.

What about atomic formulas?

$$\| x = y \| \quad \| x \in y \|$$

... we need to deal with ‘potential members’, the so-called $\mathbb{B}$-*valued sets*.

What about atomic formulas?

$$\| x = y \| \quad \| x \in y \|$$

... we need to deal with ‘potential members’, the so-called $\mathbb{B}$-*valued sets*.

The $\mathbb{B}$-valued sets

M is a given model of ZFC (or ZF).

A $\mathbb{B}$-valued set is a function from a set of $\mathbb{B}$-valued sets to $\mathbb{B}$.

$M^{\mathbb{B}}$, the set of all $\mathbb{B}$-valued sets, is defined inductively as follows:

- $M_0^{\mathbb{B}} = \emptyset$
- $M_{\alpha+1}^{\mathbb{B}} =$ the set of all functions with domain $\subseteq M_\alpha^{\mathbb{B}}$ and values in $\mathbb{B}$
- $M_\alpha^{\mathbb{B}} = \bigcup_{\beta<\alpha} M_\beta^{\mathbb{B}}$, if α is a limit ordinal

$M^{\mathbb{B}} = \bigcup_{\alpha \in Ord} M_\alpha^{\mathbb{B}}$.

Some adjustments...

$\mathfrak{F}$ the set of all first-order sentences in the language of set theory enriched with one constant symbol for each element of $M^{\mathbb{B}}$

$$\| \cdot \| : \quad \mathfrak{F} \to \mathbb{B}$$
$$\varphi \mapsto \| \varphi \| .$$

- $\| \neg\varphi \| = \neg \| \varphi \|$
- $\| \varphi \wedge \psi \| = \| \varphi \| \wedge \| \psi \|$
- $\| \varphi \vee \psi \| = \| \varphi \| \vee \| \psi \|$
- $\| \forall x\, \varphi(x) \| = \bigwedge_{a \in M^{\mathbb{B}}} \| \varphi(a) \|$

Some adjustments...

$\mathfrak{F}$ the set of all first-order sentences in the language of set theory enriched with one constant symbol for each element of $M^{\mathbb{B}}$

$$\begin{aligned} \|\cdot\| : \quad & \mathfrak{F} \to \mathbb{B} \\ & \varphi \mapsto \|\varphi\| . \end{aligned}$$

- $\|\neg\varphi\| = \neg \|\varphi\|$
- $\|\varphi \wedge \psi\| = \|\varphi\| \wedge \|\psi\|$
- $\|\varphi \vee \psi\| = \|\varphi\| \vee \|\psi\|$
- $\|\forall x\, \varphi(x)\| = \bigwedge_{a \in M^{\mathbb{B}}} \|\varphi(a)\|$

The $\mathbb{B}$-value of atomic formulas

We want the axiom of extensionality to hold in $M^{\mathbb{B}}$, thus...

$$\| a = b \| = \| \forall z\, (z \in a \Rightarrow z \in b) \wedge \forall z\, (z \in b \Rightarrow z \in a) \|$$

... and membership statements depend on equality statements, thus...

$$\| a \in b \| = \| \exists z\, (z \in b \wedge z = a) \|$$

The $\mathbb{B}$-value of atomic formulas

We want the axiom of extensionality to hold in $M^{\mathbb{B}}$, thus...

$$\| a = b \| \ = \ \| \forall z \, (z \in a \Rightarrow z \in b) \wedge \forall z \, (z \in b \Rightarrow z \in a) \|$$

... and membership statements depend on equality statements, thus...

$$\| a \in b \| \ = \ \| \exists z \, (z \in b \wedge z = a) \|$$

The $\mathbb{B}$-value of atomic formulas

... the value of $z \in x$ should be compatible with $x(z)$ (remember $x \in M^{\mathbb{B}}$ is a function from a set of $\mathbb{B}$-valued sets to $\mathbb{B}$), therefore ...

$$\llbracket a = b \rrbracket = \bigwedge_{z \in dom(a)} (a(z) \Rightarrow \llbracket z \in b \rrbracket) \wedge \bigwedge_{z \in dom(b)} (b(z) \Rightarrow \llbracket z \in a \rrbracket)$$

$$\llbracket a \in b \rrbracket = \bigvee_{z \in dom(b)} (b(z) \wedge \llbracket a = z \rrbracket)$$

Summing up...

- $\| a \in b \| = \bigvee_{z \in dom(b)} (b(z) \wedge \| a = z \|)$
- $\| a \subseteq b \| = \bigwedge_{z \in dom(a)} (a(z) \Rightarrow \| z \in b \|)$
- $\| a = b \| = \| a \subseteq b \| \wedge \| b \subseteq a \|$
- $\| \neg\varphi \| = \neg \| \varphi \|$
- $\| \varphi \wedge \psi \| = \| \varphi \| \wedge \| \psi \|$
- $\| \varphi \vee \psi \| = \| \varphi \| \vee \| \psi \|$
- $\| \forall x \, \varphi(x) \| = \bigwedge_{a \in M^{\mathbb{B}}} \| \varphi(a) \|$

The boolean-valued model

We start with a model M of ZFC, the *ground model*. We pick a suitable Boolean algebra $\mathbb{B} \in M$ which is a complete Boolean algebra in M.

