Master's thesis - final talk:

Tableaux for Higher-Order Logic with If-Then-Else, Description and Choice

by Julian Backes on April 9, 2010

Advisor: Dr. Chad E. Brown

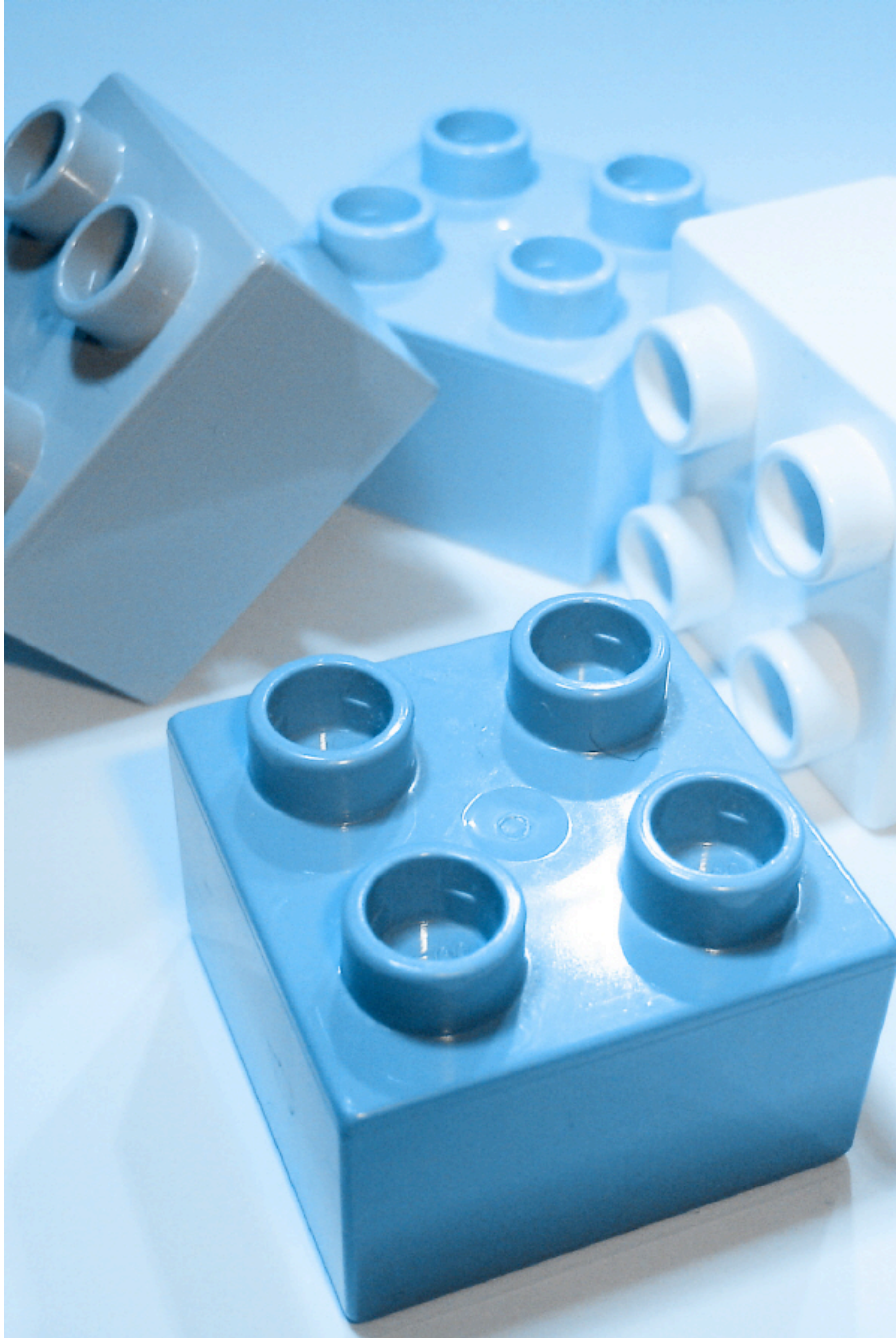
Supervisor: Prof. Dr. Gert Smolka

Thank you!

