

Implementing Cantor's Paradise in Constructive Type Theory

Furio Honsell

[M] uni[cipal|vers]ità di Udine, ITALY

Professor of Automata Theory

Mayor of Udine

President of the European Covenant on Demographic Change

Vice-President of the Italian WHO Healthy Cities Network

former Rector Udine University

Laurea degree under supervision of E.De Giorgi a.a. 1979-1980

`furio.honsell@uniud.it`

**A MATHEMATICAL TRIBUTE TO
ENNIO DE GIORGI**

Scuola Normale Superiore

Pisa, 20 9 2016

Set-theoretic paradoxes have made *comprehensive* and *self-descriptive* Foundational Theories a taboo in the 20th Century. Hilbert claimed in 1925 that: “Aus dem Paradies, das Cantor uns geschaffen hat, soll uns niemand vertreiben können”, but mathematicians have taken since an informal and naive set-theoretic background theory as their working framework. Few daring attempts to breach the taboo were made *e.g.* by W.V.O.Quine and M.Forti, by *restricting the class of formulae* allowed in Cantor’s naive Comprehension Principle, and by E. De Giorgi who advocated for a *cautious, open-ended, and non-reductionist* approach to the Foundations of Mathematics. A different, *intensional* and *proof theoretic* approach to avoid the paradoxes was taken by Fitch, later reformulated by Prawitz. The idea is to *restrict the shape of deductions* allowing only *normal* (or normalizable) deductions. The resulting theory is consistent by design, but quite expressive even if *modus ponens* and Scotus’s principle *ex contradictione quodlibet* fail. We discuss Fitch-Prawitz Set Theory (FP) and implement it in a Logical Framework based on *Constructive Type Theory*, featuring locked types, thereby providing a flexible interactive all-inclusive Mathematical Framework. This is a kind of *Computer-assisted Cantor’s Paradise*. In particular, we prove a Fixed Point Theorem, whereby one can show that all recursive functions are definable in FP. Finally, we provide an intriguing connection between an extension of FP and the *Theory of Hyperuniverses* by Forti and Honsell. Namely we show that the strongly extensional quotient, i.e. the bisimilarity quotient, of the coalgebra of closed terms of Fitch-Prawitz Set Theory satisfies the Generalized Positive Comprehension Principle for Hyperuniverses.

This is joint work M.Lenisa, L.Liquori and I.Scagnetto

De Giorgi's platonism and impredicativism

platonism - ideal objects exist (vs. realism, idealism);

predicativism - no object can be defined in terms of some other notion which *presupposes* its existence;

De Giorgi advocated the **sapiential value** of Mathematics: “umiltà, speranza, convivialità”, e.g.:

- the **axiomatic method**;
- **capitalizing on failures**: incommensurability of the diagonal, Gödel's negative result, etc.

De Giorgi's *Philosophy of Mathematics* was rooted in his *religious attitude*, in his *ethical standpoint*, in his *human rights activism*, and in his *epistemological views*.

Or was it the other way round?

All these are relevant for understanding De Giorgi's interest in the mysterious/awesome nature of **self-description**.

Some truly impredicativistic quotations

- *Operando come matematico ... per poter parlare delle cose conosciute sono costretto a fare riferimento a cose sconosciute* [As a mathematician ... in order to be able to speak on what I know, I need to refer to what I know not]
- *Il carattere misterioso dei fondamenti della matematica* [the mysterious nature of the foundations of mathematics]
- *Mi **limiterò** a notare che in Matematica, anche se ci si vuole **limitare** a procedimenti finitistici, si devono ammettere regole di tipo non finitistico. Per esempio ... per definire l'addizione si è costretti a parlare dell'insieme (infinito) degli interi. In generale la descrizione di certi oggetti può essere fatta solo ammettendo regole assai più complesse degli oggetti da descrivere.*

De Giorgi's legendary prose, manner of speech

- *Delineare le linee fondamentali dei Fondamenti della Matematica* (Outline the fundamental lines [of thought] of the Foundations of Mathematics) - Dissertation topic at the end of the first year of the Perfezionamento programme, 1982;
- “Nella *Nota* espongo nella forma più *chiara e sobria* possibile pochissime idee che *mi sembrano abbastanza* nuove, **abbastanza** interessanti e **abbastanza** *comprensibili, discutibili e criticabili* da parte di ogni persona *che le consideri con una certa attenzione*”

De Giorgi's legendary prose, manner of speech

- *Delineare le linee fondamentali dei Fondamenti della Matematica* (Outline the fundamental lines [of thought] of the Foundations of Mathematics) - Dissertation topic at the end of the first year of the Perfezionamento programme, 1982;
- “Nella *Nota* espongo nella forma più *chiara e sobria* possibile pochissime idee che *mi sembrano abbastanza* nuove, **abbastanza** interessanti e **abbastanza comprensibili, discutibili e criticabili** da parte di ogni persona *che le consideri con una certa attenzione*”
- Le **fronde** ove s'**infronda** tutto l'**orto** de l'**Ortolano** eterno, am'io cotanto quanto da lui a lor di bene è porto.
Par XXVI 64
- Etymological repetitions, internal rhymes, and equivocal rhymes.

