# On the Set Theory of Fitch-Prawitz

F. Honsell[1], M. Lenisa[1], L. Liquori[2], I. Scagnetto[1]
{furio.honsell,marina.lenisa,ivan.scagnetto}@uniud.it

Department of Mathematics and Computer Science (University of Udine)[1]
Inria Sophia Antipolis Méditerranée (France)[2]

TYPES 2016
Novi Sad, 23-26 May 2016

# Introduction

- Cantor's Set Theory with full Comprehension ($\{x \mid A(x)\}$ is a set for any formula $A$) is inconsistent.
- This made Foundational Theories of only sets almost a taboo.
- Few exceptions: Quine's NF and the Theory of Hyperuniverses [Forti-Honsell] restrict the class of formulæ in the Comprehension Principle, and preserve extensionality.
- A different approach [Fitch-Prawitz]: full comprehension, but restrict the shape of deductions to normal(izable) deductions.
- FP theory is quite powerful: we give a Fixed Point Theorem, whereby one can show that all recursive functions are definable.
- We show how to encode the highly unorthodox side condition of FP in a Logical Framework using locked types.
- We provide a connection between FP and Hyperuniverses: the strongly extensional quotient of the coalgebra of closed terms of FP satisfies the abstraction principle for Generalized Positive Formulæ.

# The Theory of Fitch-Prawitz (FP)

$$\text{Terms} \quad t ::= x \mid \lambda x.A$$

Formulæ $\quad A ::= \bot \mid \neg A \mid A \wedge A \mid A \vee A \mid A \rightarrow A \mid \forall x.A \mid \exists x.A \mid t \in u$ ,

where $\neg A$ is an abbreviation for $A \rightarrow \bot$, and $\lambda x.A$ denotes $\{x \mid A\}$.

Some rules (classical version)

$\wedge I)\quad \dfrac{A \quad B}{A \wedge B}$ $\qquad \wedge E)\quad \dfrac{A \wedge B}{A} \quad \dfrac{A \wedge B}{B}$

$\rightarrow I)\quad \dfrac{\begin{matrix}(A)\\ \vdots \\ B\end{matrix}}{A \rightarrow B}$ $\qquad \rightarrow E)\quad \dfrac{A \quad A \rightarrow B}{B}$ $\qquad \bot)\quad \dfrac{\begin{matrix}(\neg A)\\ \vdots \\ \bot\end{matrix}}{A}$

$\forall I)\quad \dfrac{A[y/x]}{\forall x.A}$ $\qquad \forall E)\quad \dfrac{\forall x.A}{A[t/x]}$

$\lambda I)\quad \dfrac{A[t/x]}{t \in \lambda x.A}$ $\qquad \lambda E)\quad \dfrac{t \in \lambda x.A}{A[t/x]}$

# Deductions in FP

- Standard deductions are called quasi-deductions in FP.
- Maximum formula in a deduction: a formula that is both the consequence of an application of a I-rule or of the $\bot$-rule, and (major) premiss of an application of the corresponding E-rule.
- A deduction in FP is a quasi-deduction with no maximum formulæ, *i.e.* a normal proof.
- Considering simply proofs which do not derive $\bot$ would lead to complications, because subproofs with conclusion $\bot$ are necessary.

**Theorem**

*Normal proofs cannot derive $\bot$, hence FP is consistent.*

# FP: pros and cons

- The $\perp$)-rule is classical negation and it encompasses the double negation rule $\frac{\neg\neg A}{A}$, and the rule ex falso sequitur quodlibet $\frac{\perp}{A}$.
- Full elimination rules are not admissible. *E.g.* Modus Ponens cannot be applied naïvely.
- The constraint of considering quasi-deductions to be legal only if already in normal form can be weakened to allow for normalizable quasi-derivations.
- Scotus rule ex absurdis sequitur quodlibet $\frac{A \quad \neg A}{\perp}$ is not admissible. But Aristotle's non-contradiction principle fails: $\vdash_{\mathsf{FP}} A \wedge \neg A$. Thus FP is paraconsistent.

