A short presentation of Dedukti and some questions to address

Gilles Dowek

The revolution of Predicate logic

Since Euclid: geometry, arithmetic, set theory... each system its syntax, its notion of proof...

Hilbert and Ackermann (1928): a common framework Predicate logic for geometry, arithmetic, set theory...

Sharing connectives, deduction rules...

A theory: symbols and axioms

Which axiom is used in which proof?

But a short revolution

At that time another theory: Type theory (*Principia Mathematica*)
No expression in Predicate logic

Soon (1940) Church: a new formulation of Type theory (based on λ-calculus) impossible to express in Predicate logic (λ binds)

1970, 1985... Martin-Löf's type theory, the Calculus of constructions... Type theory with predicate subtyping not in Predicate logic

Three attitudes

- Consider logical framework as a dead concept
- Express Russell's type theory, Church's, Martin-Löf's, the Calculus of constructions... in Predicate logic by will of by force (Henkin, Davis, D...)
- Transform Predicate logic to a better logical framework

The limits of Predicate logic

- No bound variables ($\lambda x\ x$)
- No syntax for proofs
- No notion of computation
- No good notion of proof reduction
- Classical and not constructive

New logical frameworks

- No bound variables ($\lambda x\ x$): λ-Prolog, Isabelle, $\lambda\Pi$-calculus
- No syntax for proofs: $\lambda\Pi$-calculus
- No notion of computation: Deduction modulo theory
- No good notion of proof reduction: Deduction modulo theory
- Classical and not constructive: Ecumenical logic

The $\lambda\Pi$-calculus modulo theory that generalizes them all

Dedukti: an implementation of it

Examples of axioms in Dedukti

Terms and propositions

Weak framework: terms and propositions are not primitive but need to be built

$I : TYPE$
$0 : I$
$S : I \to I$
Many-sorted?

$Prop : TYPE$
$= : I \to I \to Prop$
$\Rightarrow : Prop \to Prop \to Prop$
$\forall : (I \to Prop) \to Prop$

Proofs

Proofs are trees, they can be expressed in DEDUKTI

Curry-de Bruijn-Howard: $P \Rightarrow P$ should be the type of its proofs

But not possible here $P \Rightarrow P : \mathit{Prop} : \mathit{TYPE}$ is not itself a type

$\mathit{Prf} : \mathit{Prop} \rightarrow \mathit{TYPE}$
mapping each proposition to the type of its proofs
$\mathit{Prf}\,(P \Rightarrow P) : \mathit{TYPE}$

Proofs

Brouwer-Heyting-Kolmogorov: $\lambda x : (Prf\, P)\ x$ should be a proof of $P \Rightarrow P$ but it has type $(Prf\, P) \rightarrow (Prf\, P)$

$Prf\,(P \Rightarrow P)$ and $(Prf\, P) \rightarrow (Prf\, P)$ must be identified

A reduction rule

$$Prf\,(P \Rightarrow P) \longrightarrow (Prf\, P) \rightarrow (Prf\, P)$$

This reduction rule is the Curry-de Bruijn-Howard correspondence

Connectives

Ecumenical: constructive and classical disjunction are governed by different rules: the are different symbols (like inclusive and exclusive disjunction): $\vee$ and $\vee_c$

$\top$, $\bot$, $\neg$, $\wedge$, $\vee$, $\exists$ defined *à la* Russell

$\Rightarrow_c$, $\wedge_c$, $\vee_c$, $\forall_c$, $\exists_c$ defined using negative translation as a definition

Do we need classical connectives in B proofs?

More axioms

Propositions as objects, functions (as in HOL Light...)