- **Anti-reductionism**

There are more things in heaven and earth, Horatio,
than are dreamt of in your philosophy. - Hamlet (1.5.167-8)

- De Giorgi's addition "*vi sono più cose nella mente e nel cuore di ogni uomo di quante lui stesso non immagini*";
- all mathematical objects have the *ontological right* to be taken as *primitive* and not to be reduced to a *set-theoretic encoding*. For this reason the "Ample Theory", of De Giorgi, Forti *et al.*, took into account *qualities, pairs, numbers, relations, operations, collections, sets, functions, propositions, variables, . . .*
- **sofologi vs filosofi** [sophologists vs philosophers];
- **atteggiamento prudentiale** [cautious attitude];
- **teoria aperta** [open-ended theory];
- **semi-formal** approach;
- **axiomatic method**

Universal Declaration of Human Rights

- “*La DUDU del 10 12 1948*”
- **Tolerance, pluralism, human rights, political rights** (freedom of speech);
- These principles informed De Giorgi’s *active citizenship* but also his *epistemology* and *mathematical ontology*, and hence his *methodology*, which was essentially twofold.

De Giorgi advocated a crucial role for applications in inspiring sound mathematical and foundational research.

De Giorgi's **legendary seminars**.

- **Conjectures** Tuesday Seminar, “white-box” approach, *platonism*;
- **Axioms** Wednesday Seminar, “black-box” approach: Marco Forti, F.H., V.M.Tortorelli, M.Clavelli, G.Lenzi, *anti-predicativism*;

L'Autodescrizione [Self-description]

- The inconsistency of Frege's naïve Set Theory: **Extensionality** + **Comprehension**, because of *Russell's Paradox*, triggered the *Foundational Crisis* at the beginning of the XXth Century.

- **Leibniz Equality, Principle of Indiscernibles**

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

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

- The standard solution to this crisis was some form of **predicativism**, thus banning **all circularities**.
- *Aus dem Paradies, das Cantor uns geschaffen hat, soll uns niemand vertreiben können.*
David Hilbert allegedly said in the '20's
- Very few attempts to break the taboo were made. There are two notable attempts obtained by *restricting* the shape of the formula
 - W.V.O. Quine in the '40's introduced **stratified formulæ**
 - Marco Forti in the late '80's introduced *generalized positive formulæ* and **Hyperuniverses**, together with F.H.

- We will discuss another way out originated by Fitch in the '50's; as well as give an answer to the question: **“Who is the murderer?”** in the Russell's case;
- **Circularities**, **reflexivity**, and **non-terminating** objects appear to be dangerous, but are, in fact, ubiquitous;
- De Giorgi did not want to be the subject any **ad hominem** argument, as *type theorists* can be, hence he faced circularities with his sapiential spirit epitomized by the beginning of the biblical book of Proverbs: **Timor Domini principium sapientiæ**.

My Laurea Thesis: Modelli di Teorie degli Insiemi, Principi di Regolarità e di Libera Costruzione, PISA A.A. 1979-1980

*“Poichè non è possibile assumere solo la nozione di insieme a fondamento di una descrizione della nozione di insieme stessa, alcuni autori hanno inquadrato la nozione di insieme in ambiti intuitivi più articolati, mentre altri hanno scelto come intuitive nozioni quali simbolo, linguaggio, ecc. Lo scopo di questa tesi è quello di stabilire una linea naturale di passaggio da una teoria intuitiva degli insiemi ai tipi più sofisticati di teorie formali. Vedremo che questa via è probabilmente insostituibile dato che gli altri tentativi apparentemente più rigorosi, mentre si scontrano con la stessa incapacità di autodescrizione con cui si scontra una teoria intuitiva egli insiemi, **portano ad una comprensione ancora minore della natura sempre misteriosa di questa incapacità.**”*

[The purpose of this thesis is that of establishing a natural pathway from a naïve set theory to the more sophisticated kinds of formal theories. We will see that this pathway is unavoidable since the approaches which might appear more rigorous, while clashing against the same inability in self-describing themselves, **lead to an even lesser understanding of the ever mysterious nature of this very inability.**]

An Analysis of the Description/Formalization Process

- Does **describing** amount to **formalizing**?
- The impossibility of **formalizing the formalization process** itself;
- **formalization is irreducible to formalization**: this is the Primeval Paradox;
- this is the origin of the problematic issue of **adequacy**, and the reason we have to give up **absolute certainty**;
- but **doubt** presupposes **certainty**, much as **hopelessness** has been philosophically viewed as the paramount form of **hope**!