Theorem

The set of sentences that have $\mathbb{B}$-value 1 forms a coherent theory.

Theorem

All the axioms of ZFC hold in $M^{\mathbb{B}}$ (i.e. have $\mathbb{B}$-value 1)

The boolean-valued model

We start with a model M of ZFC, the *ground model*. We pick a suitable Boolean algebra $\mathbb{B} \in M$ which is a complete Boolean algebra in M.

Theorem

The set of sentences that have $\mathbb{B}$-value 1 forms a coherent theory.

Theorem

All the axioms of ZFC hold in $M^{\mathbb{B}}$ (i.e. have $\mathbb{B}$-value 1)

The boolean-valued model

We start with a model M of ZFC, the *ground model*. We pick a suitable Boolean algebra $\mathbb{B} \in M$ which is a complete Boolean algebra in M.

Theorem

The set of sentences that have $\mathbb{B}$-value 1 forms a coherent theory.

Theorem

All the axioms of ZFC hold in $M^{\mathbb{B}}$ (i.e. have $\mathbb{B}$-value 1)

The boolean-valued model

We start with a model M of ZFC, the *ground model*. We pick a suitable Boolean algebra $\mathbb{B} \in M$ which is a complete Boolean algebra in M.

Theorem

The set of sentences that have $\mathbb{B}$-value 1 forms a coherent theory.

Theorem

All the axioms of ZFC hold in $M^{\mathbb{B}}$ (i.e. have $\mathbb{B}$-value 1)

An example

Theorem

The axiom of extensionality holds in $M^{\mathbb{B}}$

Proof

Let $a, b \in M^{\mathbb{B}}$.Observe that:

- if $x \le x'$, then $(x' \Rightarrow y) \le (x \Rightarrow y)$
- $a(u) \le \| u \in a \|$

Then, for every $u \in M^{\mathbb{B}}$, we have $(\| u \in a \| \Rightarrow \| u \in b \|) \le (a(u) \Rightarrow \| u \in b \|)$.Thus

$$\bigwedge_{u \in M^{\mathbb{B}}} (\| u \in a \| \Rightarrow \| u \in b \|) \le \bigwedge_{u \in M^{\mathbb{B}}} (a(u) \Rightarrow \| u \in b \|)$$

The former corresponds to $\| \forall u (u \in a \Rightarrow u \in b) \|$, the latter is $\| a \subseteq b \|$ .So we have

$$\| \forall u (u \in a \iff u \in b) \| \le \| a = b \| .$$

An example

Theorem

The axiom of extensionality holds in $M^{\mathbb{B}}$

Proof

Let $a, b \in M^{\mathbb{B}}$. Observe that:

- if $x \leq x'$, then $(x' \Rightarrow y) \leq (x \Rightarrow y)$
- $a(u) \leq \llbracket u \in a \rrbracket$

Then, for every $u \in M^{\mathbb{B}}$, we have $(\llbracket u \in a \rrbracket \Rightarrow \llbracket u \in b \rrbracket) \leq (a(u) \Rightarrow \llbracket u \in b \rrbracket)$. Thus

$$\bigwedge_{u \in M^{\mathbb{B}}} (\llbracket u \in a \rrbracket \Rightarrow \llbracket u \in b \rrbracket) \leq \bigwedge_{u \in M^{\mathbb{B}}} (a(u) \Rightarrow \llbracket u \in b \rrbracket)$$

The former corresponds to $\llbracket \forall u (u \in a \Rightarrow u \in b) \rrbracket$, the latter is $\llbracket a \subseteq b \rrbracket$. So we have

$$\llbracket \forall u (u \in a \iff u \in b) \rrbracket \leq \llbracket a = b \rrbracket .$$

An example

Theorem

The axiom of extensionality holds in $M^{\mathbb{B}}$

Proof

Let $a, b \in M^{\mathbb{B}}$.Observe that:

- if $x \leq x'$, then $(x' \Rightarrow y) \leq (x \Rightarrow y)$
- $a(u) \leq [\![u \in a]\!]$

Then, for every $u \in M^{\mathbb{B}}$, we have $([\![u \in a]\!] \Rightarrow [\![u \in b]\!]) \leq (a(u) \Rightarrow [\![u \in b]\!])$.Thus

$$\bigwedge_{u \in M^{\mathbb{B}}} ([\![u \in a]\!] \Rightarrow [\![u \in b]\!]) \leq \bigwedge_{u \in M^{\mathbb{B}}} (a(u) \Rightarrow [\![u \in b]\!])$$

