On Model-Theoretic Strong Normalization for Truth-Table Natural Deduction

Andreas Abel
Department of Computer Science and Engineering,
Chalmers University of Technology, Göteborg, Sweden
Gothenburg University, Göteborg, Sweden

Abstract

Intuitionistic truth table natural deduction (ITTND) by Geuvers and Hurkens (2017), which is inherently non-confluent, has been shown strongly normalizing (SN) using continuation-passing-style translations to parallel lambda calculus by Geuvers, van der Giessen, and Hurkens (2019). We investigate the applicability of standard model-theoretic proof techniques and show (1) SN of detour reduction (β) using Girard's reducibility candidates, and (2) SN of detour and permutation reduction ($\beta\pi$) using biorthogonals. In the appendix, we adapt Tait's method of saturated sets to β, clarifying the original proof of 2017, and extend it to $\beta\pi$.

2012 ACM Subject Classification Theory of computation → Proof theory

Keywords and phrases Natural deduction, Permutative conversion, Reducibility, Strong normalization, Truth table

Digital Object Identifier 10.4230/LIPIcs.TYPES.2020.1

Supplementary Material *Software (Source Code)*: `https://github.com/andreasabel/truthtable`
archived at `swh:1:dir:ad022539d7490ea9943b3f497f41ab2108acebc2`

Funding This work has been supported by grant no. 2019-04216 *Modal Dependent Type Theory* of the Swedish Research Council (Vetenskapsrådet).

Acknowledgements Thanks to Herman Geuvers for explaining me truth-table natural deduction during a 2018 visit to Nijmegen for the purpose of Henning Basold's PhD ceremony. Thanks to Ralph Matthes, Herman Geuvers and Tonny Hurkens for some email discussions on the topics of this article. I am also grateful for the feedback of the reviewer that led to a substantial clarification of the proof using orthogonality.

1 Introduction

Recently, Geuvers and Hurkens [13] have observed that, departing from the truth table of a logical connective, one can in a schematic way construct introduction and elimination rules for that connective both for intuitionistic and classical natural deduction. For each line in the truth table where the connective computes to *true* one obtains an introduction rule, and for the *false* lines one obtains an elimination rule. It is shown that these *truth table natural deduction* (TTND) calculi are equivalent to Gentzen's original calculi [12] in the sense that the same judgements can be derived. However, the schematic rules are sometimes unwieldy and unintuitive – for instance, in TTND there are three introduction rules for implication since $A \to B$ is true for three out of four valuations of (A, B). As a remedy, Geuvers and Hurkens show how the original TTND rules can be optimized in a systematic way. In this article, we shall confine ourselves to the schematic, unoptimized rules of intuitionistic TTND (ITTND).

When studying proof terms and proof normalization for ITTND, one can observe that β-reduction – the reduction of detours, i.e., introductions followed directly by eliminations[1]– is essentially non-deterministic and even non-confluent. Non-confluence poses some challenges

[1] Geuvers and Hurkens call detour redexes *direct intuitionistic cuts* [13] or *a*-redexes [14] and with van der Giessen D-redexes [16]. We follow Joachimski and Matthes [20] and call detour reductions simply β-reductions, as these are a generalization of the β-reduction of λ-calculus.

26th International Conference on Types for Proofs and Programs (TYPES 2020).
Editors: Ugo de'Liguoro, Stefano Berardi, and Thorsten Altenkirch; Article No. 1; pp. 1:1–1:21
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

to the proof that reduction is terminating, the so-called strong normalization (SN) property. In the original presentation [13], the authors confine the SN proof to ITTND with a single but universal connective *if-then-else* and the optimized inference rules for if-then-else which yield confluent and standardizing β-reduction. The proof follows the *saturated sets* method pioneered by Tait [30] which is known to rely on standardization by using deterministic weak head reduction.[2]

In subsequent work [14], the authors attack SN for full ITTND with non-confluent β-reduction, introducing elements of Girard's technique of *reducibility candidates* (RCs) [17, 19]. However, this innovative mix of Tait and Girard is not without pitfalls, as we shall investigate in Section 4.2. We tread on safer grounds by returning to Girard's original definition of RCs in Section 4. Our proof in Section 4.1 relies on impredicativity and could not be formalized in a predicative metatheory such as Martin-Löf Type Theory [24]. We thus give in Section 4.3 a variant that replaces the use of impredicativity by inductive definitions.