# The taming of Russell's Paradox

Russell's Paradox. Let $t \triangleq \lambda x.(x \notin x)$, where $t \notin t \triangleq (t \in t \to \bot)$.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{t \in t^{(1)}}{t \notin t} \qquad t \in t^{(1)}}{\bot}}{t \notin t}}{t \in t} \qquad \dfrac{\dfrac{\dfrac{t \in t^{(1)}}{t \notin t} \qquad t \in t^{(1)}}{\bot}}{t \notin t}}{\bot}$$

- $\vdash_{\mathrm{FP}} (t \in t) \wedge (t \notin t)$ (failure of Aristotle's Principle of non-contradiction).
- But $\nvdash_{\mathrm{FP}} \bot$.
- Contraction rule is used.
- Naïve Set Theory without contraction is consistent [Grishin82]. This amounts to a Set Theory with Girard's Linear Logic without exponentials.
- Minimal logic is already inconsistent because of contraction.

# Equality and Extensionality

Leibniz Equality $t_1 = t_2 \stackrel{\Delta}{=} \forall x.\ t_1 \in x \leftrightarrow t_2 \in x$ .

Extensionality Equality $t_1 \simeq t_2 \stackrel{\Delta}{=} \forall x.\ x \in t_1 \leftrightarrow x \in t_2$ .

- $\vdash_{\mathsf{FP}} t_1 \simeq t_2 \to t_1 = t_2$.
- The converse implication amounts to the Extensionality Axiom $t_1 = t_2 \to t_1 \simeq t_2$.
- [Grishin82]: adding Extensionality Axiom, contraction rule is admissible.
- $\mathsf{FP} + \mathsf{Ext} \vdash_{\mathsf{FP}} \bot$.

# Developing Mathematics in FP

- Recursive definitions in FP as in functional programming.
- Fixed Point Theorem: Given a formula $A$ with free variables $x, z_1, \ldots, z_n$, $n > 0$, there exists $u$ s.t.

$$\vdash_{\mathrm{FP}} \vec{z} \in u \longleftrightarrow A[u/x] \ .$$

- Numerals: Let $A_{\mathrm{Nat}} \stackrel{\Delta}{=} z = 0 \ \vee \ \exists y. \ (y \in x \ \wedge \ z =< S, y >)$ .
Then there exists a term Nat s.t.

$$\vdash_{\mathrm{FP}} z \in \mathrm{Nat} \ \longleftrightarrow \ (z = 0 \ \vee \ \exists y. \ (y \in \mathrm{Nat} \ \wedge \ z =< S, y >)) \ .$$

- Factorial: Let
$A_{\mathrm{Fact}} \stackrel{\Delta}{=} ((z_1 = 0 \ \wedge \ z_2 = 1) \ \vee \ \exists y_1, y_2. \ (z_1 = y_1 + 1 \ \wedge \ \langle y_1, y_2 \rangle \in x \ \wedge \ z_2 = y_2 \times z_1)$ .
Then there exists a term Fact s.t.

$$\vdash_{\mathrm{FP}} \langle z_1, z_2 \rangle \in \mathrm{Fact} \ \longleftrightarrow \ ((z_1 = 0 \ \wedge \ z_2 = 1) \ \vee \ \exists y_1, y_2. \ (z_1 = y_1 + 1 \ \wedge \ \langle y_1, y_2 \rangle \in \mathrm{Fact} \ \wedge \ z_2 = y_2 \times z_1)) \ .$$

- FP is a universal model of computation.

# FP in Type Theory based on Logical Frameworks

Problem: capture the side-condition of normal deductions.

In [Honsell-Liquori-Scagnetto2016] FP is encoded in $\text{LLF}_{\mathcal{P}}$.

$\text{LLF}_{\mathcal{P}}$ extends LF with the lock constructor for building objects $\mathcal{L}^{\mathcal{P}}_{N,\sigma}[M]$ of type $\mathcal{L}^{\mathcal{P}}_{N,\sigma}[\rho]$. Locks allow to factor out specific constraints.