Self-referential and circular situations

- All circularities used to be taken as *vicious circles*;
- This clashed with De Giorgi's anti-reductionist approach.
- “Most italian grammars are in italian!”
- “The collection of all objects I thought of today!”
- Euclid's definition of a **point** as the intersection of two **lines** which are themselves construed as a collection of points.
- The singleton set, of the class of all sets V , clearly satisfies

$$Qqual \quad Qqual \quad V \in \{V\} \in V \quad Coll \in Ins, Coll \in Coll;$$

- the defining power of *equations*, *implicit definitions*, and *Fixed Points*;
- **streams**: Erathostenes Sieve;
- **Semantics of Programming Languages**;
- Web pages are sets of addresses of web pages.

- **Mathematics, Logic, Philosophy, Informatics, Language, Psychology, Ethics, Politics, Art** are replete with circular phenomena and situations.
- The *post-modern* cultural milieu is characterized by the emergence of a range of reflexive discourses, and for the constant interplay between theoretic and metatheoretic levels.
- But, notwithstanding all this, and e.g. Gödel's results and **stored-program computers**, up until **De Giorgi's attention**, little interest was given to the **Mathematical and Logical Foundations** of **circular** and **reflexive** objects.
 - **Free Construction Principles** - M. Forti, F. Honsell. *Set Theory with Free Construction Principles. Ann. Scuola Norm. Sup. Pisa* **10**, (1983);
 - **Hyperuniverses**
 - M. Forti, R. Hinnion. *The consistency problem for positive comprehension principles. J.Symb.Logic* **54**, 1989.
 - M. Forti, F. Honsell. *Models of Self-descriptive Set Theories. Dedicated to Ennio De Giorgi on his sixtieth birthday, Birkhäuser*, 1989.
 - M. Forti, F. Honsell, M. Lenisa. *Processes and Hyperuniverses. MFCS 1994*, Springer LNCS, 1994.
 - M. Forti, F. Honsell. *A General Construction of Hyperuniverses. Theor. Comput. Sci.* **156(1&2)**, 1996.

A Cook's tour of circular phenomena and situations

- **Co-algebras**;
- **Minimal automata, concurrent processes, non-terminating processes**;
- from the catalogue of a recent art exhibition on *analytic painting* "... This results in paintings which are remarkable for the self-referentiality of their language";
- from the catalogue of a recent Cinema Festival "... every citation of a movie is a reflection on Cinema itself, targeted to educated audiences capable of deciphering the *metatheory of Cinema*";
- the **mise en abîme** in paintings and stories; the most remarkable such example being the Mousetrap in Hamlet;
- History and Sociology are **self-referential**, almost by definition, there is no History without Historiography;
- Mythology is often described as the way a culture narrates itself;
- self-awareness: **Know thyself**; the cornerstone of philosophical systems, e.g. **Cogito ergo sum**;

- the *third man paradox* in Plato's Parmenides undermined the Theory of Ideas;
- formal accounts of such notions as **conventions**, **common knowledge**, **intentionality**, **fashion**, and **statistics** usually involve self-reference in an essential way. Many **epistemic logic** paradoxes arise from self referentiality;
- a possible definition of "recursion": see *recursion*;
- a *mind* emerging from a *brain*, which is an invention of the mind;
- Akbar the Moghul emperor, who championed tolerance, secularism, and reason, made the point, in 1590, that *even to dispute reason one has to give a reason for that disputation*;
- a circular assumption of the form: (X) if A , B , C , and X are true then Z is true could stop the infinite regress of Achilles in Carroll's anecdote;
 - (A) Things that are equal to the same are equal to each other.
 - (B) The two sides of this Triangle are things that are equal to the same.
 - (Z) The two sides of this Triangle are equal to each other.
 - (C) If A and B are true, Z must be true.
 - (D) If A and B and C are true, Z must be true.
 - (E) If A and B and C and D are true, Z must be true.

Set-membership can be non-wellfounded

Definition

Let $\mathcal{M} \equiv (M, \in_M)$ be a model of set theory. The membership relation \in_M is **wellfounded** if there is no infinite descending \in_M -sequence. The **model** \mathcal{M} is **wellfounded** if there is no infinite descending \in_M -sequence in M or equivalently

Axiom

Foundation $\forall x \neq \emptyset \exists y \in x. x \cap y = \emptyset.$

- If ZF (Zermelo-Fränkel) Set Theory is consistent, by Gödel's Consistency Theorem, also ZFC (ZF + Axiom of Choice) is consistent. Then by Gödel's Second Incompleteness Theorem, the consistency of ZFC is unprovable in ZFC. Therefore there exists a model of ZFC where there is **no** model of ZFC. But then by Gödel's Completeness Theorem one can derive a **contradiction** from the Axioms of ZFC. The **length** of such a proof, we better hope, be a **non-standard Von Neumann integer** ($n + 1 = \{n\} \cup n$). Membership in that model cannot be wellfounded. Try to picture this!
- If we want all models to be isomorphic to a set with the standard membership. The universe **cannot** be wellfounded.

