Primeros pasos de una formalización de Forcing

E. Gunther M. Pagano P. Sánchez Terraf[1]

CIEM-FaMAF — Universidad Nacional de Córdoba

Reunión Anual UMA
Universidad Nacional de La Plata, 21 / 09 / 2018

[1] Supported by CONICET and SeCyT-UNC

Resumen

1. Teoría de Conjuntos
   - Modelos de ZFC
   - Forcing
2. Verificación
   - Isabelle, Isar
3. Resultados Verificados

Modelos de ZFC

$ZFC =$ Zermelo + Fraenkel + Axioma de Elección (AC)

1. Es una **teoría de primer orden**. Existencia, Fundación, Pares, Union, Infinito, Partes, Separación, Reemplazo, Elección.

$$\forall x \exists p : \forall y \big(y \in p \longleftrightarrow \forall z \in y (z \in x) \big).$$

2. Se aplica la **Teoría de Modelos** estándar. Por ejemplo, por Löwenheim-Skolem, todo modelo $\langle M, E \rangle$ tiene un submodelo elemental contable.
3. **Modelo transitivo**: $\langle M, E \rangle$ tal que M es una familia de conjuntos que satisface $x \in y \in M \Rightarrow x \in M$ y $E := \in \cap (M \times M)$. Un **ctm** es un modelo contable transitivo.

Modelos de ZFC

$ZFC =$ Zermelo + Fraenkel + Axioma de Elección (AC)

1. Es una **teoría de primer orden**. Existencia, Fundación, Pares, Union, Infinito, Partes, Separación, Reemplazo, Elección.

$$\forall x \exists p : \forall y \big(y \in p \longleftrightarrow \forall z \in y (z \in x) \big).$$

2. Se aplica la **Teoría de Modelos** estándar. Por ejemplo, por Löwenheim-Skolem, todo modelo $\langle M, E \rangle$ tiene un submodelo elemental contable.

3. **Modelo transitivo**: $\langle M, E \rangle$ tal que M es una familia de conjuntos que satisface $x \in y \in M \Rightarrow x \in M$ y $E := \in \cap (M \times M)$. Un **ctm** es un modelo contable transitivo.

Modelos de ZFC

ZFC = Zermelo + Fraenkel + Axioma de Elección (AC)

1. Es una **teoría de primer orden**. Existencia, Fundación, Pares, Union, Infinito, Partes, Separación, Reemplazo, Elección.

$$\forall x \exists p : \forall y \big(y \in p \longleftrightarrow \forall z \in y (z \in x) \big).$$

2. Se aplica la **Teoría de Modelos** estándar. Por ejemplo, por Löwenheim-Skolem, todo modelo $\langle M, E \rangle$ tiene un submodelo elemental contable.
3. **Modelo transitivo**: $\langle M, E \rangle$ tal que M es una familia de conjuntos que satisface $x \in y \in M \Rightarrow x \in M$ y $E := \in \cap (M \times M)$. Un **ctm** es un modelo contable transitivo.

Modelos de ZFC

$ZFC =$ Zermelo + Fraenkel + Axioma de Elección (AC)

1. Es una **teoría de primer orden**. Existencia, Fundación, Pares, Union, Infinito, Partes, Separación, Reemplazo, Elección.

$$\forall x \exists p : \forall y \big(y \in p \longleftrightarrow \forall z \in y (z \in x) \big).$$

2. Se aplica la **Teoría de Modelos** estándar. Por ejemplo, por Löwenheim-Skolem, todo modelo $\langle M, E \rangle$ tiene un submodelo elemental contable.
3. **Modelo transitivo**: $\langle M, E \rangle$ tal que M es una familia de conjuntos que satisface $x \in y \in M \Rightarrow x \in M$ y $E := \in \cap \big(M \times M\big)$. Un **ctm** es un modelo contable transitivo.