The former corresponds to $[\![\forall u(u \in a \Rightarrow u \in b)]\!]$, the latter is $[\![a \subseteq b]\!]$.So we have

$$[\![\forall u(u \in a \iff u \in b)]\!] \leq [\![a = b]\!].$$

An example

Theorem

The axiom of extensionality holds in $M^{\mathbb{B}}$

Proof

Let $a, b \in M^{\mathbb{B}}$.Observe that:

- if $x \leq x'$, then $(x' \Rightarrow y) \leq (x \Rightarrow y)$
- $a(u) \leq [\![u \in a]\!]$

Then, for every $u \in M^{\mathbb{B}}$, we have $([\![u \in a]\!] \Rightarrow [\![u \in b]\!]) \leq (a(u) \Rightarrow [\![u \in b]\!])$.Thus

$$\bigwedge_{u \in M^{\mathbb{B}}} ([\![u \in a]\!] \Rightarrow [\![u \in b]\!]) \leq \bigwedge_{u \in M^{\mathbb{B}}} (a(u) \Rightarrow [\![u \in b]\!])$$

The former corresponds to $[\![\forall u(u \in a \Rightarrow u \in b)]\!]$, the latter is $[\![a \subseteq b]\!]$.So we have

$$[\![\forall u(u \in a \iff u \in b)]\!] \leq [\![a = b]\!].$$

An example

Theorem

The axiom of extensionality holds in $M^{\mathbb{B}}$

Proof

Let $a, b \in M^{\mathbb{B}}$.Observe that:

- if $x \leq x'$, then $(x' \Rightarrow y) \leq (x \Rightarrow y)$
- $a(u) \leq \| u \in a \|$

Then, for every $u \in M^{\mathbb{B}}$, we have $(\| u \in a \| \Rightarrow \| u \in b \|) \leq (a(u) \Rightarrow \| u \in b \|)$.Thus

$$\bigwedge_{u \in M^{\mathbb{B}}} (\| u \in a \| \Rightarrow \| u \in b \|) \leq \bigwedge_{u \in M^{\mathbb{B}}} (a(u) \Rightarrow \| u \in b \|)$$

The former corresponds to $\| \forall u (u \in a \Rightarrow u \in b) \|$, the latter is $\| a \subseteq b \|$.So we have

$$\| \forall u (u \in a \iff u \in b) \| \leq \| a = b \| .$$

An example

Theorem

The axiom of extensionality holds in $M^{\mathbb{B}}$

Proof

Let $a, b \in M^{\mathbb{B}}$.Observe that:

- if $x \leq x'$, then $(x' \Rightarrow y) \leq (x \Rightarrow y)$
- $a(u) \leq \,|\, u \in a \,|$

Then, for every $u \in M^{\mathbb{B}}$, we have $(\,|\, u \in a \,| \Rightarrow \|\, u \in b \,\|\,) \leq (a(u) \Rightarrow \|\, u \in b \,\|\,)$.Thus

$$\bigwedge_{u \in M^{\mathbb{B}}} (\,|\, u \in a \,| \Rightarrow \|\, u \in b \,\|\,) \leq \bigwedge_{u \in M^{\mathbb{B}}} (a(u) \Rightarrow \|\, u \in b \,\|\,)$$

The former corresponds to $\|\, \forall u (u \in a \Rightarrow u \in b) \,\|$, the latter is $\|\, a \subseteq b \,\|$ .So we have

$$\|\, \forall u (u \in a \iff u \in b) \,\| \leq \|\, a = b \,\| .$$

An example

Theorem

The axiom of extensionality holds in $M^{\mathbb{B}}$

Proof

Let $a, b \in M^{\mathbb{B}}$.Observe that:

- if $x \leq x'$, then $(x' \Rightarrow y) \leq (x \Rightarrow y)$
- $a(u) \leq \| u \in a \|$

Then, for every $u \in M^{\mathbb{B}}$, we have $(\| u \in a \| \Rightarrow \| u \in b \|) \leq (a(u) \Rightarrow \| u \in b \|)$.Thus

$$\bigwedge_{u \in M^{\mathbb{B}}} (\| u \in a \| \Rightarrow \| u \in b \|) \leq \bigwedge_{u \in M^{\mathbb{B}}} (a(u) \Rightarrow \| u \in b \|)$$

The former corresponds to $\| \forall u(u \in a \Rightarrow u \in b) \|$, the latter is $\| a \subseteq b \|$ .So we have

$$\| \forall u(u \in a \iff u \in b) \| \leq \| a = b \| .$$

An example

Theorem

The axiom of extensionality holds in $M^{\mathbb{B}}$

Proof

Let $a, b \in M^{\mathbb{B}}$.Observe that:

- if $x \leq x'$, then $(x' \Rightarrow y) \leq (x \Rightarrow y)$
- $a(u) \leq \| u \in a \|$