Axiom

Antifoundation Every **extensional** relation R

$$\forall x, y. (\forall z. zRx \Leftrightarrow zRy) \Rightarrow x = y$$

is isomorphic to the membership relation over a **transitive** set

$$\forall y \in x. y \in x \rightarrow y \subseteq x.$$

The Antifoundation Axiom X_1

Axiom (X_1 - Forti Honsell)

For all $f : A \rightarrow \mathcal{P}(A)$ there exists a unique function $g : A \rightarrow B$ such that $g(x) = \{g(y) \mid y \in f(x)\}$.

The relative consistency of Antifoundation X_1 was proved by Forti and Honsell in 1982. Sets in universes satisfying Antifoundation X_1 are called **hypersets**.

Axiom (X_1)

*Alternately, for every binary relation R there exists a **unique** mapping j onto a transitive set such that $xRy \rightarrow j(x) \in j(y)$.*

The Antifoundation Axiom X_1

Alternately $\forall X, f. f : X \rightarrow \mathcal{P}(X) \exists! g : X \rightarrow V$. such that

$$\begin{array}{ccc} X & \xrightarrow{f} & \mathcal{P}(X) \\ g \downarrow & \swarrow & \\ & & g^+ \\ V & & \end{array}$$

where $g^+ : \mathcal{P}(X) \rightarrow V$ is defined as $g^+(x) = \{g(y) \mid y \in x\}$, i.e.
 $\forall x \in X. g(x) = \{g(y) \mid y \in f(x)\}$.

Axiom (X_1)

Alternately the class of all sets V is a **final** $\mathcal{P}(\)$ -coalgebra.

Strong Extensionality

This latter formulation is related to the fact that Axiom X_1 implies that the universe satisfies a **very strong extensionality property**.

Axiom (Strong Extensionality)

*Two sets x and y are equal if and only if there exists a **bisimulation** R such that xRy .*

The equivalence induced by g on the structure $f : A \rightarrow \mathcal{P}(A)$, namely the \mathcal{P} -coalgebra (A, f) is the **maximal fixed point** of the operator

$(\)^+ : \text{Equiv}_A \rightarrow \text{Equiv}_A$ defined by

$(R)^+ = \{(x, y) \mid (\forall t \in f(x). \exists s \in f(y). tRs) \ \& \ (\forall t \in f(y). \exists s \in f(x). tRs)\}$.

Definition (Bisimulation)

A bisimulation is a relation $R \subseteq V \times V$ such that $R \subseteq (R)^+$, where $R^+ = \{(x, y) \mid (\forall t \in x. \exists s \in y. tRs) \ \& \ (\forall t \in y. \exists s \in x. tRs)\}$

Example

The unique non-wellfounded set \bar{x} which satisfies the equation,

$$x = \{x, \{\emptyset, x\}\}$$

is obtained instantiating X_1 with the set of parameters $\{a, b, c\}$ and defining $f : X \rightarrow \mathcal{P}(X)$, $f(a) = \emptyset$, $f(b) = \{b, c\}$, $f(c) = \{a, b\}$. We have then $\bar{x} = g(b)$.

If e.g.

$$x = \{y, \{\emptyset, x\}\}$$

and

$$y = \{x, \{\emptyset, y\}\}$$

then $x = y$ by strong extensionality.

The extraordinary applications of Strong Extensionality and X_1

- **Non-wellfounded sets** are the seminal example of **co-algebras**;
- *i.e.* **Minimal non-deterministic automaton**, when **membership** is viewed as **transition**.
- establishing euivalence using the maximal fixed point principle, called **Coinduction Principle**, is the fundamental **reasoning tool** for proving correctness of Concurrent Systems w.r.t. specifications,
- The reason is that in Concurrency we deal with **circular objects** and **non-terminating objets**, much more than we do we terminating objects, e.g. **operating systems** or the **internet**.
- Describing objects and characterizing their *behavioural equivalences*, using maximal fixed points via *bisimulations* is at the core of the **formal methods** for reasoning on communicating and mobile systems and circuitry since the late '80's. Currently it is very much in use in **life-critical** software applications.
- To this day the number of publications which generalize and elaborate on the principles underpinning X_1 and Strong Extensionality can be measured only in terms of journals or dedicated conferences.

The **interpretation** function

$$\mathcal{I} : \mathbf{Language} \rightarrow \mathbf{Model}$$

can be seen in two different ways: as a morphism in a **category of algebras**, thus giving rise to what is called **Initial Semantics**, or of **coalgebras**, thus giving rise to **Final Semantics**.