An unlock destructor, $\mathcal{U}^{\mathcal{P}}_{N,\sigma}[M]$, and an elimination rule $(O \cdot Top \cdot Unlock)$, eliminates the lock-type constructor, under the condition that a specific predicate $\mathcal{P}$ is verified, possibly externally, on a judgement:

$$\frac{\Gamma \vdash_\Sigma M : \rho \quad \Gamma \vdash_\Sigma N : \sigma}{\Gamma \vdash_\Sigma \mathcal{L}^{\mathcal{P}}_{N,\sigma}[M] : \mathcal{L}^{\mathcal{P}}_{N,\sigma}[\rho]} \text{(O·Lock)} \qquad \frac{\Gamma \vdash_\Sigma M : \mathcal{L}^{\mathcal{P}}_{N,\sigma}[\rho] \quad \mathcal{P}(\Gamma \vdash_\Sigma N : \sigma)}{\Gamma \vdash_\Sigma \mathcal{U}^{\mathcal{P}}_{N,\sigma}[M] : \rho} \text{(O·Top·Unlock)}$$

Equality rule for lock types (lock reduction): $\mathcal{U}^{\mathcal{P}}_{N,\sigma}[\mathcal{L}^{\mathcal{P}}_{N,\sigma}[M]] \to_{\mathcal{L}} M$.

Capitalizing on the monadic nature of the lock constructor, one can use locked terms without necessarily establishing the predicate, provided an outermost lock is present.

# Encoding FP in $LLF_{\mathcal{P}}$

In our encoding, the global normalization constraint is enforced locally by specifying a suitable lock on the proof-object:

- the obvious predicate to use in the lock-type (*i.e.*, checking that a proof term is normalizable) would not be well-behaved: free variables, *i.e.* assumptions, have to be "sterilized";
- hence, we make a distinction between generic judgements, which can be assumed, but not used directly, and apodictic judgements, which are directly involved in proof rules;
- in order to make use of generic judgements, one has to downgrade them to apodictic ones, by a suitable coercion function.

# The encoding of FP in $\mathrm{LLF}_{\mathcal{P}}$

The signature is the following:

$$
\begin{array}{llll}
\texttt{o} : \texttt{Type} & & \iota : \texttt{Type} \\
\texttt{T} : \texttt{o -> Type} & & \delta : \Pi\texttt{A:o. (V(A) -> T(A))} \\
\texttt{V} : \texttt{o -> Type} & & \lambda_{\texttt{intro}} : \Pi\texttt{A:}\iota\texttt{ ->o.}\Pi\texttt{x:}\iota\texttt{.T(A x) -> T(}\epsilon\texttt{ x (lam A))} \\
\texttt{lam} : (\iota\texttt{ -> o)->}\ \iota & & \lambda_{\texttt{elim}} : \Pi\texttt{A:}\iota\texttt{ ->o.}\Pi\texttt{x:}\iota\texttt{.T(}\epsilon\texttt{ x (lam A))->T(A x)} \\
\epsilon : \iota\texttt{ -> }\iota\texttt{ -> o} & & \supset_{\texttt{intro}} : \Pi\texttt{A,B:o.(V(A) -> T(B)) -> (T(A}\supset\texttt{B))} \\
\supset : \texttt{o -> o -> o} & & \supset_{\texttt{elim}} : \Pi\texttt{A,B:o.}\Pi\texttt{x:T(A).}\Pi\texttt{y:T(A}\supset\texttt{B) -> } \mathcal{L}^{\texttt{Fitch}}_{\langle\texttt{x,y}\rangle,\texttt{T(A)}\times\texttt{T(A}\supset\texttt{B)}}[\texttt{T(B)}]
\end{array}
$$

where:

- o is the type of propositions,
- $\supset$ and the "membership" predicate $\epsilon$ are the syntactic constructors for propositions,
- lam is the "abstraction" operator for building "sets",
- T is the apodictic judgement,
- V is the generic judgement,
- $\delta$ is the coercion function,
- $\langle \mathrm{x}, \mathrm{y} \rangle$ denotes the encoding of pairs.