However, β-reduction is not the only form of proof optimization in ITTND. The schematic elimination rules of ITTND have the flavor of disjunction elimination which does not pose any restriction on the formula on the right. Likewise, eliminations in ITTND have an arbitrary target. In such settings, one eliminates a hypothesis to directly prove the desired conclusion. Eliminating into an intermediate conclusion which is then eliminated again is thus considered a detour. Joachimski and Matthes [20] call such a detour a *permutation redex* or *π-redex*[3] – in the context of intuitionistic sequent calculus restricted to implication. Permutation reduction for ITTND by itself is terminating [14], and in *loc. cit.* it is shown that the free combination with β-reduction, $\beta\pi$, is weakly normalizing. Strong normalization was left open until the joint work of Geuvers and Hurkens with van der Giessen [16], where SN was established via a continuation-passing-style (CPS) translation to the parallel simply-typed lambda calculus (parallel STLC).[4]

The change of proof strategy begs the question whether the usual model-theoretic SN proofs could not work also for $\beta\pi$-reduction. While the saturated sets method applied in a similar situation by Joachimski and Matthes [20] seems not applicable due to non-confluence of β, Girard's RCs do not cover π. However, there is a third popular method, *(bi)orthogonals*, that has been developed to prove SN for classical lambda-calculi which are essentially non-confluent. [5] Biorthogonals have been successfully applied by Lindley and Stark [22] to prove SN for Moggi's "monadic metalanguage", that is STLC with introduction, elimination, and permutation rules for the monad. We show in Section 6 that biorthogonals, putting elimination sequences at the center of attention, can show SN for $\beta\pi$ of ITTND. Finally, in the Appendix A, we demonstrate how the the saturated sets method can also be adapted.

While we limit our presentation on the implicational fragment of ITTND for didactic purposes and convenience of exposition, our techniques scale immediately to the general case.

Overview

In Section 2 we recapitulate Geuvers and Hurkens' construction of intuitionistic inference rules from truth tables and the associated β-rules. In Section 3 we present a common structure of model-theoretic SN proofs. This structure is instantiated to RCs in Section 4 and we present the two ways of constructing the interpretation of the connectives: via the

[2] Weak head reduction is sometimes called *key reduction* in the context of saturated sets.

[3] Geuvers and Hurkens call π-redexes *b*-redexes [14] and, with van der Giessen, P-redexes [16].

[4] In a first approximation, one can think of parallel STLC as STLC with explicit non-determinism.

[5] Early applications of orthogonality can be found in the works of Parigot [27, 28] and Barbanera and Berardi [4].

elimination rules (Section 4.1) and via the introduction rules (Section 4.3). Further, we take a critical look at the proof of Geuvers and Hurkens [14] in Section 4.2. In Section 5 we turn to π-reduction, laying some foundation for the SN proof for $\beta\pi$ using orthogonality (Section 6), which is the main contribution of this paper. We conclude with a short discussion in Section 7.

2 Intuitionistic Truth Table Natural Deduction

Geuvers and Hurkens [13] introduced a method to derive natural deduction proof rules from truth tables of logical connectives. For instance, consider the truth table for implication:

A	B	$A \to B$
0	0	1
0	1	1
1	0	0
1	1	1

For each line where $A \to B$ holds, e.g., the second line, an introduction rule is created where 0-valued (or *negative*) operands A become premises $\Gamma.A \vdash A \to B$ and 1-valued (or *positive*) operands B become premises $\Gamma \vdash B$. Lines like the third where $A \to B$ is false become elimination rules with a conclusion $\Gamma \vdash C$ for an arbitrary formula C. The premises of this elimination rule are, besides the principal premise $\Gamma \vdash A \to B$, a premise $\Gamma \vdash A$ for each 1-valued operand A, and a premise $\Gamma.B \vdash C$ for each 0-valued operand B. This yields the following four rules of judgement $\boxed{t : \Gamma \vdash A}$:[6]

$$\frac{t : \Gamma.A \vdash A \to B \qquad u : \Gamma.B \vdash A \to B}{\mathsf{in}^{00}_{\to}(t, u) : \Gamma \vdash A \to B} \qquad \frac{t : \Gamma.A \vdash A \to B \qquad b : \Gamma \vdash B}{\mathsf{in}^{01}_{\to}(t, b) : \Gamma \vdash A \to B}$$

$$\frac{f : \Gamma \vdash A \to B \qquad a : \Gamma \vdash A \qquad t : \Gamma.B \vdash C}{f \cdot \mathsf{el}^{10}_{\to}(a, t) : \Gamma \vdash C} \qquad \frac{a : \Gamma \vdash A \qquad b : \Gamma \vdash B}{\mathsf{in}^{11}_{\to}(a, b) : \Gamma \vdash A \to B}$$