- In Initial Semantics, *Languages* and *Models* are viewed as **F-Algebras**, while in Final Semantics they are viewed as **F-Coalgebras**, for suitable functors F .
- *F-Algebras* are pairs (A, F) such that $f : F(A) \rightarrow A$, e.g. terms of a language given a finite set of constructors, or Natural Numbers, i.e. $1 + N = N$.
- *F-coalgebras* are pairs (A, F) such that $f : A \rightarrow F(A)$, e.g. $Stream = Nat \times Stream$ and the behaviours of processes $Proc = A \times Proc$

- Usually terms of the Language are construed as an **initial** F -algebra (*i.e.* it maps in all F -algebras), whereby \mathcal{I} is the **initial** mapping.
- While behaviours are construed as a **final coalgebra** (*i.e.* all F -coalgebras can be mapped into it), whereby \mathcal{I} is the **final** mapping.
- Initial Semantics is **syntax-oriented** and it induces a **congruence relation**, which can be seen as a **least fixed point**, thereby supporting an **induction principle**: **bottom-up, algebraic, observational, denotational, initial, reductionistic**;
- Final Semantics is **behaviour oriented** and it induces a **bisimilarity relation** which can be seen as a **greatest fixed point** of *bisimulations*, thereby supporting a **coinduction principle**: **top-down, co-algebraic, intentional, operational, behavioural, final, holistic**.
- In initial semantics the **reduction system** parallels the functor F , while in final semantics F arises from a **redtransition system**.
- There is a precise **duality** between Initial and Final Semantics concepts.

Recent Philosophical contributions concerning Foundation and Anti-Foundation

- Yves André *Qu'est-ce que coagir?* (I thank U. Zannier from the Scuola Normale Superiore in Pisa for pointing it out to me) presented at a Seminar held in Paris in 2014 on the Mathematical Ontology of Alain Badiou, the outstanding philosopher, playwright, and militant intellectual.

André illustrates the insights provided by **dualities** in various areas of Mathematics and discusses **co-actions** philosophically¹. He makes the intriguing suggestion of how would Mathematics develop if in high school we would learn to encode functions $f : X \rightarrow Y$, besides by the traditional representation as a *graph*, also by means of its *cograph*. The *cograph* is a *partition* on the disjoint sum $X \uplus Y$, or equivalently, the equivalence relation on $X \uplus Y$ induced by the pairs $(x, f(x))$. In this respect André suggests to think about the *partita doppia* of Luca Pacioli, that is to the *stream* of the double entries of credits and debits. A double entry is a means to make a relation *symmetric* thus enforcing an *invariance check*. He discusses the axioms X_1 mentioned above as “une théorie coactive de la circularité vertueuse”.

¹This is a very inspiring passage: “En reprenant la métaphore théâtrale, on pourrait rapprocher le contexte des processus où opèrent les notions algébriques du théâtre classique, où un petit nombre de protagonistes mène l'action dans un champ spatio-temporel circonscrit. Le contexte où opèrent les notions co-algébriques serait analogue, lui à ces opéras où le protagoniste est un peuple, et où de scène en scène, les changements d'états sont marqués d'intégrales de destins.”

- The **Foundation/Antifoundation divide** plays a significant role in the philosophy of Alain Badiou himself, where *Ontology* is argued to be *Zermelo-Frænkel-Gödel-Cohen Set Theory*.

In *L'être et l'événement*, he asserts that the *event* escapes *Ontology* precisely because ontological concepts are *well-founded sets*, *i.e.* sets founded on \emptyset , which he calls the “pure doctrine of the multiple”. This is also the key point to understand why he purports that *the empty is the proper name of being* and hence that *the one is not*. Badiou maintains that the Foundation Axiom is a “metaontological thesis of Ontology”. On the other hand *events* belong to themselves, or as he puts it, the *matheme* e_x (*i.e.* the mathematical counterpart) of an event of the site X is such that $e_x = X \cup \{e_x\}$. Badiou claims that in grasping an *event* we implicitly have to take into account the event *itself*, through its name, because our very reference to that event is what makes it an event, in a potentially infinite regress. Our modern co-algebraic understanding of non-wellfounded sets is also a possible key to understand the outstanding 19th Meditation in on the poem of Mallarmé *Un coup de dès*: “. . . ou se fût l'événement accompli en vue de tout résultat nul . . .”.