El forcing es una técnica para extender modelos contables transitivos de ZFC.
Sea $M = \langle M, \in \rangle$ un ctm de ZFC. Sean $\mathbb{P}, \leq, \mathbb{0}, \mathbb{1} \in M$ tales que

$$M \models \langle \mathbb{P}, \leq, \mathbb{0}, \mathbb{1} \rangle \text{ es un retículo booleano.}$$

Si $\mathbb{P}$ es infinito, la mayoría de los $X \subseteq \mathbb{P}$ no estarán en M.
Idea: Tomar $G \in \mathscr{P}(\mathbb{P}) \setminus M$ y generar el menor modelo $M[G]$ de ZFC que contenga a G e incluya a M.

Problemas

1. Aun si existe modelo $N \supseteq \{G\} \cup M$, la intersección de modelos de ZFC no siempre lo es.
2. Aun si existe uno mínimo, no se sabe qué propiedades de primer orden tiene.

Forcing (un curso de 7')

El forcing es una técnica para extender modelos contables transitivos de ZFC.
Sea $M = \langle M, \in \rangle$ un ctm de ZFC. Sean $\mathbb{P}, \leq, \mathbb{0}, \mathbb{1} \in M$ tales que

$$M \models \langle \mathbb{P}, \leq, \mathbb{0}, \mathbb{1} \rangle \text{ es un retículo booleano.}$$

Si $\mathbb{P}$ es infinito, la mayoría de los $X \subseteq \mathbb{P}$ no estarán en M.
Idea: Tomar $G \in \mathscr{P}(\mathbb{P}) \setminus M$ y generar el menor modelo $M[G]$ de ZFC que contenga a G e incluya a M.

Problemas

1. Aun si existe modelo $N \supseteq \{G\} \cup M$, la intersección de modelos de ZFC no siempre lo es.
2. Aun si existe uno mínimo, no se sabe qué propiedades de primer orden tiene.

Forcing (un curso de 7')

El forcing es una técnica para extender modelos contables transitivos de ZFC. Sea $M = \langle M, \in \rangle$ un ctm de ZFC. Sean $\mathbb{P}, \leq, \mathbb{0}, \mathbb{1} \in M$ tales que

$$M \models \langle \mathbb{P}, \leq, \mathbb{0}, \mathbb{1} \rangle \text{ es un retículo booleano.}$$

Si $\mathbb{P}$ es infinito, la mayoría de los $X \subseteq \mathbb{P}$ no estarán en M.
Idea: Tomar $G \in \mathscr{P}(\mathbb{P}) \setminus M$ y generar el menor modelo $M[G]$ de ZFC que contenga a G e incluya a M.

Problemas

1. Aun si existe modelo $N \supseteq \{G\} \cup M$, la intersección de modelos de ZFC no siempre lo es.
2. Aun si existe uno mínimo, no se sabe qué propiedades de primer orden tiene.

Forcing (un curso de 7')

Solución

$G \subsetneq \mathbb{P}$ debe ser un filtro genérico:

1. $D \subseteq \mathbb{P} \setminus \{\mathbb{0}\}$ es **denso** si $\forall x \in \mathbb{P} \exists d \in D.(d \leq p)$.
2. G es **genérico** si corta a todos los densos *en* M.

Teorema (Cohen, 1963)

1. *Si G es genérico, existe el menor ctm $M[G]$ de ZFC que contiene a G e incluye a M.*
2. *Todo elemento $a \in M[G]$ está nombrado por un elemento $\dot{a}$ de M.*
3. *Hay traducción de la verdad en $M[G]$ a la de M.*

$$\left(\forall G. \quad M[G] \models \varphi(\mathrm{val}(G, \dot{a}))\right) \leftrightsquigarrow M \models \mathrm{forces}_{\varphi}(\mathbb{P}, \dot{a}).$$

Solución

$G \subsetneq \mathbb{P}$ debe ser un filtro genérico:

1. $D \subseteq \mathbb{P} \setminus \{\mathbb{0}\}$ es **denso** si $\forall x \in \mathbb{P} \exists d \in D.(d \leq p)$.
2. G es **genérico** si corta a todos los densos *en* M.