As seen from these instances, we preferably use letters t, u, v for terms with a distinguished hypothesis and letters a, b, c, d, e, f for terms without such. Replacing the distinguished hypothesis, i.e., the 0th de Bruijn index, in term t by a term a is written $t[a]$. We use letter I for introduction terms, i.e., such with "in" at the root, and letter E for an elimination in term $f \cdot E$, i.e., the "el" part. Heads h are either variables x or introductions I, and each term can be written in spine form $h \cdot E_1 \cdot \dots \cdot E_n$. This may be written $h \cdot \vec{E}$.

Detour or β reductions can fire when an introduction is immediately eliminated, i.e., on well-typed subterms of the form $I \cdot E$. For the case of implication, there are three introduction rules that can be paired with the only elimination rule. There are two ways in which a β

[6] Additional information for the reader unfamiliar with natural deduction and proof terms:
Natural deduction asserts the truth of a proposition A under a list of assumed propositions Γ, a *context*, via the judgement $\Gamma \vdash A$. Derivations of such judgements form proof trees where nodes are labeled by the name of the applied proof rule and the ordered subtrees correspond to the premises of that rule. Leaves are either applications of a rule that has no premises or references to one of the hypotheses in Γ.
We write ε for empty lists. The list Γ can be extended on the right by a proposition A using the notation $\Gamma.A$. Following de Bruijn [11], we number the hypotheses from the right starting with zero. A reference to a hypothesis – a so-called *de Bruijn index* – is a non-negative number i strictly smaller than the length of Γ. For example, de Bruijn index zero, written x_0, refers to proposition A in context $\Gamma.A$. We write $x : \Gamma \vdash A$ to denote a de Bruijn index x pointing to proposition A in context Γ.
In general, we use the notation $t : \Gamma \vdash A$ to state that t is a valid proof tree, also called proof term, whose conclusion is the judgement $\Gamma \vdash A$. We will only refer to terms t that correspond to a valid proof tree, thus, we consider terms as intrinsically typed [3, 5]. This choice however affects neither presentation nor results in this article very much; they apply the same to extrinsic typing.

redex can fire: Either, a positive premise (1) of the introduction matches a negative premise (0) of the elimination. For the case of implication, the second premise of the elimination $\mathsf{el}_{\to}^{10}$ is negative, and it can react with the positive second premise of $\mathsf{in}_{\to}^{01}$ and $\mathsf{in}_{\to}^{11}$:

$$\mathsf{in}_{\to}^{\_1}(\_, b) \cdot \mathsf{el}_{\to}^{10}(\_, t) \quad \mapsto_\beta \quad t[b]$$

The other reaction is between a negative premise of the introduction and a matching positive premise of the elimination. In this case, the elimination persists, but the introduction is replaced with an instantiation of its respective negative premise. In the case of implication, the first premise of $\mathsf{in}_{\to}^{00}$ and $\mathsf{in}_{\to}^{01}$ can be instantiated with the first premise of $\mathsf{el}_{\to}^{10}$:

$$\mathsf{in}_{\to}^{0\_}(u, \_) \cdot \mathsf{el}_{\to}^{10}(a, t) \quad \mapsto_\beta \quad u[a] \cdot \mathsf{el}_{\to}^{10}(a, t)$$

The case of implication already demonstrates the inherent non-confluence of β-reduction: the reducts of $\mathsf{in}_{\to}^{01}(u, b) \cdot \mathsf{el}_{\to}^{10}(a, t)$ form the critical pair $(t[b],\ u[a] \cdot \mathsf{el}_{\to}^{10}(a, t))$ which can in general not be joined. Non-confluence excludes some techniques to show strong normalization, e.g., those that rely on deterministic weak head reduction. However, Girard's reducibility candidates accommodate non-confluent reduction, thus, his technique may be adapted to the present situation.

3 Model-theoretic proofs of strong normalization

In this section we explain the general format of a model-theoretic proof of strong normalization. We will instantiate this framework to two techniques later: reducibility candidates (Section 4) and orthogonality (Section 6).

