The Relative Consistency of the Axiom of Choice

Mechanized Using Isabelle/ZF

Lawrence C. Paulson
Computer Laboratory

UNIVERSITY OF
CAMBRIDGE

Why Do Proofs By Machine?

- Too many been done already!
  - Gödel’s incompleteness theorem (Shankar)
  - thousands of Mizar proofs
- But many types of reasoning are hard to formalize.
  - Algebraic structures (e.g. group theory)
  - Proofs involving metamathematics
- And this one concerns Hilbert’s First Problem!

Outline of Gödel’s Proof

- Define the *constructible universe*, **L**
- Show that **L** satisfies the ZF axioms
- Show that **L** satisfies the axiom **V=L**
- Show that **V=L** implies AC and GCH

A contradiction from ZF and **V=L** can be translated into one from ZF alone.

The Sets That Must Exist

$\mathcal{D}(X)$: the *definable* subsets of X

$$L_0 = 0$$

$$L_{\alpha+1} = \mathcal{D}(L_\alpha)$$

$$L_\alpha = \bigcup_{\xi<\alpha} L_\xi \quad \text{when } \alpha \text{ is limit}$$

finally $\quad \mathbf{L} = \bigcup_{\alpha \in \mathbf{ON}} L_\alpha$

L satisfies the ZF axioms

- Union, pairing
  - Unions and pairs are definable by formulae
- Powerset, replacement scheme
  - Using a rank function for **L**
- Comprehension scheme (separation)
  - By the Reflection Theorem
  - Scheme can be proved only in the metatheory

Show that **L** satisfies **V=L**

- **V=L** means “all sets are constructible”
- The concept of “constructible” is *absolute*
- Absolute means *same in all models*
  - Most concepts are absolute: unions, ordinals, functions, bijections, etc.
  - Not absolute: powersets, function spaces, cardinals

Show that $\mathbf{V}=\mathbf{L}$ implies AC
(or rather, the well-ordering theorem)

- The set of formulae is countable
- Parameter lists for formulae can be well-ordered lexicographically
- So, if X is well-ordered then so is $\mathcal{D}(X)$
- Inductively construct a well-ordering on $\mathbf{L}$

Satisfaction for Class Models?

For M a set, can define satisfaction recursively:

$$M \models \phi(x_1, \ldots, x_n) \quad \text{for } x_1, \ldots, x_n \in M$$

For $\mathbf{M}$ a class, satisfaction cannot be defined!

The nondefinability of truth (Tarski)

Satisfaction Defined Syntactically

$$
\begin{aligned}
(x = y)^{\mathbf{M}} &\mapsto x = y \\
(x \in y)^{\mathbf{M}} &\mapsto x \in y \\
(\phi \wedge \psi)^{\mathbf{M}} &\mapsto \phi^{\mathbf{M}} \wedge \psi^{\mathbf{M}} \\
(\neg\phi)^{\mathbf{M}} &\mapsto \neg(\phi^{\mathbf{M}}) \\
(\exists x\, \phi)^{\mathbf{M}} &\mapsto \exists x\, (x \in \mathbf{M} \wedge \phi^{\mathbf{M}})
\end{aligned}
$$

The *relativization* of □to $\mathbf{M}$

A contradiction using **V=L**?

- Can prove that $(\mathbf{V}=\mathbf{L})^{\mathbf{L}}$ is a ZF theorem
- … as is $\square^{\mathbf{L}}$ provided $\square$ is a ZF axiom
- Thus, a contradiction from ZF + $(\mathbf{V}=\mathbf{L})$ amounts to a contradiction in ZF alone
- Developing the argument (Gödel never did) requires proof theory

Isabelle/ZF

- Same code base as Isabelle/HOL
- Higher-order metalogic, ideal for
  - Theorem schemes
  - Classes
  - Class functions
- Develops set theory from the Zermelo-Fraenkel axioms to transfinite cardinals