Teorema (Cohen, 1963)

1. *Si G es genérico, existe el menor ctm $M[G]$ de ZFC que contiene a G e incluye a M.*
2. *Todo elemento $a \in M[G]$ está nombrado por un elemento $\dot{a}$ de M.*
3. *Hay traducción de la verdad en $M[G]$ a la de M.*

$$\left(\forall G. \quad M[G] \models \varphi(\mathrm{val}(G, \dot{a}))\right) \leftrightsquigarrow M \models \mathrm{forces}_{\varphi}(\mathbb{P}, \dot{a}).$$

Solución

$G \subsetneq \mathbb{P}$ debe ser un filtro genérico:

1. $D \subseteq \mathbb{P} \setminus \{\mathbb{0}\}$ es **denso** si $\forall x \in \mathbb{P} \exists d \in D.(d \leq p)$.
2. G es **genérico** si corta a todos los densos *en* M.

Teorema (Cohen, 1963)

1. *Si G es genérico, existe el menor ctm $M[G]$ de ZFC que contiene a G e incluye a M.*
2. *Todo elemento $a \in M[G]$ está nombrado por un elemento $\dot{a}$ de M.*
3. *Hay traducción de la verdad en $M[G]$ a la de M.*

$$\left(\forall G. \quad M[G] \models \varphi(\mathrm{val}(G, \dot{a}))\right) \leftrightsquigarrow M \models \mathrm{forces}_{\varphi}(\mathbb{P}, \dot{a}).$$

Forcing (un curso de 7')

$$M[G] := \{\mathrm{val}(G,a) : a \in M\}$$

Interpretación por G

$\mathrm{val}(G,a) := \{\mathrm{val}(G,b) : \langle b,p\rangle \in a \wedge p \in G\}$.

¿$M \subseteq M[G]$?

Lema

$\mathrm{val}(G,\mathrm{check}(x)) = x$.

$$M[G] := \{\mathrm{val}(G,a) : a \in M\}$$

Interpretación por G

$\mathrm{val}(G,a) := \{\mathrm{val}(G,b) : \langle b,p\rangle \in a \wedge p \in G\}$.

¿$M \subseteq M[G]$?

Lema

$\mathrm{val}(G,\mathrm{check}(x)) = x$.

Forcing (un curso de 7')

$$M[G] := \{\mathrm{val}(G,a) : a \in M\}$$

Interpretación por G

$\mathrm{val}(G,a) := \{\mathrm{val}(G,b) : \langle b,p\rangle \in a \wedge p \in G\}$.

¿$M \subseteq M[G]$?

Lema

$\mathrm{val}(G,\mathrm{check}(x)) = x.$

Forcing (un curso de 7')

$$M[G] := \{\mathrm{val}(G,a) : a \in M\}$$

Interpretación por G

$\mathrm{val}(G,a) := \{\mathrm{val}(G,b) : \langle b,p\rangle \in a \wedge p \in G\}$.

¿$M \subseteq M[G]$?

$$\check{x} := \{\langle \check{y}, \mathbb{1}\rangle : y \in x\}$$

Lema

$\mathrm{val}(G,\mathrm{check}(x)) = x$.

Forcing (un curso de 7')

$$M[G] := \{\mathrm{val}(G,a) : a \in M\}$$

Interpretación por G

$\mathrm{val}(G,a) := \{\mathrm{val}(G,b) : \langle b,p\rangle \in a \wedge p \in G\}$.

¿$M \subseteq M[G]$?

$$\mathrm{check}(x) := \{\langle \mathrm{check}(y), \mathbb{1}\rangle : y \in x\}$$

Lema

$\mathrm{val}(G,\mathrm{check}(x)) = x$.

Forcing (un curso de 7')

$$M[G] := \{\mathrm{val}(G,a) : a \in M\}$$

Interpretación por G

$\mathrm{val}(G,a) := \{\mathrm{val}(G,b) : \langle b,p\rangle \in a \wedge p \in G\}$.