Implementing Cantor's Paradise

Joint work with Lenisa, Liquori, Scagnetto, to appear in **Asian Symp. on Programming Languages and Systems Conference, 2016**

- Cantor's Set Theory with **full Comprehension** ($\{x \mid A(x)\}$) is **inconsistent**. This made Foundational Theories consisting of only Sets almost a taboo. Few exceptions restrict the class of formulæ in the Comprehension Principle: **Quine's NF** and the **Theory of Hyperuniverses** [Forti-Honsell], but preserve **extensionality**.
- An **intensional** and **proof theoretic** approach by F.Fitch '50 reformulated by D.Prawitz '6's0: allow for **full comprehension**, but **restrict** the shape of deductions to **normal(izable) deductions**.
- FP theory is powerful: we prove a **Fixed Point Theorem**, whereby one can show that **all partial recursive functions** are definable.
- We **encode** FP in a **Logical Framework** using **locked types**, thereby providing a *computer assisted proof-development environment*.
- We establish a **connection** between **FP⁺ Hyperuniverses**: the strongly extensional quotient of the coalgebra of closed terms of an extension of FP satisfies the abstraction principle for **Generalized Positive Formulæ**.

The Theory of Fitch-Prawitz (FP)

Terms $t ::= x \mid \lambda x.A$

Formulæ $A ::= \perp \mid \neg A \mid A \wedge A \mid A \vee A \mid A \rightarrow A \mid \forall x.A \mid \exists x.A \mid t \in u$,
where $\neg A$ is an abbreviation for $A \rightarrow \perp$, and $\lambda x.A$ denotes $\{x \mid A\}$.

Some rules (classical version)

$$\wedge I) \frac{A \quad B}{A \wedge B}$$

$$\wedge E) \frac{A \wedge B}{A} \quad \frac{A \wedge B}{B}$$

(A)

\vdots

B

$$\rightarrow I) \frac{}{A \rightarrow B}$$

$$\rightarrow E) \frac{A \quad A \rightarrow B}{B}$$

($\neg A$)

\vdots

\perp

$$\perp) \frac{}{A}$$

$$\forall I) \frac{A[y/x]}{\forall x.A}$$

$$\forall E) \frac{\forall x.A}{A[t/x]}$$

$$\lambda I) \frac{A[t/x]}{t \in \lambda x.A}$$

$$\lambda E) \frac{t \in \lambda x.A}{A[t/x]}$$

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 \perp -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 simplistically deductions which do not derive \perp would lead to complications, because subdeductions with conclusion \perp are necessary to deal with negation. Normal form can be checked **locally**

Theorem

Normal proofs cannot derive \perp , hence FP is consistent.

There is no introduction rule for \perp , but the shape of normal proofs is such that in each branch the elimination rules precede the introduction rules. So there cannot be a normal proof of namely \perp .

- 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. And Aristotle's **non-contradiction** principle fails: $\vdash_{\text{FP}} A \wedge \neg A$. Thus FP is **paraconsistent**.
- Since \perp is not derivable, FP is **non-trivial**.

The taming of Russell's Paradox

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

$$\begin{array}{c}
 \frac{t \in t^{(1)}}{t \notin t} \quad \frac{t \in t^{(1)}}{t \in t^{(1)}} \quad \frac{t \in t^{(1)}}{t \notin t} \quad \frac{t \in t^{(1)}}{t \in t^{(1)}} \\
 \frac{\perp}{t \notin t} \quad \frac{\perp}{t \in t^{(1)}} \\
 \frac{t \notin t}{t \in t} \quad \frac{\perp}{t \notin t} \\
 \hline
 \perp
 \end{array}$$

- $\vdash_{\text{FP}} (t \in t) \wedge (t \notin t)$ (failure of Aristotle's **Principle of non-contradiction**).
- But $\not\vdash_{\text{FP}} \perp$ because the proof is not normal.
- The structural rule of **Contraction** is used.
- Naïve Set Theory without contraction is consistent [Grishin82]. This would amount to Set Theory with Girard's Linear Logic without exponentials. *LLS* is a slightly stronger theory, with a *modal control* of contraction.
- **Minimal logic** is already inconsistent because of contraction. So the “murderer” in Frege's case is neither **lack of stratification**, nor **negation**, but rather **contraction**, and we will see also **extensionality**

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

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

- $\vdash_{\text{FP}} t_1 \simeq t_2 \rightarrow t_1 = t_2 .$
- The converse implication amounts to the **Extensionality Axiom** $t_1 = t_2 \rightarrow t_1 \simeq t_2 .$
- [Grishin82]: adding the **Extensionality Axiom, Contraction Rule** is admissible, hence the theory becomes inconsistent.
- $\text{FP} + \text{Ext} \vdash_{\text{FP}} \perp .$