Contents

Introduction & Basics

Syntax & Semantics



Three Papers

- Three papers about fragments of simply typed higher order logic by Brown and Smolka:
  - "Extended First-Order Logic":
    No higher-order equations, quantifiers at base types; proof system cut-free and complete wrt standard models
  - "Complete Cut-Free Tableaux for Equational Simple Type Theory":
    Full higher-order logic, proof system cut-free and complete wrt general models
  - "Analytic Tableaux for Simple Type Theory and its First-Order Fragment":
    Essentially combines the two papers from above
- Goal of my thesis: Extend these fragments with more powerful logical constants while maintaining the existing properties (completeness, cut-freeness)

Syntax

- Context: Simply typed higher order logic
- Types (σ, τ, μ): $\iota \mid o \mid \sigma\ \tau$
- Logical Constants *LC* = $\{\neg, \vee, \exists_\tau, =_\tau, \top, \bot, if_\tau, \varepsilon_\tau, \iota_\tau\}$
- Signature *S* is a subset of *LC*
  - "Fragments" can be seen as signatures
- *S*-terms (*s, t, u, v, w*): $x \mid c\ (\in S) \mid st \mid \lambda x.t$
- Typed *S*-terms as usual, we only consider well-typed *S*-terms
- Λ_σ^S denotes the set of all *S*-terms of type σ

Frames

- A frame D is a function mapping types to nonempty sets such that
  - $D(o) \subseteq \{0, 1\}$ (true/false)
  - $D(\sigma\tau) \subseteq D(\sigma) \to D(\tau)$
- A standard frame D is a frame such that
  - $D(o) = \{0, 1\}$
  - $D(\sigma\tau) = D(\sigma) \to D(\tau)$
- What is a (standard) S-frame?

7

Logical Constants and Frames

- For each logical constant *c*, there is a property P_c that must hold for a function *f* represented by *c*

- Examples:

$$P_\neg(f) = (f1 = 0 \wedge f0 = 1)$$

$$P_{\varepsilon_\sigma}(f) = \forall g \in D(\sigma o).\ (\exists a \in D\sigma.\ ga) \rightarrow g(fg)$$

- A frame realizes a logical constant *c* iff there is some *f* in *D* such that $P_c(f)$ is true

- An *S*-frame is a frame that realizes all logical constants in *S*
  - A standard frame is trivially an *S*-frame for all *S*

- *S*-Interpretations (into *S*-frames) / satisfiability / validity as usual

8

A New Goal

- Given the definition of a signature, we decided to work towards an additional goal for my thesis:
  - "Give me any signature you want and I give you back a complete tableau system. I will also tell you whether this tableau system is complete with respect to standard models"

A Signature Dependent Tableau System

Give me any signature you want...

10

Signatures and Quasiformulas

- Goal: A modular, signature dependent tableau system
- Problem: Disequations will be the "internal workhorses" of the system; should we require ¬ and $=_\tau$ to be always in the signature?
  - No! $=_\tau$ is a very powerful logical constant and we will not be able to get completeness wrt. standard models
- Solution: Introduce quasiformulas
  - Every S-formula is a quasi-S-formula
  - If s is an S-formula then $\neg s$ is an quasi-S-formula
  - If s and t are S-terms of the same type then $s \neq t$ is a quasi-S-formula

Tableau rules

- Tableau rules:

$$\frac{A}{A_1 \quad | \quad \ldots \quad | \quad A_n}\; A \subsetneq A_i \qquad\qquad \textsc{Closed}\ \frac{A}{}$$

- For simplicity: We only write what is needed in *A* to apply a rule and what is added in the A_i

- All *A* and A_i must only contain quasi-*S*-formulas

- Requirement: The tableau system should depend on the signature but not vice versa
  - This means that a tableau rule must not introduce new logical constants (where "new" is relative to the premise)

12

The Basic Tableau System

- For the empty signature, we have four rules to handle quasiformulas:

$$\text{FE}\ \frac{s \neq_{\sigma\tau} t}{[sx] \neq_{\tau} [tx]}\ x \text{ fresh} \qquad\qquad \text{BE}\ \frac{s \neq_{o} t}{s,\ \neg t \mid \neg s,\ t}$$

$$\textsc{Dec}\ \frac{xs_1 \dots s_n \neq_{\iota} xt_1 \dots t_n}{s_1 \neq t_1 \mid \dots \mid s_n \neq t_n}\ n \geq 0$$

$$\textsc{Mat}\ \frac{xs_1 \dots s_n,\ \neg xt_1 \dots t_n}{s_1 \neq t_1 \mid \dots \mid s_n \neq t_n}\ n \geq 0$$