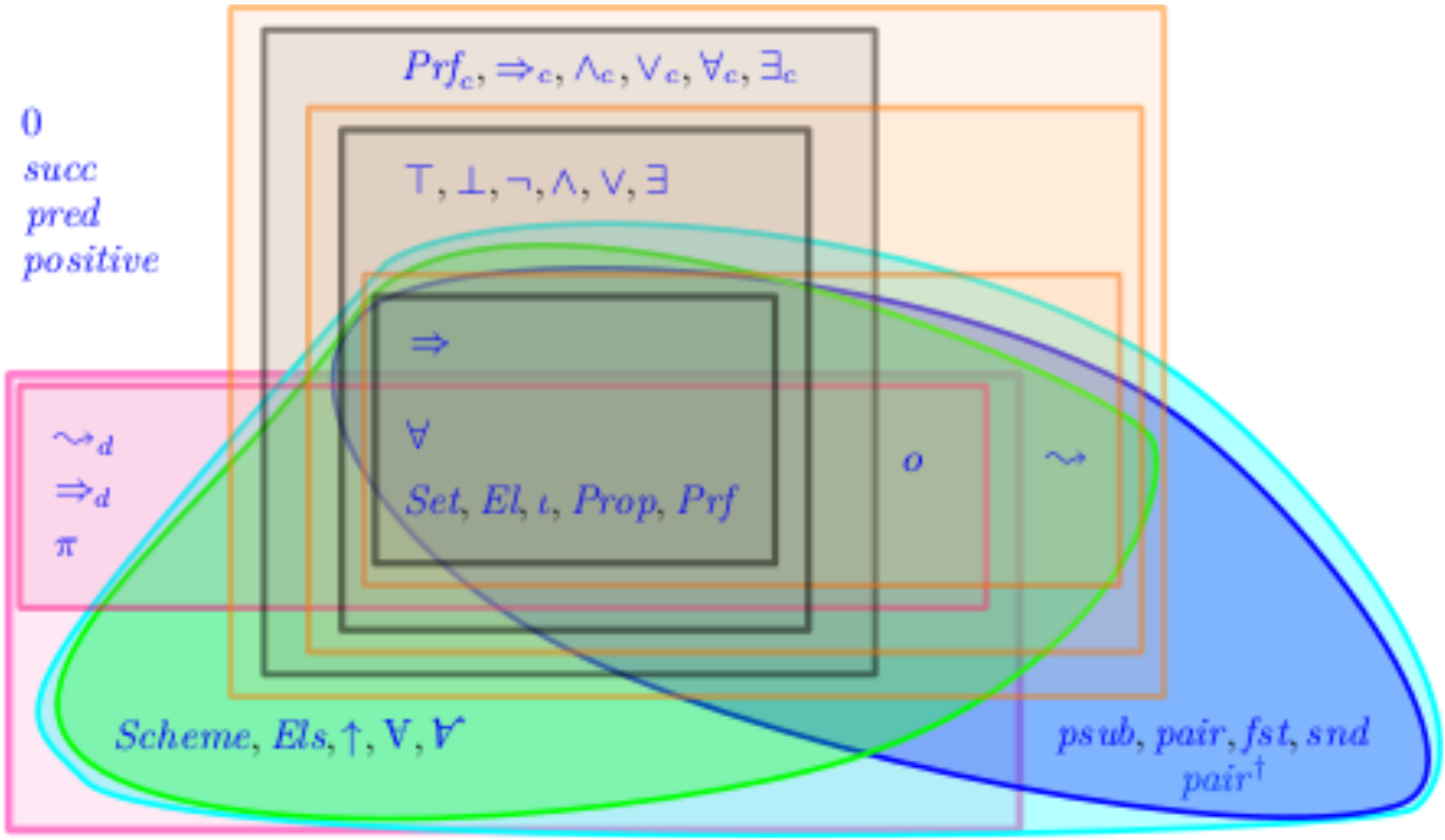
Dependency (as in Coq...)

Object-level predicative polymorphism (as in HOL Light...)

Predicate subtyping (as in PVS)

Infinity

Some axioms and some theories



(with Blanqui, Grienenberger, Hondet, Thiré...)
And more: universes, universe polymorphism (Assaf, Férey, Genestier...)