# Adequacy

In the type of the constructor $\supset_{\mathtt{elim}}$:

$$\supset_{\mathtt{elim}} : \Pi\mathtt{A},\mathtt{B}:\mathtt{o}.\Pi\mathtt{x}:\mathtt{T(A)}.\Pi\mathtt{y}:\mathtt{T(A\supset B)} \texttt{ -> } \mathcal{L}^{\mathtt{Fitch}}_{\langle\mathtt{x,y}\rangle,\mathtt{T(A)}\times\mathtt{T(A\supset B)}}[\mathtt{T(B)}]$$

the predicate $\mathtt{Fitch}(\Gamma \vdash_{\Sigma_{\mathsf{FPST}}} \langle \mathtt{x}, \mathtt{y}\rangle \Leftarrow \mathtt{T(A)}\times\mathtt{T(A} \supset \mathtt{B))}$ holds iff: $\mathtt{x}$ and $\mathtt{y}$ have skeletons in $\Lambda_{\Sigma_{\mathsf{FPST}}}$, *i.e.* can be expressed as instantiations of contexts such that all the holes of which have

- either type o
- or are guarded by a $\delta$, and hence have type $\mathtt{V(A)}$,

and, moreover, the proof derived by combining the skeletons of $\mathtt{x}$ and $\mathtt{y}$ is normalizable in the natural sense.

**Theorem (Adequacy for Fitch-Prawitz Naive Set Theory)**

*If $A_1, \ldots, A_n$ are the atomic formulas occurring in $B_1, \ldots, B_m, A$, then $B_1 \ldots B_m \vdash_{\mathsf{FPST}} A$ iff there exists a normalizable* $\mathtt{M}$ *such that* $\mathtt{A_1}{:}\mathtt{o}, \ldots, \mathtt{A_n}{:}\mathtt{o}, \mathtt{x_1}{:}\mathtt{V(B_1)}, \ldots, \mathtt{x_m}{:}\mathtt{V(B_m)} \vdash_{\Sigma_{\mathsf{FPST}}} \mathtt{M} \Leftarrow \mathtt{T(A)}$ *(where* $\mathtt{A}$*, and* $\mathtt{B_i}$ *represent the encodings of, respectively, $A$ and $B_i$ in* $\mathsf{CLLF}_{\mathcal{P}}$*, for $1 \le i \le m$).*

# The Theory of Hyperuniverses TH

The naive Comprehension Principle can be approximated, by restricting the class of admissible formulæ.

Generalized Positive Comprehension Scheme (GPC) [Forti-Hinnion89,Forti-Honsell89]

$\{x \mid A\}$ is a set, if $A$ is a Generalized Positive Formula ,

where Generalized Positive Formulæ (GPF) are the smallest class of formulæ

- including $u \in t$, $u = t$;
- closed under the logical connectives $\wedge, \vee$;
- closed under the quantifiers $\forall x, \exists x, \forall x \in y, \exists x \in y$, where $\forall x \in y.A$ ($\exists x \in y.A$) is an abbreviation for $\forall x.(x \in y \to A)$ ($\exists x.(x \in y \to A)$);
- closed under the formula $\forall x.(B \to A)$, where $A$ is a generalized positive formula and $B$ is any formula such that $\mathrm{Fv}(B) \subseteq \{x\}$. Akin to restricted quantification.

The Theory of Hyperuniverses TH, namely GPC + Extensionality, is consistent [Forti-Honsell89].

# Set-theoretic Structures and $\mathcal{P}(\ )$-coalgebras

- A set-theoretic structure $(X, \in)$ is a first-order structure with a predicate $\in$ on $X \times X$.
- Set-theoretic structures are coalgebras for the powerset functor $\mathcal{P}(\ )$:

$$f_X : X \longrightarrow \mathcal{P}(X) \qquad f_X(x) = \{y \mid y \in x\} \ .$$

- A $\mathcal{P}(\ )$-coalgebra $(X, f_X)$ is extensional if $f_X$ is injective.
- A $\mathcal{P}(\ )$-coalgebra $(X, f_X)$ is strongly extensional if the unique coalgebra morphism from $(X, f_X)$ into the final coalgebra is injective.