Let $Y \triangleq \{x \mid x \in x\}$, $\emptyset \triangleq \{x \mid \perp\}$, $R \triangleq \{x \mid x \in x \rightarrow \perp\}$,
 $X \triangleq \{x \mid R \in R\}$. Then $R \in R \vdash_{\text{FP}} \forall x. x \in \emptyset \leftrightarrow x \in X$. Namely,

$$\frac{R \in R \quad \frac{\frac{x \in X^{(1)}}{R \in R}}{R \in R \rightarrow \perp}}{\perp}}{x \in \emptyset}}{x \in X \rightarrow x \in \emptyset}$$

$$\frac{x \in \emptyset^{(1)} \quad R \in R^{(2)}}{\perp}}{\frac{R \in R \rightarrow \perp}}{R \in R}}{x \in X}}{x \in \emptyset \rightarrow x \in X}$$

Using *Ext*, we have $R \in R \vdash_{\text{FP}} \forall x. \emptyset \in x \leftrightarrow X \in x$. By instantiating x to Y we get $R \in R \vdash_{\text{FP}} \emptyset \in Y \leftrightarrow X \in Y$, hence using λE), we obtain $R \in R \vdash_{\text{FP}} \emptyset \in \emptyset \leftrightarrow X \in X$. Since, by λI) $R \in R \vdash_{\text{FP}} X \in X$, by $\rightarrow E$) we get $R \in R \vdash_{\text{FP}} \emptyset \in \emptyset$ and by λE) $R \in R \vdash_{\text{FP}} \perp$. Finally, since $\vdash_{\text{FP}} R \in R$ (see Russell's Paradox) we get a contradiction. All the above arguments are indeed normal deductions. \square

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

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

Proof. Let $u \triangleq \{\vec{z} \mid \langle \vec{z}, t \rangle \in t\}$, where $t \triangleq \{\langle \vec{z}, y \rangle \mid A[\{\vec{w} \mid \langle \vec{w}, y \rangle \in y\}/x]\}$. Then the implication $\vec{z} \in u \longrightarrow A[u/x]$ and its converse can be derived via two applications, respectively, of the λE -rule, and of the λI -rule. □

Consider two fixed conventional sets/terms, which we denote by 0 and S , to represent zero and successor. *E.g.* take \emptyset and V . Then apply *FPT* to the formula A_{Nat} :

$$A_{\text{Nat}}[z, x] \stackrel{\Delta}{=} (\forall A. (0 \in A \wedge \forall y \in A. \langle S, y \rangle \in A)) \longrightarrow z \in A \longrightarrow z \in x.$$

By *FPT* there exists a term Nat such that

$$\vdash_{\text{FP}} z \in \text{Nat} \longleftrightarrow A_{\text{Nat}}[z, \text{Nat}].$$

Subtraction

Consider the following formula: $A_{\text{Subt}}[\vec{z}, x] \triangleq (\forall A.$

$$\forall y_1, y_2, y_3 \in \text{Nat.} \left\{ \begin{array}{l} \langle \langle 0, y_2 \rangle, 0 \rangle \in A \wedge \\ \langle \langle y_1, 0 \rangle, y_1 \rangle \in A \wedge \\ \langle \langle y_1, y_2 \rangle, y_3 \rangle \in A \rightarrow \langle \langle y_1 + 1, y_2 + 1 \rangle, y_3 \rangle \in A \end{array} \right\} \\ \rightarrow \vec{z} \in A) \\ \rightarrow \vec{z} \in x.$$

Then, by the *FPT*, there exists a term `Subt` such that $\vdash_{\text{FP}} \langle \langle z_1, z_2 \rangle, z_3 \rangle \in \text{Subt} \longleftrightarrow A_{\text{Subt}}[\vec{z}, \text{Subt}]$.

FP is a **universal model of computation**.

FP in Constructive 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 $\mathcal{L}_{N,\sigma}^{\mathcal{P}}[M]$ of type $\mathcal{L}_{N,\sigma}^{\mathcal{P}}[\rho]$. Locks allow to factor out specific constraints.

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

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

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

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.

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 $LLF_{\mathcal{P}}$

The signature is the following:

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

where:

- o is the type of propositions,
- \supset and the “membership” predicate ϵ are the syntactic constructors for propositions,
- lam is the “abstraction” operator for building “sets”,
- T is the apodictic judgement,
- V is the generic judgement,
- δ is the coercion function,
- $\langle x, y \rangle$ denotes the encoding of pairs.

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

$$\supset_{\text{elim}} : \prod A, B : o . \prod x : T(A) . \prod y : T(A \supset B) \rightarrow \mathcal{L}_{\langle x, y \rangle, T(A) \times T(A \supset B)}^{\text{Fitch}} [T(B)]$$

the predicate $\text{Fitch}(\Gamma \vdash_{\Sigma_{\text{FPST}}} \langle x, y \rangle \Leftarrow T(A) \times T(A \supset B))$ holds iff: x and y have **skeletons** in $\Lambda_{\Sigma_{\text{FPST}}}$, 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 δ , and hence have type $V(A)$,

and, moreover, the proof derived by combining the skeletons of x and y is **normalizable** in the natural sense.