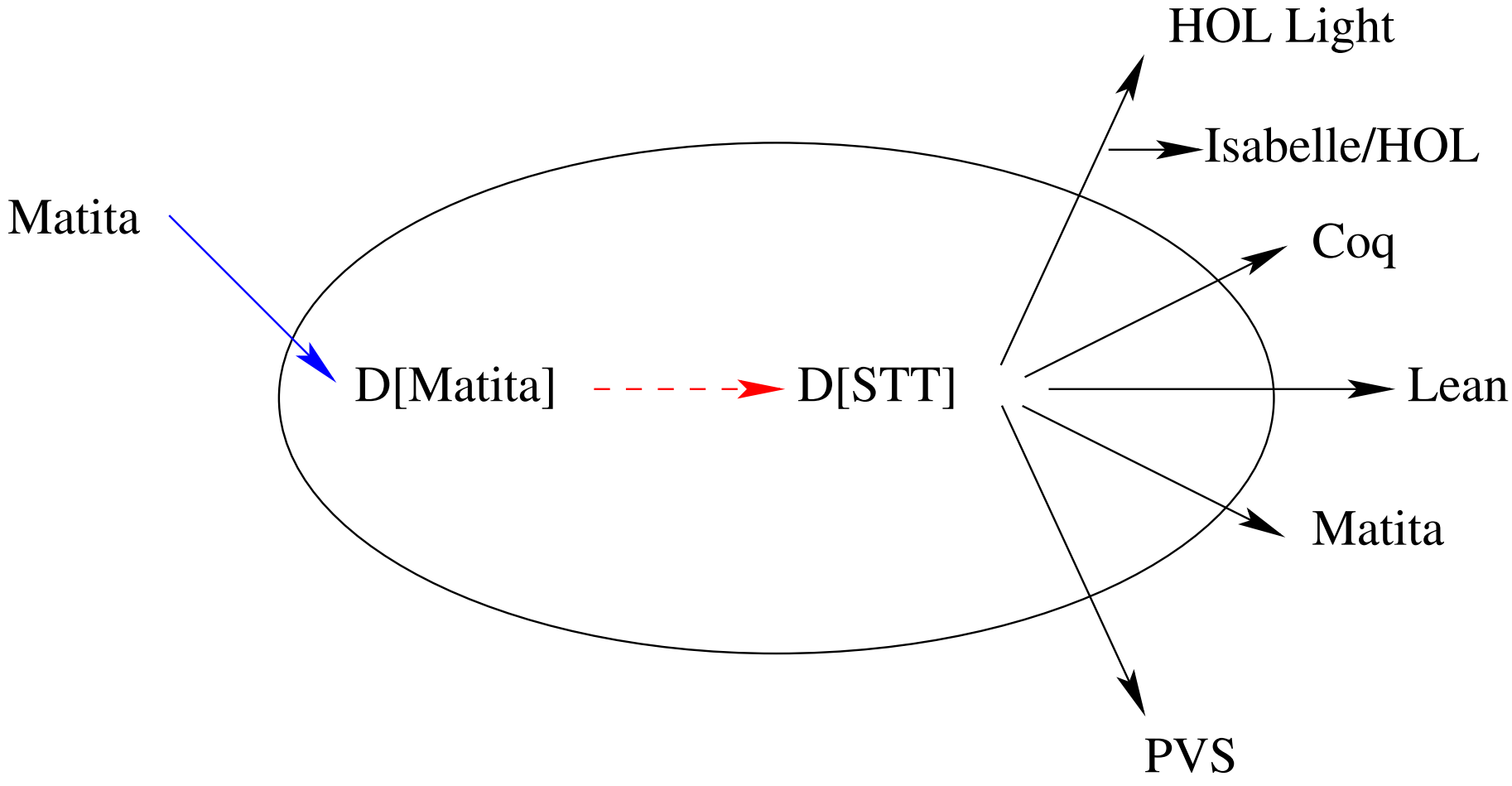
Reverse mathematics in Dedukti

The Calculus of constructions: 12 axioms
Simple type theory: a subset formed with 9 axioms

- All proofs in Simple type theory can be translated to the Calculus of constructions
- The proofs in the Calculus of constructions that do not use these three axioms can be translated to Simple type theory (not the others: genuine Calculus of constructions proofs)

For example (Thiré): all the proofs of the arithmetic library of Matita

"First" proof of Fermat's little theorem in constructive Simple type theory



The proof of Fermat's little theorem cross-checked in seven systems. Higher confidence in its correctness

What about set theory? (B, TLA...)

Set theory: can be expressed with axioms, such as

$$\forall x \exists y \forall z \ (z \in y \Leftrightarrow \forall w \ (w \in z \Rightarrow w \in x))$$

Skolemized

$$\forall x \forall z \ (z \in \mathcal{P}(x) \Leftrightarrow \forall w \ (w \in z \Rightarrow w \in x))$$

Should we transform it into a reduction rule

$$z \in \mathcal{P}(x) \longrightarrow \forall w \ (w \in z \Rightarrow w \in x)$$

?

If not each time π is a proof of $z \in \mathcal{P}(x)$, $(F \ \pi)$ a proof of $\forall w \ (w \in z \Rightarrow w \in x))$

But not a "nice" reduction system

if $C = \{w \in x \mid \neg w \in w\}$ (Crabbé's set)

$$z \in C \longrightarrow z \in x \wedge \neg z \in z$$

in particular

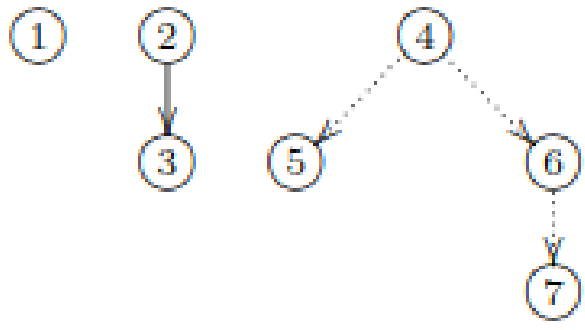
$$C \in C \longrightarrow C \in x \wedge \neg C \in C$$

Non terminating
Moreover the proof of $\neg C \in x$ non terminating either

An alternative

Proposed by several persons including Miquel

A notion of graph more primitive that that of set
$\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}$



Developed in Deduction modulo theory (in 2007) and in Dedukti (2021) (with Traversié and Blot)

Three options and need for empirical study needed

Interoperability sustainability, and cross checking

Interoperability

Between B and TLA+

And also with type theories (arithmetic libraries)

Cross-checking

Allow oneself insecure proofs (SMT solvers...) and use DEDUKTI to recheck proofs