¿$M \subseteq M[G]$?

$$\mathrm{check}(x) := \{\langle \mathrm{check}(y), \mathbb{1}\rangle : y \in x\}$$

Lema

$\mathrm{val}(G, \mathrm{check}(x)) = x$.

Forcing (un curso de 7')

$$M[G] := \{\mathrm{val}(G,a) : a \in M\}$$

Interpretación por G

$\mathrm{val}(G,a) := \{\mathrm{val}(G,b) : \langle b,p\rangle \in a \wedge p \in G\}$.

¿$M \subseteq M[G]$?

$$\mathrm{check}(x) := \{\langle \mathrm{check}(y), \mathbb{1}\rangle : y \in x\}$$

Lema

$\mathrm{val}(G,\mathrm{check}(x)) = x$.

Verificación

La **verificación formal**: uso de *asistentes de prueba* para chequear que una demostración es correcta al máximo nivel de detalle.

No se omite ningún detalle, reduciendo el resultado a probar hasta los mismos axiomas.

Atención

Prueba formalizada $\neq$ Prueba automática

Herramientas

Agda, Coq, HOL Light, Lean, ACL2, Isabelle.

Verificación

La **verificación formal**: uso de *asistentes de prueba* para chequear que una demostración es correcta al máximo nivel de detalle.
No se omite ningún detalle, reduciendo el resultado a probar hasta los mismos axiomas.

Atención

$$\text{Prueba formalizada} \neq \text{Prueba automática}$$

Herramientas

Agda, Coq, HOL Light, Lean, ACL2, Isabelle.

Verificación

La **verificación formal**: uso de *asistentes de prueba* para chequear que una demostración es correcta al máximo nivel de detalle.
No se omite ningún detalle, reduciendo el resultado a probar hasta los mismos axiomas.

Atención

Prueba formalizada $\neq$ Prueba automática

Herramientas

Agda, Coq, HOL Light, Lean, ACL2, Isabelle.

Verificación

La **verificación formal**: uso de *asistentes de prueba* para chequear que una demostración es correcta al máximo nivel de detalle.
No se omite ningún detalle, reduciendo el resultado a probar hasta los mismos axiomas.

Atención

$$\text{Prueba formalizada} \neq \text{Prueba automática}$$

Herramientas

Agda, Coq, HOL Light, Lean, ACL2, Isabelle.

Isabelle: Pruebas hacia atrás

Una **regla**:

$$\llbracket P(0)\ ;\ \bigwedge n.\ (P(n) \implies P(n+1)) \rrbracket \implies \forall n \in \text{nat}.\ P(n) \tag{1}$$

Estado de prueba

1. $n^2 \geq 0.$

Aplicamos la regla (1) (`apply rule (1)`):

Estado de prueba

1. $0^2 \geq 0.$
2. $\bigwedge n.\quad n^2 \geq 0 \implies (n+1)^2 \geq 0.$

Una **regla**:

$$[\![P(0)\ ;\ \bigwedge n.\ (P(n) \implies P(n+1))]\!] \implies \forall n \in \text{nat}.\ P(n) \qquad (1)$$

Estado de prueba

1. $n^2 \geq 0.$

Aplicamos la regla (1) (`apply rule (1)`):

Estado de prueba

1. $0^2 \geq 0.$
2. $\bigwedge n.\quad n^2 \geq 0 \implies (n+1)^2 \geq 0.$

Isabelle: Pruebas hacia atrás

Una **regla**:

$$\llbracket P(0) \; ; \; \bigwedge n. \; (P(n) \implies P(n+1)) \rrbracket \implies \forall n \in \text{nat}. \; P(n) \tag{1}$$

Estado de prueba

1. $n^2 \geq 0$.

Aplicamos la regla (1) (`apply rule (1)`):

Estado de prueba

1. $0^2 \geq 0$.
2. $\bigwedge n. \quad n^2 \geq 0 \implies (n+1)^2 \geq 0$.