Then, for every $u \in M^{\mathbb{B}}$, we have $(\| u \in a \| \Rightarrow \| u \in b \|) \leq (a(u) \Rightarrow \| u \in b \|)$.Thus

$$\bigwedge_{u \in M^{\mathbb{B}}} (\| u \in a \| \Rightarrow \| u \in b \|) \leq \bigwedge_{u \in M^{\mathbb{B}}} (a(u) \Rightarrow \| u \in b \|)$$

The former corresponds to $\| \forall u(u \in a \Rightarrow u \in b) \|$, the latter is $\| a \subseteq b \|$ .So we have

$$\| \forall u(u \in a \iff u \in b) \| \leq \| a = b \| .$$

The forcing model

Attention: $\mathbb{M}^{\mathbb{B}}$ is not a model of ZFC: for an arbitrary $\varphi \in \mathfrak{F}$, the $\mathbb{B}$-value $\| \varphi \|$ may be neither 1 nor 0.

So far the only ' trustful' condition was 1, we need to pick more ' trustful' conditions so that for every statement $\varphi \in \mathfrak{F}$, either φ or $\neg\varphi$ will hold in the model. We need to define a set $G \subseteq \mathbb{B}$ of 'trustful' conditions such that:

- $1 \in G$
- $0 \notin G$
- if $x, y \in G$, then $x \wedge y \in G$
- if $x \in G$ and $x \leq y$ (i.e. $x \wedge y = x$), then $y \in G$
- for all $x \in \mathbb{B}$, then either x or $\neg x \in G$

Thus, G is an ultrafilter on $\mathbb{B}$.

The forcing model

Attention: $\mathbb{M}^{\mathbb{B}}$ is not a model of ZFC: for an arbitrary $\varphi \in \mathfrak{F}$, the $\mathbb{B}$-value $\| \varphi \|$ may be neither 1 nor 0.

So far the only ' trustful' condition was 1, we need to pick more ' trustful' conditions so that for every statement $\varphi \in \mathfrak{F}$, either φ or $\neg\varphi$ will hold in the model. We need to define a set $G \subseteq \mathbb{B}$ of 'trustful' conditions such that:

- $1 \in G$
- $0 \notin G$
- if $x, y \in G$, then $x \wedge y \in G$
- if $x \in G$ and $x \leq y$ (i.e. $x \wedge y = x$), then $y \in G$
- for all $x \in \mathbb{B}$, then either x or $\neg x \in G$

Thus, G is an ultrafilter on $\mathbb{B}$.

The forcing model

Attention: $\mathbb{M}^{\mathbb{B}}$ is not a model of ZFC: for an arbitrary $\varphi \in \mathfrak{F}$, the $\mathbb{B}$-value $\|\varphi\|$ may be neither 1 nor 0.

So far the only ‘ trustful’ condition was 1, we need to pick more ‘ trustful’ conditions so that for every statement $\varphi \in \mathfrak{F}$, either φ or $\neg\varphi$ will hold in the model. We need to define a set $G \subseteq \mathbb{B}$ of ‘trustful’ conditions such that:

- $1 \in G$
- $0 \notin G$
- if $x, y \in G$, then $x \wedge y \in G$
- if $x \in G$ and $x \leq y$ (i.e. $x \wedge y = x$), then $y \in G$
- for all $x \in \mathbb{B}$, then either x or $\neg x \in G$

Thus, G is an ultrafilter on $\mathbb{B}$.

The forcing model

Attention: $\mathbb{M}^{\mathbb{B}}$ is not a model of ZFC: for an arbitrary $\varphi \in \mathfrak{F}$, the $\mathbb{B}$-value $\| \varphi \|$ may be neither 1 nor 0.

So far the only ' trustful' condition was 1, we need to pick more ' trustful' conditions so that for every statement $\varphi \in \mathfrak{F}$, either φ or $\neg\varphi$ will hold in the model. We need to define a set $G \subseteq \mathbb{B}$ of 'trustful' conditions such that:

- $1 \in G$
- $0 \notin G$
- if $x, y \in G$, then $x \wedge y \in G$
- if $x \in G$ and $x \leq y$ (i.e. $x \wedge y = x$), then $y \in G$
- for all $x \in \mathbb{B}$, then either x or $\neg x \in G$

Thus, G is an ultrafilter on $\mathbb{B}$.

The forcing model

Attention: $\mathbb{M}^{\mathbb{B}}$ is not a model of ZFC: for an arbitrary $\varphi \in \mathfrak{F}$, the $\mathbb{B}$-value $\| \varphi \|$ may be neither 1 nor 0.