Usual Logical Constants

- The rules for the usual logical constants are not new:

$$\textsc{Bot}\ \frac{\bot}{} \qquad \textsc{Top}\ \frac{\neg\top}{} \qquad \textsc{Or}\ \frac{s \vee t}{s \mid t} \qquad \textsc{OrN}\ \frac{\neg(s \vee t)}{\neg s,\ \neg t} \qquad \text{DN}\ \frac{\neg\neg s}{s}$$

$$\textsc{Ex}\ \frac{\exists s}{[sx]}\ x \text{ fresh} \qquad \textsc{ExN}\ \frac{\neg(\exists s)}{[st]}\ t \in \Lambda^S \text{ normal}$$

$$\text{BQ}\ \frac{s =_{\tau_1 \ldots \tau_n o} t}{[su_1 \ldots u_n],\ [tu_1 \ldots u_n] \mid \neg[su_1 \ldots u_n],\ \neg[tu_1 \ldots u_n]}\ \begin{array}{l} n \geq 0, \\ u_i \in \Lambda^S_{\tau_i} \text{ normal} \end{array}$$

$$\textsc{Con}\ \frac{s =_{\tau_1 \ldots \tau_n \iota} t,\ u \neq_\iota v}{[sw_1 \ldots w_n] \neq_\iota u,\ [tw_1 \ldots w_n] \neq_\iota u \mid [sw_1 \ldots w_n] \neq_\iota v,\ [tw_1 \ldots w_n] \neq_\iota v}\ \begin{array}{l} n \geq 0, \\ w_i \in \Lambda^S_{\tau_i} \text{ normal} \end{array}$$

Towards the New Logical Constants

- Def: Let *E* be a branch. A term $s{:}\iota$ is discriminating in *E* if and only if there is a term *t* such that $(s \neq_\iota t) \in E$ or $(t \neq_\iota s) \in E$

- Def: Let *E* be a branch. A term s is accessible in *E* if and only if there is a context $C = [\,]\ t_1 \ldots t_n$ such that
  - $C[s]$ is discriminating in *E* for $C[s]$ of type ι or
  - $C[s] \in E$ or $\neg C[s] \in E$ for $C[s]$ of type o

- We call *C* an accessibility context

- Examples: Is "ε *s*" accessible?
  - Not accessible: $s\ (\varepsilon\ s)$
  - Accessible: $v \neq_\iota \varepsilon\ s\ t\ u$; accessibility context: $v \neq_\iota [\,]\ t\ u$

If-Then-Else

- The interesting fact about if-then-else is that it does not necessarily return something of type o (*if*$_\iota$:oιιι returns something of type ι)

- Consequence: *if* does not always occur as the "head" of a formula

$$\text{IFL}\ \frac{(\text{if}_\sigma stu)v_1 \dots v_n \neq_\iota v'}{s,\ [tv_1 \dots v_n] \neq_\iota v' \mid \neg s,\ [uv_1 \dots v_n] \neq_\iota v'}\ n \geq 0$$

$$\text{IFR}\ \frac{v' \neq_\iota (\text{if}_\sigma stu)v_1 \dots v_n}{s,\ [tv_1 \dots v_n] \neq_\iota v' \mid \neg s,\ [uv_1 \dots v_n] \neq_\iota v'}\ n \geq 0$$

$$\text{IF}\ \frac{C[\text{if}_\sigma stu]}{s,\ [C[t]] \mid \neg s,\ [C[u]]}\ C \text{ accessibility context}$$

$$\text{IFB}\ \frac{(\text{if}_\sigma stu)v_1 \dots v_n}{s,\ [tv_1 \dots v_n] \mid \neg s,\ [uv_1 \dots v_n]}\ n \geq 0$$

$$\text{IFBN}\ \frac{\neg((\text{if}_\sigma stu)v_1 \dots v_n)}{s,\ \neg[tv_1 \dots v_n] \mid \neg s,\ \neg[uv_1 \dots v_n]}\ n \geq 0$$

16

Choice and Description

- The rules for choice are based on a paper by Mints

$$\textsc{Mat}_\varepsilon\ \frac{\varepsilon s_1 \dots s_n,\ \neg\varepsilon t_1 \dots t_n}{s_1 \neq t_1 \mid \dots \mid s_n \neq t_n} \qquad \textsc{Dec}_\varepsilon\ \frac{\varepsilon s_1 \dots s_n \neq_\iota \varepsilon t_1 \dots t_n}{s_1 \neq t_1 \mid \dots \mid s_n \neq t_n}$$

$$\textsc{Choice}\ \frac{C[\varepsilon s]}{\neg[st] \mid [s(\varepsilon s)]}\ \ \begin{array}{l} C \text{ accessibility context,} \\ t \in \Lambda^S_\sigma \text{ normal} \end{array}$$