Ejemplo: Prueba de DC, aplicativa

Teorema

```
"(∀x∈A. ∃y∈A. ⟨x,y⟩∈ R) ⟹
                          ∀a∈A. (∃f ∈ nat→A. f`0 = a
∧ (∀n ∈ nat. ⟨f`n,f`succ(n)⟩∈R))"
```

Ejemplo: Prueba de DC, aplicativa

Teorema

"(∀x∈A. ∃y∈A. ⟨x,y⟩∈ R) ⟹
∀a∈A. (∃f ∈ nat→A. f‘0 = a
∧ (∀n ∈ nat. ⟨f‘n,f‘succ(n)⟩∈R))"

```
theorem pointed_DC  : "(∀x∈A. ∃y∈A. ⟨x,y⟩∈ R) ⟹
                        ∀a∈A. (∃f ∈ nat→A. f`0 = a ∧ (∀n ∈ nat. ⟨f`n,f`succ(n)⟩∈R))"
  apply (rule)
  apply (insert AC_func_Pow)
  apply (drule allI)
  apply (drule_tac x="A" in spec)
  apply (drule_tac P="λf .∀x∈Pow(A) - {0}. f ` x ∈ x"
              and A="Pow(A)-{0}→ A"
              and Q=" ∃f∈nat→ A. f ` 0 = a ∧ (∀n∈nat. ⟨f ` n, f ` succ(n)⟩ ∈ R)" in bexE
  prefer 2 apply (assumption)
  apply (rename_tac s)
  apply (rule_tac x="λn∈nat. dc_witness(n,A,a,s,R)" in bexI)
   prefer 2  apply (blast intro:witness_funtype)
  apply (rule  conjI, simp)
  apply (rule ballI, rename_tac m)
  apply (subst beta, simp)+
  apply (rule witness_related, auto)
  done
```

Isar: Pruebas “del derecho”

lemma : $\forall x \in \{4,5,6\}.\ 0 < x$

Estado

1. $\forall x \in \{4,5,6\}.\ 0 < x$

Isar: Pruebas "del derecho"

lemma : $\forall x \in \{4,5,6\}.\ 0 < x$
proof

Estado

1. $\bigwedge x.\ \ x \in \{4,5,6\} \implies 0 < x$

Isar: Pruebas “del derecho”

lemma : $\forall x \in \{4,5,6\}.\ 0 < x$
proof
  fix x
  assume $x \in \{4,5,6\}$

Estado

1. $\bigwedge x.\ \ x \in \{4,5,6\} \implies 0 < x$

Isar: Pruebas “del derecho”

lemma : $\forall x \in \{4,5,6\}.\ 0 < x$
proof
fix x
assume $x \in \{4,5,6\}$
then show $0 < x$

Estado

1. $0 < x$

Isar: Pruebas “del derecho”

lemma : $\forall x \in \{4,5,6\}.\ 0 < x$
proof
  fix x
  assume $x \in \{4,5,6\}$
  then show $0 < x$
    by auto

Estado

$$?x \in \{4,5,6\} \implies 0 < ?x$$

Isar: Pruebas "del derecho"

lemma : $\forall x \in \{4,5,6\}.\ 0 < x$
proof
  fix x
  assume $x \in \{4,5,6\}$
  then show $0 < x$
    by auto
qed

Estado

theorem $\forall x \in \{4,5,6\}.\ 0 < x$

Existencia de filtros genéricos

Lema (Rasiowa-Sikorski)

Sea $\mathbb{P}$ retículo booleano y $D_n \subseteq \mathbb{P} \setminus \{\mathbb{0}\}$ ($n \in \mathbb{N}$) densos. Entonces existe un filtro $G \subseteq \mathbb{P} \setminus \{\mathbb{0}\}$ que corta a cada D_n.