So far the only ' trustful' condition was 1, we need to pick more ' trustful' conditions so that for every statement $\varphi \in \mathfrak{F}$, either φ or $\neg\varphi$ will hold in the model. We need to define a set $G \subseteq \mathbb{B}$ of 'trustful' conditions such that:

- $1 \in G$
- $0 \notin G$
- if $x, y \in G$, then $x \wedge y \in G$
- if $x \in G$ and $x \leq y$ (i.e. $x \wedge y = x$), then $y \in G$
- for all $x \in \mathbb{B}$, then either x or $\neg x \in G$

Thus, G is an ultrafilter on $\mathbb{B}$.

The forcing model

Attention: $\mathbb{M}^{\mathbb{B}}$ is not a model of ZFC: for an arbitrary $\varphi \in \mathfrak{F}$, the $\mathbb{B}$-value $\| \varphi \|$ may be neither 1 nor 0.

So far the only ' trustful' condition was 1, we need to pick more ' trustful' conditions so that for every statement $\varphi \in \mathfrak{F}$, either φ or $\neg\varphi$ will hold in the model. We need to define a set $G \subseteq \mathbb{B}$ of 'trustful' conditions such that:

- $1 \in G$
- $0 \notin G$
- if $x, y \in G$, then $x \wedge y \in G$
- if $x \in G$ and $x \leq y$ (i.e. $x \wedge y = x$), then $y \in G$
- for all $x \in \mathbb{B}$, then either x or $\neg x \in G$

Thus, G is an ultrafilter on $\mathbb{B}$.

The forcing model

Attention: $\mathbb{M}^{\mathbb{B}}$ is not a model of ZFC: for an arbitrary $\varphi \in \mathfrak{F}$, the $\mathbb{B}$-value $\| \varphi \|$ may be neither 1 nor 0.

So far the only ' trustful' condition was 1, we need to pick more ' trustful' conditions so that for every statement $\varphi \in \mathfrak{F}$, either φ or $\neg\varphi$ will hold in the model. We need to define a set $G \subseteq \mathbb{B}$ of 'trustful' conditions such that:

- $1 \in G$
- $0 \notin G$
- if $x, y \in G$, then $x \wedge y \in G$
- if $x \in G$ and $x \leq y$ (i.e. $x \wedge y = x$), then $y \in G$
- for all $x \in \mathbb{B}$, then either x or $\neg x \in G$

Thus, G is an ultrafilter on $\mathbb{B}$.

The forcing model

Attention: $\mathbb{M}^{\mathbb{B}}$ is not a model of ZFC: for an arbitrary $\varphi \in \mathfrak{F}$, the $\mathbb{B}$-value $\| \varphi \|$ may be neither 1 nor 0.

So far the only ‘ trustful’ condition was 1, we need to pick more ‘ trustful’ conditions so that for every statement $\varphi \in \mathfrak{F}$, either φ or $\neg\varphi$ will hold in the model. We need to define a set $G \subseteq \mathbb{B}$ of ‘trustful’ conditions such that:

- $1 \in G$
- $0 \notin G$
- if $x, y \in G$, then $x \wedge y \in G$
- if $x \in G$ and $x \leq y$ (i.e. $x \wedge y = x$), then $y \in G$
- for all $x \in \mathbb{B}$, then either x or $\neg x \in G$

Thus, G is an ultrafilter on $\mathbb{B}$.

The forcing model

The quotient

We define the quotient $M^{\mathbb{B}}/G$ as follows. We define an equivalence relation $\sim_G$ on $M^{\mathbb{B}}$.

$$x \sim_G y \iff \|\, x = y \,\| \in G$$

$M^{\mathbb{B}}/G$ is the set of equivalence classes of elements of $M^{\mathbb{B}}$ under the relation $\sim_G$. If $[x], [y]$ denote the equivalence classes of x and y resp. then we let

$$[x] \in_G [y] \iff \|\, x \in y \,\| \in G.$$

Theorem

$M^{\mathbb{B}}/G$ is a model of ZFC.

The generic filter

$M^{\mathbb{B}}/G$ is not in general isomorphic to a transitive model. For that, we introduce an additional requirement for G, the *genericity*.

Let $\mathbb{P} := \mathbb{B} \setminus \{0\}$ and $\leq$ is defined by $p \leq q \iff p \wedge q = p$ for $p, q \in \mathbb{P}$.

Definition

$D \subseteq \mathbb{P}$ is a *dense* set if for all $p \in \mathbb{P}$ there exists $q \leq p$ such that $q \in D$.

Definition

A filter G on $\mathbb{P}$ is *M-generic* if it intersects every dense subset of $\mathbb{P}$ which is in M.

Theorem

If G is an M-generic (ultra)-filter, then $M^{\mathbb{B}}/G$ is (isomorphic to) a transitive model of ZFC. Moreover, $M^{\mathbb{B}}/G$ it is the smallest transitive model of ZFC that contains both M and G; it is usually denoted by $M[G]$.

The generic filter

$M^{\mathbb{B}}/G$ is not in general isomorphic to a transitive model. For that, we introduce an additional requirement for G, the *genericity*.
Let $\mathbb{P} := \mathbb{B} \setminus \{0\}$ and $\leq$ is defined by $p \leq q \iff p \wedge q = p$ for $p, q \in \mathbb{P}$.