- The rules for description look similar

$$\textsc{Mat}_\iota\ \frac{\iota s_1 \dots s_n,\ \neg\iota t_1 \dots t_n}{s_1 \neq t_1 \mid \dots \mid s_n \neq t_n} \qquad \textsc{Dec}_\iota\ \frac{\iota s_1 \dots s_n \neq_\iota \iota t_1 \dots t_n}{s_1 \neq t_1 \mid \dots \mid s_n \neq t_n}$$

$$\textsc{Desc}\ \frac{C[\iota s]}{\neg[st] \mid x \neq y,\ [sx],\ [sy] \mid [s(\iota s)]}\ \ \begin{array}{l} C \text{ accessibility context,} \\ t \in \Lambda^S_\sigma \text{ normal, x, y fresh} \end{array}$$

Generic Completeness Result

A proof sketch

18

Completeness Proof

- I will not explain the whole completeness proof here :-)
- The hard part reduces to the Model Existence Theorem:
  - Def: A set *E* of formulas (representing a branch) is called evident if it is not closed and no tableau rule applies
  - Model Existence Theorem: If a set *E* is evident, then there exists an interpretation which satifies all formulas in *E*
- We need to construct an *S*-frame *D* and an *S*-interpretation into *D*

19

Possible Values

- Given an evident set E, define possible values relation by induction on types:
  - $s \triangleright_o 0$:<=> $[s] \notin E$
  - $s \triangleright_o 1$:<=> $\neg[s] \notin E$
  - $s \triangleright_{\sigma\tau} f$:<=> $st \triangleright_\tau fa$ whenever $t \triangleright_\sigma a$
  - (We skip $\triangleright_\iota$ here, it is defined using discriminants)
- $D(\sigma)$ is defined as $\mathrm{Ran}(\triangleright_\sigma)$, i.e., D may be a nonstandard frame
- We need to show that D is an S-frame
  - For all $c \in S$ we need to find some f such that $c \triangleright f$ and $P_c(f)$ holds
  - This is straightforward for all usual logical constants including *if* since the *f* are unique and should be clear (equality function for = etc.)
  - For $c \in \{\varepsilon, \iota\}$, the *f* is not unique so we have to define it...

20

Interpretations for ε and ι

- The interpretation for ε is also based on the work by Mints
- We define a function $\Phi \in D(\sigma o) \to D(\sigma)$ such that
  - $\Phi\ f$ = some b such that $f\ b = 1$ if f^ε is empty and such a b exists
  - $\Phi\ f$ = some a such that $f^\varepsilon \triangleright a$ otherwise
- $f^\varepsilon = \{\varepsilon s \mid s \triangleright f \text{ and } \varepsilon s \text{ is accessible}\}$
  - In the second case, there is always a common possible value for f^ε, i.e., for each element in f^ε, even if it is empty (proof uses Mat_ε and Dec_ε)
- Lemma 1: $\varepsilon \triangleright \Phi$
- Lemma 2: Φ is a choice function (proof uses Choice)

Interpretations for **ε** and **ι** ctd.

- For description, everything will look familiar
- We define a function $\psi \in D(\sigma o) \to D(\sigma)$ such that
  - $\psi\ f$ = some b such that $f\ b = 1$ if f^ι is empty and such a b exists and is unique
  - $\psi\ f$ = some a such that $f^\iota \triangleright a$ otherwise
- $f^\iota = \{\iota s \mid s \triangleright f$ and ιs is accessible$\}$
  - In the second case, there is always a common possible value for f^ι, i.e., for each element in f^ι, even if it is empty (proof uses Mat_ι and Dec_ι)
- Lemma 1: $\iota \triangleright \psi$
- Lemma 2: ι is a description function (proof uses Desc)

Standard Frames

- It is desirable to get completeness wrt. standard frames
- Problematic lemma: For all σ and for all *a* in *D*(σ) there is some term *s* such that $s \triangleright_\sigma a$
  - Having *D* defined as Ran(▹), this lemma is trivial
  - Having *D* defined as a standard frame, this lemma does not hold anymore for all types σ
    - It still holds for type ι (believe me)
    - It holds for type o if for example $\{\top, \bot\} \subseteq S$ (of course, there are other choices)

23

Standard Frames ctd.