Corolario

Si M es un ctm y $\mathbb{P} \in M$ es como arriba, existe un filtro genérico $G \subseteq \mathbb{P} \setminus \{\mathbb{0}\}$.

Existencia de filtros genéricos

Lema (Rasiowa-Sikorski)

Sea $\mathbb{P}$ retículo booleano y $D_n \subseteq \mathbb{P} \setminus \{\mathbb{0}\}$ ($n \in \mathbb{N}$) densos. Entonces existe un filtro $G \subseteq \mathbb{P} \setminus \{\mathbb{0}\}$ que corta a cada D_n.

Corolario

Si M es un ctm y $\mathbb{P} \in M$ es como arriba, existe un filtro genérico $G \subseteq \mathbb{P} \setminus \{\mathbb{0}\}$.

Pares en la extensión genérica

$$\langle N, E\rangle \models \forall x, y \exists c : \forall z(z \in c \leftrightarrow z = x \vee z = y)$$

Si N es un ctm, varias propiedades son absolutas.

Para todos $x, y \in N$, $\{x, y\} \in N$.

[Paulson 2003]: Implementación en Isabelle/ZF de constructibilidad
$\longrightarrow$ consistencia de AC

Lema

$\mathrm{val}(G, \{\langle a, \mathbb{1}\rangle, \langle b, \mathbb{1}\rangle\}) = \{\mathrm{val}(G, a), \mathrm{val}(G, b)\}$

Pares en la extensión genérica

$$\langle N, E\rangle \models \forall x, y \exists c : \forall z (z \in c \leftrightarrow z = x \vee z = y)$$

Si N es un ctm, varias propiedades son absolutas.

Para todos $x, y \in N$, $\{x, y\} \in N$.

[Paulson 2003]: Implementación en Isabelle/ZF de constructibilidad
$\longrightarrow$ consistencia de AC

Lema

$\mathrm{val}(G, \{\langle a, \mathbb{1}\rangle, \langle b, \mathbb{1}\rangle\}) = \{\mathrm{val}(G, a), \mathrm{val}(G, b)\}$

Pares en la extensión genérica

$$\langle N, E\rangle \models \forall x, y \exists c : \forall z (z \in c \leftrightarrow z = x \vee z = y)$$

Si N es un ctm, varias propiedades son absolutas.

Para todos $x, y \in N$, $\{x, y\} \in N$.

[Paulson 2003]: Implementación en Isabelle/ZF de constructibilidad
$\longrightarrow$ consistencia de AC

Lema

$\mathrm{val}(G, \{\langle a, \mathbb{1}\rangle, \langle b, \mathbb{1}\rangle\}) = \{\mathrm{val}(G, a), \mathrm{val}(G, b)\}$

Pares en la extensión genérica

$$\langle N, E\rangle \models \forall x, y \exists c : \forall z (z \in c \leftrightarrow z = x \vee z = y)$$

Si N es un ctm, varias propiedades son absolutas.

Para todos $x, y \in N$, $\{x, y\} \in N$.

[Paulson 2003]: Implementación en Isabelle/ZF de constructibilidad

$\longrightarrow$ consistencia de AC

Lema

$\mathrm{val}(G, \{\langle a, \mathbb{1}\rangle, \langle b, \mathbb{1}\rangle\}) = \{\mathrm{val}(G, a), \mathrm{val}(G, b)\}$

Pares en la extensión genérica

$$\langle N, E\rangle \models \forall x, y \exists c : \forall z (z \in c \leftrightarrow z = x \lor z = y)$$

Si N es un ctm, varias propiedades son absolutas.

Para todos $x, y \in N$, $\{x, y\} \in N$.

[Paulson 2003]: Implementación en Isabelle/ZF de constructibilidad
$\longrightarrow$ consistencia de AC

Lema

$\mathrm{val}(G, \{\langle a, \mathbb{1}\rangle, \langle b, \mathbb{1}\rangle\}) = \{\mathrm{val}(G, a), \mathrm{val}(G, b)\}$

A los fierros…

¡Gracias!