Defining the Class **L** in Isabelle

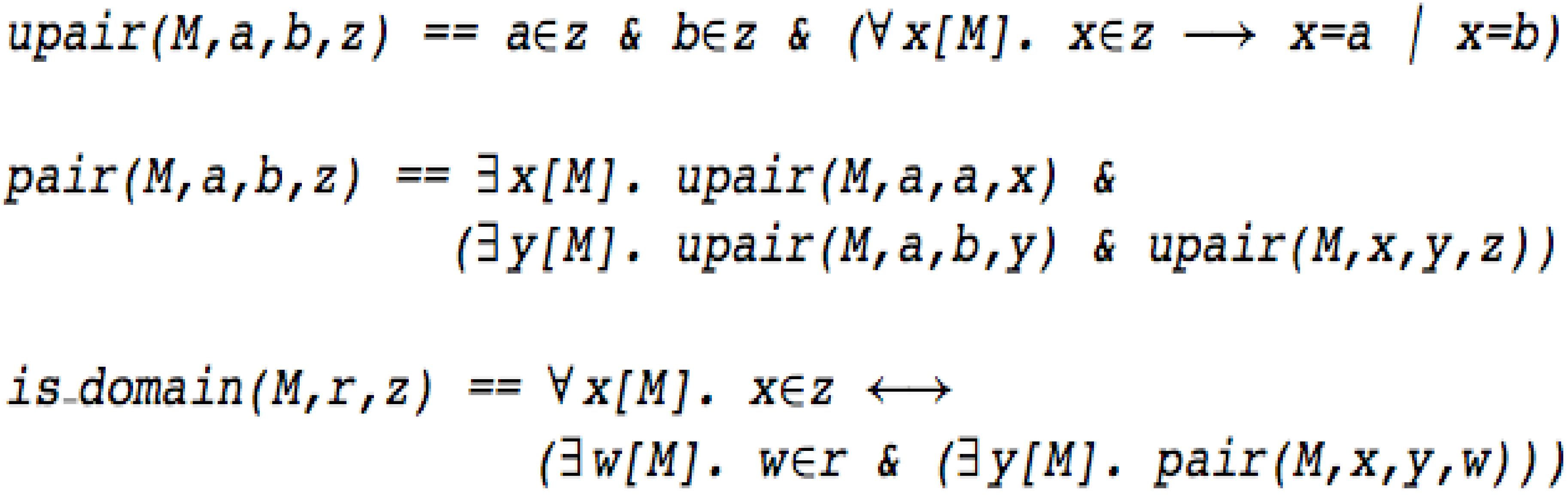
- Datatype declaration of the set `formula`
- Primitive recursive functions:
  - Satisfaction relation
  - Arity of a formula
  - De Bruijn renaming
- Definable powersets: `Dpow(X)`
- Constructible hierarchy: `Lset(i)`
- The predicate `L`

Relativization in Isabelle

- Define a separate predicate for each concept: 0, □, □, function, limit ordinal, …
- Make each predicate relative to a class **M**
- Absoluteness: prove that the predicate agrees with the native concept

Outcome: a relational language of sets

Examples: Pairs and Domains



```
upair(M,a,b,z) == a∈z & b∈z & (∀x[M]. x∈z ⟶ x=a | x=b)

pair(M,a,b,z) == ∃x[M]. upair(M,a,a,x) &
                   (∃y[M]. upair(M,a,b,y) & upair(M,x,y,z))

is_domain(M,r,z) == ∀x[M]. x∈z ⟷
                      (∃w[M]. w∈r & (∃y[M]. pair(M,x,y,w)))
```

Proving that **L** is a Model of ZF

- Express ZF axioms using the predicates
- Mechanize proofs from Kunen (1980)
- Separation axiom (comprehension):
  - By previous proof of Reflection Theorem
  - Meta-□ quantifier to hide giant classes
  - Automatic translation from real formulae to elements of the set *`formula`*
  - 40 separate instances proved

Proving that $\mathbf{L}$ is a Model of $\mathbf{V{=}L}$

- Absoluteness of well-founded recursion
- Absoluteness and relativization for …
  - Recursive datatypes
  - About 100 primitive concepts
  - The satisfaction function (detailed breakdown needed)
- The concepts *Dpow(X)* and *Lset(i)*
- Define *Constructible(M,x)*
- Finally prove *L(x)* ▯ *Constructible(L,x)*

Comparative Sizes of Theories

(in Tokens)

Reflection theorem	3400
Definition of L	4140
ZF holds in **L** (excluding separation)	5100
V=**L** holds in **L**	29700
V=**L** implies AC	1769

Doing without Metamathematics

- Can’t reason on the structure of formulae
- Can’t prove separation schematically
- Can’t formalize how a contradiction from **V=L** leads to a contradiction in ZF
- But: can use native set theory
  - Isabelle/ZF’s built-in set theory libraries
  - benefits of a shallow embedding

Conclusions

- A mechanized proof of consistency for AC
- Big:12000 lines or 49000 tokens
- Just escape having to formalize metatheory
- Future challenges:
  - Repeat, with a formalized metatheory
  - Prove generalized continuum hypothesis
  - Formalize forcing proofs: independence of AC