- This restriction affects all rules that quantify over terms:

$$\textsc{ExN}\ \frac{\neg(\exists s)}{[st]}\ \boxed{t \in \Lambda^S \text{ normal}} \qquad \textsc{Choice}\ \frac{C[\varepsilon s]}{\neg[st] \mid [s(\varepsilon s)]}\ \begin{array}{l} C \text{ accessibility context,} \\ \boxed{t \in \Lambda^S_\sigma \text{ normal}} \end{array}$$

$$\textsc{Desc}\ \frac{C[\iota s]}{\neg[st] \mid x \neq y,\ [sx],\ [sy] \mid [s(\iota s)]}\ \begin{array}{l} C \text{ accessibility context,} \\ \boxed{t \in \Lambda^S_\sigma \text{ normal,}}\ \text{x, y fresh} \end{array}$$

$$\text{BQ}\ \frac{s =_{\tau_1 \ldots \tau_n o} t}{[su_1 \ldots u_n],\ [tu_1 \ldots u_n] \mid \neg[su_1 \ldots u_n],\ \neg[tu_1 \ldots u_n]}\ \begin{array}{l} n \geq 0, \\ \boxed{u_i \in \Lambda^S_{\tau_i} \text{ normal}} \end{array}$$

$$\textsc{Con}\ \frac{s =_{\tau_1 \ldots \tau_n \iota} t,\ u \neq_\iota v}{[sw_1 \ldots w_n] \neq_\iota u,\ [tw_1 \ldots w_n] \neq_\iota u \mid [sw_1 \ldots w_n] \neq_\iota v,\ [tw_1 \ldots w_n] \neq_\iota v}\ \begin{array}{l} n \geq 0, \\ \boxed{w_i \in \Lambda^S_{\tau_i} \text{ normal}} \end{array}$$

- Consequence: $=_{\tau 1 \ldots \tau n\ \sigma}$, $\exists_\sigma$, ι_σ and ε_σ only for σ, τ_1, ... $\tau_n \in \{o, \iota\}$ allowed

- Interesting fact: *if* is not affected!

24

Extensions

Future Work

Extensions

- n-ary choice
  - Choice as presented in this thesis is just for sets (type σo)
  - What about binary relations (type $\sigma\tau o$)?
  - It turns out that choice for (arbitrary) relations is implied by choice for sets
  - Introducing additional logical constants makes them easier to use
- Restricting instantiations
  - Paper by Chad and myself (accepted to IJCAR 2010)
  - It is enough to consider as instantiations
    - $\top$, $\bot$ at type o
    - discriminating terms at type ι
    - at function types terms which only contain free variables that are already free

Extensions ctd

- Primitive Recursion and the Natural Numbers
  - New type *n*, new logical constants *0:n* (zero), *S:nn* (successor function), *pr:σ(nσσ)nσ* (primitive recursion)
  - Rules bases on the peano axioms

$$\frac{St = 0}{} \qquad \frac{0 = St}{} \qquad \frac{St = Su}{t = u} \qquad \frac{[tu]}{[t0] \mid \neg[ty],\ [t(Sy)]}\ t : no,\ y \text{ fresh}$$

$$\frac{x \neq_n x}{} \qquad \frac{0 \neq 0}{} \qquad \frac{St \neq Su}{t \neq u}$$

$$\frac{C[pr\, s\, t\, u]}{u = 0,\ [C[s]] \ \mid\ u = Sx,\ [C[t\, x\, (pr\, s\, t\, x)]]}\ \begin{array}{l} C \text{ accessibility} \\ \text{context},\ x \text{ fresh}\end{array}$$

  - It looks like we need to extend quasiformulas to (dis-)equations at type *n*

27

Thank you!

28

References

- P. B. Andrews. "General Models, Descriptions, and Choice in Type Theory". J. Symb. Log., 37(2): 385–394, 1972.
- J. Backes, C. E. Brown: "Analytic Tableaux for Higher-Order Logic with Choice". In Fifth International Joint Conference on Automated Reasoning (IJCAR 2010), 2010. to appear.
- C. E. Brown, G. Smolka: "Terminating Tableaux for the Basic Fragment of Simple Type Theory". TABLEAUX 2009:138-151, Springer LNCS 5607.
- C. E. Brown, G. Smolka: "Extended First-Order Logic". TPHOLs 2009, Springer LNCS 5674.
- C. E. Brown, G. Smolka: "Complete Cut-Free Tableaux for Equational Simple Type Theory". 2009.
- C. E. Brown, G. Smolka. "Analytic Tableaux for Simple Type Theory and its First-Order Fragment". 2009.
- G. Mints: "Cut-Elimination for Simple Type Theory with an Axiom of Choice". The Journal of Symbolic Logic, Vol. 64, No. 2., pp. 479-485. 1999.
- G. Takeuti: "Proof Theory (Studies in Logic and the Foundations of Mathematics)". Elsevier Science Ltd, 2 Rev Sub edition. 1987.

29