Theorem (Adequacy for Fitch-Prawitz Set Theory)

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

The Theory of Hyperuniverses TH

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

Forti's Principle: 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 $\forall x.(x \in y \rightarrow A)$ ($\exists x.(x \in y \rightarrow A)$);
- closed under the formula $\forall x.(B \rightarrow A)$, where A is a generalized positive formula and B is any formula such that $Fv(B) \subseteq \{x\}$. 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}(\)$:

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

- 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** $f_{\mathcal{T}^0} : \mathcal{T}^0 \rightarrow \mathcal{P}(\mathcal{T}^0)$

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

- **Bisimilarity** can be defined in FP:

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

where $A_{\text{Bis}} \triangleq \forall t, t' (\langle t, t' \rangle \in x \rightarrow$
 $\forall u (u \in t \rightarrow \exists u' (u' \in t' \wedge \langle u, u' \rangle \in x)) \wedge$
 $\forall u' (u' \in t' \rightarrow \exists u. (u \in t \wedge \langle u, u' \rangle \in x))) .$

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

$$\underline{t} \triangleq \{t' \mid \vdash_{\text{FP}} t \sim t'\} .$$

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

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

$$\begin{array}{ccc} \mathcal{T}^0 & \xrightarrow{f_{\mathcal{T}^0}} & \mathcal{P}(\mathcal{T}^0) \\ \pi \downarrow & & \downarrow \mathcal{P}(\pi) \\ \mathcal{M} & \xrightarrow{f_{\mathcal{M}}} & \mathcal{P}(\mathcal{M}) \end{array}$$

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

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

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

Theorem

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 **Forti's Principle**, i.e. the Generalized Positive Comprehension Scheme, namely it is a **hyperuniverse**.

Definition

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

$$\begin{aligned} A \triangleq \underline{u} \in \underline{t} &\implies \hat{A} \triangleq \exists u'. u' \sim u \wedge u' \in t & A \triangleq \neg A_1 &\implies \hat{A} \triangleq \neg \hat{A}_1 \\ A \triangleq \underline{u} = \underline{t} &\implies \hat{A} \triangleq u \sim t & A \triangleq \forall x. A_1 &\implies \hat{A} \triangleq \forall x. \hat{A}_1 \\ \dots & & & \end{aligned}$$

Theorem (\mathcal{M} satisfies GPC)

For any formula A in GPF with free variable x ,

$$\mathcal{M} \models \underline{t} \in \underline{v} \iff \mathcal{M} \models A[\underline{t}/x], \text{ where } \underline{v} \triangleq \underline{\{x \mid \hat{A}\}}.$$

Using FP as a Logical Framework

- FP is a Computer-assisted Cantor's Paradise: interactive and, unlike Coq and Agda, closer to the familiar informal way of **conjecturing** in Mathematics and **delaying and consolidating** tests.
- FP is essentially Naïve Set-Theory, probably the most natural and straightforward Logical Framework.
- **Pragmatically**, FP allows **fast and loose formal reasoning** on general recursion and datatypes;
- **Foundationally**, FP allows for a fine-tuned analysis of paradoxes arising from diagonal arguments.
- The formal methods community (e.g. in program transformation and program synthesis in non-terminating functional languages and general recursion) is interested in logical systems supporting convenient and fast, even if logically unsound or invalid, features and heuristics. Justification is postponed once there is a good reason for going through the daunting overhead of checking all the preconditions.
- The principled but cautious, approach of Coq and Agda is akin to **pessimistic concurrency**, *i.e.* assuming shared resources are contended and hence have to be proactively protected with locks.
- FP corresponds to **optimistic concurrency**, *i.e.* proceed as if no contention, check for consistency when transaction ends.

- Using FP as a Logical Framework goes precisely in the direction of **optimistic reasoning**: Lock types allow for postponing and for aggregating and simplifying checks, so that they can be done possibly at some other level, rather than delegated to the metalanguage as in Coq or Agda.
- Are **Paraconsistent systems** useful. De Bruijn provocatively asked: do we really need a terminating metalanguage?
Of course if we use Scotus rule, then our reasoning is empty. But otherwise we still have plenty of useful arguments to carry out which can make visible truly false or missing requirements. So, even paraconsistent systems can increase our confidence in the outcome. Absolute certainty cannot be ever achieved.

- Which statements have a **paraconsistent cognate**? All arising from diagonal arguments?
- FP is a **conservative extension** of FOL, small sets or, GPF. Are there larger classes of sentences, e.g. in **foundations of Category Theory**?
- **Alternate Inner Models**: \mathcal{M} satisfies strong extensionality, but there are inner models which have more than one **selfsingleton** and hence do not satisfy strong 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.
 - $\mathcal{N}_\omega(\emptyset)$ is the **extensional quotient** of **Fitch-Prawitz coalgebra**.