Definition

$D \subseteq \mathbb{P}$ is a *dense* set if for all $p \in \mathbb{P}$ there exists $q \leq p$ such that $q \in D$.

Definition

A filter G on $\mathbb{P}$ is *M-generic* if it intersects every dense subset of $\mathbb{P}$ which is in M.

Theorem

If G is an M-generic (ultra)-filter, then $M^{\mathbb{B}}/G$ is (isomorphic to) a transitive model of ZFC. Moreover, $M^{\mathbb{B}}/G$ it is the smallest transitive model of ZFC that contains both M and G; it is usually denoted by $M[G]$.

The generic filter

$M^{\mathbb{B}}/G$ is not in general isomorphic to a transitive model. For that, we introduce an additional requirement for G, the *genericity*.
Let $\mathbb{P} := \mathbb{B} \setminus \{0\}$ and $\leq$ is defined by $p \leq q \iff p \wedge q = p$ for $p, q \in \mathbb{P}$.

Definition

$D \subseteq \mathbb{P}$ is a *dense* set if for all $p \in \mathbb{P}$ there exists $q \leq p$ such that $q \in D$.

Definition

A filter G on $\mathbb{P}$ is *M-generic* if it intersects every dense subset of $\mathbb{P}$ which is in M.

Theorem

If G is an M-generic (ultra)-filter, then $M^{\mathbb{B}}/G$ is (isomorphic to) a transitive model of ZFC. Moreover, $M^{\mathbb{B}}/G$ it is the smallest transitive model of ZFC that contains both M and G; it is usually denoted by $M[G]$.

The generic filter

$M^{\mathbb{B}}/G$ is not in general isomorphic to a transitive model. For that, we introduce an additional requirement for G, the *genericity*.
Let $\mathbb{P} := \mathbb{B} \setminus \{0\}$ and $\leq$ is defined by $p \leq q \iff p \wedge q = p$ for $p, q \in \mathbb{P}$.

Definition

$D \subseteq \mathbb{P}$ is a *dense* set if for all $p \in \mathbb{P}$ there exists $q \leq p$ such that $q \in D$.

Definition

A filter G on $\mathbb{P}$ is *M-generic* if it intersects every dense subset of $\mathbb{P}$ which is in M.

Theorem

If G is an M-generic (ultra)-filter, then $M^{\mathbb{B}}/G$ is (isomorphic to) a transitive model of ZFC. Moreover, $M^{\mathbb{B}}/G$ it is the smallest transitive model of ZFC that contains both M and G; it is usually denoted by $M[G]$.

The generic filter

Definition

A filter G on $\mathbb{P}$ is *M-generic* if it intersects every dense subset of $\mathbb{P}$ which is in M.

Do M-generic filters always exist?

No, but if M is countable they do. We assume ZFC is consistent, we use Lowenheim Skolem to find a countable model M of ZFC.

The generic filter does not exist in M, unless $M[G] = M$.

The generic filter

Definition

A filter G on $\mathbb{P}$ is *M-generic* if it intersects every dense subset of $\mathbb{P}$ which is in M.

Do M-generic filters always exist?

No, but if M is countable they do. We assume ZFC is consistent, we use Lowenheim Skolem to find a countable model M of ZFC.

The generic filter does not exist in M, unless $M[G] = M$.

The intuition

Suppose you want to add a new set $\dot{a} \subseteq \mathbb{N}$. We can identify $\dot{a}$ with its characteristic function, so it is enough to add a new function $\dot{g} : \mathbb{N} \to \{0, 1\}$.Consider all the possible finite approximations of $\dot{g}$, namely

$$\mathbb{P} := \{f : \mathbb{N} \to \{0, 1\};\ f \text{ is finite}\}$$

For $p, q \in \mathbb{P}$, let

$$p \leq q \iff p \sqsupseteq q.$$

Let $1 := \emptyset$, $p \wedge q := p \cup q$, $p \vee q := p \cap q$.

If G is a generic *filter* on $\mathbb{P}$, then $\bigcup G : \mathbb{N} \to \{0, 1\}$ is a total function.

The intuition

Suppose you want to add a new set $\dot{a} \subseteq \mathbb{N}$. We can identify $\dot{a}$ with its characteristic function, so it is enough to add a new function $\dot{g} : \mathbb{N} \to \{0, 1\}$. Consider all the possible finite approximations of $\dot{g}$, namely

$$\mathbb{P} := \{f : \mathbb{N} \to \{0, 1\};\ f \text{ is finite}\}$$

For $p, q \in \mathbb{P}$, let

$$p \leq q \iff p \sqsupseteq q.$$

Let $1 := \emptyset$, $p \wedge q := p \cup q$, $p \vee q := p \cap q$.