# The Extensional Quotient of the Fitch-Prawitz Coalgebra

- Fitch-Prawitz Coalgebra $f_{\mathcal{T}^0} : \mathcal{T}^0 \longrightarrow \mathcal{P}(\mathcal{T}^0)$

$$f_{\mathcal{T}^0}(t) = \{u \mid \vdash_{\mathsf{FP}} u \in t\} \ .$$

- Bisimilarity can be defined in FP:

$$\sim \ \stackrel{\Delta}{=} \{\langle t, t'\rangle \mid \exists R. \ (\langle t, t'\rangle \in R \ \wedge \ A_{\mathsf{Bis}}[R/x])\} \ ,$$

where $A_{\mathsf{Bis}} \stackrel{\Delta}{=} \forall t, t' \ (\langle t, t'\rangle \in x \ \longrightarrow$
$$\forall u(u \in t \ \longrightarrow \ \exists u'(u' \in t' \ \wedge \ \langle u, u'\rangle \in x)) \ \wedge$$
$$\forall u'(u' \in t' \ \longrightarrow \ \exists u.(u \in t \ \wedge \ \langle u, u'\rangle \in x))) \ .$$

- $\sim$-quotient of the FP-coalgebra: for any $t \in \mathcal{T}^0$, $\underline{t} \in \mathcal{M}$, where

$$\underline{t} \stackrel{\Delta}{=} \{t' \mid \ \vdash_{\mathsf{FP}} t \sim t'\} \ .$$

- $\mathcal{P}(\ )$-coalgebra on $\mathcal{M}$, $f_{\mathcal{M}} : \mathcal{M} \to \mathcal{P}(\mathcal{M})$:

$$f_{\mathcal{M}}(\underline{t}) = \{\underline{s} \mid \ \vdash_{\mathsf{FP}} s \in t\} \ .$$

# Strong Extensionality of $\mathcal{M}$ in FP$^+$

We work in FP$^+$, *i.e.* FP plus

$$(\text{Bounded-}\omega) \quad \frac{A[w/x] \text{ for all closed } w \text{ s.t. } B[w/x],\ \mathrm{Fv}(B) \subseteq \{x\}}{\forall x.(B[w/x] \to A)}$$

**Proposition**

*The quotient $\mathcal{M}$ is extensional, i.e. for all $\underline{t}, \underline{t}' \in \mathcal{M}$,*

$$\underline{t} = \underline{t}' \iff f_{\mathcal{M}}(\underline{t}) = f_{\mathcal{M}}(\underline{t}')\ .$$

*Moreover, $\mathcal{M}$ is strongly extensional.*

# Relating FP to TH

$\mathcal{M}$ satisfies the Generalized Positive Comprehension Scheme, namely it is a hyperuniverse.

## Definition

Given a $A$ formula with constants in $\mathcal{M}$, we define $\widehat{A}$ corresponding formula in $FP^+$:

$$A \triangleq \underline{u} \in \underline{t} \implies \widehat{A} \triangleq \exists u'.u' \sim u \;\wedge\; u' \in t \qquad A \triangleq \neg A_1 \implies \widehat{A} \triangleq \neg \widehat{A}_1$$

$$A \triangleq \underline{u} = \underline{t} \implies \widehat{A} \triangleq u \sim t \qquad A \triangleq \forall x.A_1 \implies \widehat{A} \triangleq \forall x.\widehat{A}_1$$

$\ldots$

## Theorem ($\mathcal{M}$ satisfies GPC)

*For any formula $A$ in GPF with free variable $x$,*
$\mathcal{M} \models \underline{t} \in \underline{v} \iff \mathcal{M} \models A[\underline{t}/x]$ , *where* $\underline{v} \triangleq \underline{\{x \mid \widehat{A}\}}$.

# Open Questions

- Alternative Inner Models: $\mathcal{M}$ satisfies strong extensionality, but there are inner models which have more than one selfsingleton and hence do not satisfy stong extensionality.
- The ubiquitous hyperuniverse $\mathcal{N}_\omega(\emptyset)$:
  - $\mathcal{N}_\omega(\emptyset)$ is Cantor-1 space;
  - $\mathcal{N}_\omega(\emptyset)$ is the unique solution of the metric equation $X \cong \mathcal{P}_{cl}(X_{\frac{1}{2}})$;
  - $\mathcal{N}_\omega(\emptyset)$ is the space of maximal points of the solution in Plotkin's category of SFP domains of $X \cong \mathcal{P}_P(X_\perp) \oplus_\perp 1$ [Alessi-Baldan-Honsell03]
  - $\mathcal{N}_\omega(\emptyset)$ is the free Stone modal Algebra over 0 generators.
  - Conjecture: $\mathcal{N}_\omega(\emptyset)$ is the extensional quotient of Fitch-Prawitz coalgebra.