If G is a generic *filter* on $\mathbb{P}$, then $\bigcup G : \mathbb{N} \to \{0, 1\}$ is a total function.

The intuition

Suppose you want to add a new set $\dot{a} \subseteq \mathbb{N}$. We can identify $\dot{a}$ with its characteristic function, so it is enough to add a new function $\dot{g} : \mathbb{N} \to \{0, 1\}$.Consider all the possible finite approximations of $\dot{g}$, namely

$$\mathbb{P} := \{f : \mathbb{N} \to \{0, 1\};\ f \text{ is finite}\}$$

For $p, q \in \mathbb{P}$, let

$$p \leq q \iff p \sqsupseteq q.$$

Let $1 := \emptyset$, $p \wedge q := p \cup q$, $p \vee q := p \cap q$.

If G is a generic *filter* on $\mathbb{P}$, then $\bigcup G : \mathbb{N} \to \{0, 1\}$ is a total function.

The intuition

Suppose you want to add a new set $\dot{a} \subseteq \mathbb{N}$. We can identify $\dot{a}$ with its characteristic function, so it is enough to add a new function $\dot{g} : \mathbb{N} \to \{0, 1\}$.Consider all the possible finite approximations of $\dot{g}$, namely

$$\mathbb{P} := \{f : \mathbb{N} \to \{0, 1\};\ f \text{ is finite}\}$$

For $p, q \in \mathbb{P}$, let

$$p \leq q \iff p \sqsupseteq q.$$

Let $1 := \emptyset$, $p \wedge q := p \cup q$, $p \vee q := p \cap q$.

If G is a generic *filter* on $\mathbb{P}$, then $\bigcup G : \mathbb{N} \to \{0, 1\}$ is a total function.

The intuition

Suppose you want to add a new set $\dot{a} \subseteq \mathbb{N}$. We can identify $\dot{a}$ with its characteristic function, so it is enough to add a new function $\dot{g} : \mathbb{N} \to \{0, 1\}$.Consider all the possible finite approximations of $\dot{g}$, namely

$$\mathbb{P} := \{f : \mathbb{N} \to \{0, 1\};\ f \text{ is finite}\}$$

For $p, q \in \mathbb{P}$, let

$$p \leq q \iff p \sqsupseteq q.$$

Let $1 := \emptyset$, $p \wedge q := p \cup q$, $p \vee q := p \cap q$.

If G is a generic *filter* on $\mathbb{P}$, then $\bigcup G : \mathbb{N} \to \{0, 1\}$ is a total function.

The forcing relation

Remark

If $p \leq \| \varphi \|$, then for every G such that $p \in G$, we have $M[G] \models \varphi$.

Definition

$$p \Vdash \varphi \text{ iff } p \leq \| \varphi \|$$

Forcing vs. realizability

Forcing	**Realizability**
$\mathbb{B}$: set of conditions (Boolean algebra)	Λ: the 'programs' ; Π : the 'stacks'
$\wedge$ 'meet'	( ) 'application' ; . 'push' ; $\star$ 'process' k_π 'continuation'
$\leq$ partial order on $\mathbb{B} \setminus \{0\}$	$\succ$ preorder on $\Lambda \star \Pi$
$\{1\}$	$\Lambda^* \subseteq \Lambda$: the 'proof-like programs' Contains the instructions I, K, W, C, B, cc and it's closed by application.
$\{0\}$ $p \perp q \iff p \wedge q = 0$	$\perp\subseteq \Lambda \star \Pi$ final segment
$\lVert \varphi \rVert \in \mathbb{B}$	$\lvert\varphi\rvert \subseteq \Lambda$; $\lVert\varphi\rVert \subseteq \Pi$
$p \Vdash \varphi$ iff $p \leq \lVert \varphi \rVert$	$\theta \Vdash \varphi$ iff $\theta \in \lvert\varphi\rvert$ i.e. $\theta \star \pi \in \perp$ for every $\pi \in \lVert\varphi\rVert$
$M^{\mathbb{P}} \models \varphi$ if $\lVert \varphi \rVert = 1$	$\mathcal{N} \models \varphi$ if $\exists\theta \in \Lambda^* \, (\theta \in \lvert\varphi\rvert)$

Krivine's machine

Krivine's machine

$\succ$ is the least preorder on $\Lambda \star \Pi$ such that for all $\xi, \eta, \zeta \in \Lambda$ and $\pi, \sigma \in \Pi$,

- $\xi(\eta) \star \pi \succ \xi \star \eta \,.\, \pi$
- $I \star \xi \,.\, \pi \succ \xi \star \pi$
- $K \star \xi \,.\, \eta \,.\, \pi \succ \xi \star \pi$
- $E \star \xi \,.\, \eta \,.\, \pi \succ \xi(\eta) \star \pi$
- $W \star \xi \,.\, \eta \,.\, \pi \succ \xi \star \eta \,.\, \eta \,.\, \pi$
- $C \star \xi \,.\, \eta \,.\, \zeta \,.\, \pi \succ \xi \star \zeta \,.\, \eta \,.\, \pi$
- $B \star \xi \,.\, \eta \,.\, \zeta \,.\, \pi \succ \xi(\eta(\zeta)) \star \pi$
- $cc \star \xi \,.\, \pi \succ \xi \star k_\pi \,.\, \pi$
- $k_\pi \star \xi \,.\, \sigma \succ \xi \star \pi$

Krivine's machine

We call 'combinatory terms' or *c*-terms the programs which are written with variables, instructions and the application. Every lambda-term can be translated into a *c*-term.

Execution theorem

Let $\theta[x_1, ..., x_n] \in \Lambda$ be a *c*-term, let $\xi_1, ..., \xi_n \in \Lambda$ and $\pi \in \Pi$, then

$$\lambda x_1 ... \lambda x_n . \theta \star \xi_1 \,.\, ... \,.\, \xi_n \,.\, \pi \succ \theta[\xi_1 / x_1, ..., \xi_n / x_n] \star \pi$$

Non extensional set theory ZF_ε

$\mathcal{L} = \{\varepsilon\ , \in, \subseteq\}$.
$x \simeq y$ is the formula $x \subseteq y \land y \subseteq x$

- Extensionality: $\forall x \forall y(x \in y \iff \exists z\ \varepsilon\ y(x \simeq z))$;
  $\forall x \forall y(x \subseteq y \iff \forall z\ \varepsilon\ x(z \in y))$
- Foundation:
  $\forall x_1 ... \forall x_n \forall a(\forall x(\forall y\ \varepsilon\ xF[y, x_1, ..., x_n] \Rightarrow F[x, x_1, ..., x_n]) \Rightarrow F[a, x_1, ..., x_n])$
- Pairing: $\forall a \forall b \exists x(a\ \varepsilon\ x \land b\ \varepsilon\ x)$
- Union: $\forall a \exists b \forall x\ \varepsilon\ a \forall y\ \varepsilon\ x(y\ \varepsilon\ b)$
- Powerset: $\forall a \exists b \forall x \exists y\ \varepsilon\ b \forall z(z\ \varepsilon\ y \iff (z\ \varepsilon\ a \land z\ \varepsilon\ x))$
- Replacement: $\forall x_1 ... \forall x_n \forall a \exists b \forall x\ \varepsilon\ a(\exists y F[x, y, x_1, ..., x_n] \Rightarrow (\exists y\ \varepsilon\ bF[x, y, x_1 ... x_n]))$
- Infinity $\forall x_1 ... x_n \forall a \exists b[a\ \varepsilon\ b \land \forall x\ \varepsilon\ b(\exists y F[x, y, x_1, ..., x_n] \Rightarrow \exists y\ \varepsilon\ bF[x, y, x_1, ..., x_n])]$

ZF_ε is a conservative extension of ZF.

The realizability relation

We define the two 'truth values' $|\varphi| \subseteq \Lambda$ and $\|\varphi\| \subseteq \Pi$.

$\xi \in |\varphi| \iff \forall \pi \in \|\varphi\| (\xi \star \pi \in \perp\!\!\!\perp)$

$\xi \Vdash \varphi$ means $\xi \in |\varphi|$

- $\|\top\| = \emptyset$, $\|\perp\| = \Pi$, $\|a \not\varepsilon b\| = \{\pi \in \Pi;\ (a, \pi) \in b\}$
- $\|a \subseteq b\| = \{\xi \,.\, \pi;\ \exists c (c, \pi) \in a \text{ and } \xi \Vdash c \notin b\}$
- $\|a \notin b\| = \{\xi \,.\, \xi' \,.\, \pi;\ \exists c (c, \pi) \in b \text{ and } \xi \Vdash a \subseteq c \text{ and } \xi' \Vdash c \subseteq a\}$
- $\|\varphi \Rightarrow \psi\| = \{\xi \,.\, \pi;\ \xi \Vdash \varphi \text{ and } \pi \in \|\psi\|\}$
- $\|\forall x \varphi\| = \bigcup_a \|\varphi[a/x]\|$

Adequacy lemma

Adequacy lemma

Let $A_1, ..., A_n, A$ be closed formulas of ZF_ε and suppose $x_1 : A_1, ..., x_n : A_n \vdash t : A$.
If $\xi_1 \Vdash A_1, ...\xi_n \Vdash A_n$, then $t[\xi_1/x_1, ..., \xi_n/x_n] \Vdash A$.

Corollary

If $\vdash t : A$, then $t \Vdash A$

The axioms of set theory are realized

$\mathcal{M}$ the ground model (a model of ZFC), $\mathcal{N}$ the realizability algebra.

Theorem

The axioms of ZF+DC are realized (i.e. $\mathcal{N} \models \varphi$ for every φ provable in ZF+DC)

Thank you