3.1 Preliminaries

We work with sets $\Gamma \vdash A$ of nameless well-typed terms. De Bruijn indices are written $\mathsf{x}_n : \Gamma.A.\Delta \vdash A$ where Δ has length n. Instead of full-fledged renaming, we confine to weakening under order-preserving embeddings (OPE) $\boxed{\tau : \Delta \leq \Gamma}$. Here, τ witnesses that and how Γ is a subsequence of Δ. Then, $\Uparrow\tau : \Delta.B \leq \Gamma.B$ be the *lifted* OPE. Further, $\uparrow : \Gamma.B \leq \Gamma$ is the OPE for weakening by one variable, and OPEs form a category with identity $\mathbb{1} : \Gamma \leq \Gamma$ and composition $(\Gamma \leq \Delta) \to (\Delta \leq \Phi) \to (\Gamma \leq \Phi)$ written as juxtaposition. If $a : \Gamma \vdash A$ then *weakening* $a\tau : \Delta \vdash A$ is defined in the usual way. In particular, $\Uparrow$ is used to traverse under binders, for instance, $\mathsf{in}_{\to}^{01}(t, b)\tau = \mathsf{in}_{\to}^{01}(t(\Uparrow\tau), b\tau)$.

Substitutions $\boxed{\sigma : \Delta \vdash \Gamma}$ are defined as lists of terms $\sigma = \varepsilon.b_1.\cdots.b_{|\Gamma|}$ typed by list Γ under context Δ. Parallel substitution $a\sigma : \Delta \vdash A$ for $a : \Gamma \vdash A$ is defined as usual. OPEs $\tau : \Delta \leq \Gamma$ are silently coerced to substitutions $\Delta \vdash \Gamma$ consisting only of de Bruijn indices. Substitutions form a category, and we reuse $\mathbb{1}$ for identity and juxtaposition for substitution. Like for OPEs, we have lifting $\Uparrow : (\Delta \vdash \Gamma) \to (\Delta.B \vdash \Gamma.B)$ to push substitutions under binders. Single substitution $t[b]$ is an instance of parallel substitution $t\sigma$ for substitution $\sigma = \mathbb{1}.b : (\Gamma \vdash \Gamma.B)$ obtained from $b : \Gamma \vdash B$.

Reduction $\boxed{a \longrightarrow a'}$, which is defined using single substitution, acts on same-typed terms $a, a' : \Gamma \vdash A$ by definition. It is closed under weakening and substitution. It is even closed under *anti-weakening*, i.e., if $a\tau \longrightarrow a'\tau$ then also $a \longrightarrow a'$. (Not so for substitution: it is not closed under anti-substitution, of course.) Further, reduction commutes with weakening: If $a\tau \longrightarrow b'$ then there is b with $a \longrightarrow b$ and $b' = b\tau$.

Via the parallel substitution operation, the family $\_ \vdash A$ of terms of type A is a contravariant functor (i.e., presheaf) targeting the category Set of sets and functions. Its source is the category of substitutions, and thus also its subcategory OPE. We will work a lot with presheaves of the latter kind, especially with families of predicates $P_\Gamma \subseteq (\Gamma \vdash A)$ closed under weakening, meaning if $a \in P_\Gamma$ and $\tau : \Delta \leq \Gamma$ then $a\tau \in P_\Delta$. We call such predicates *term set families.* We may simply write $a \in P$ instead of $a \in P_\Gamma$ if Γ is fixed but arbitrary or can be determined by the context.

Our prime example of a term set family are the strongly normalizing terms SN given inductively by rule

$$\frac{(a \longrightarrow \_) \subseteq \mathsf{SN}}{a \in \mathsf{SN}}.$$

While it is formally a family of inductive predicates on well-typed terms $a : \Gamma \vdash A$, we mostly write $a \in \mathsf{SN}$ instead of $a \in \mathsf{SN}(\Gamma \vdash A)$ for simplicity. The set SN is closed under weakening, i.e., if $\tau : \Delta \leq \Gamma$ then $a\tau \in \mathsf{SN}$ as well. This follows easily from anti-weakening for reduction.

3.2 Semantic types and normalization proofs

A typical model-theoretic proof of strong normalization will interpret types A by families $\mathcal{A} = [\![A]\!]$ of strongly normalizing terms of type A. To work smoothly for open terms, a further requirement on such semantic types $\mathcal{A}$ is that they contain the variables, i.e., if $x : \Gamma \vdash A$ then $x \in \mathcal{A}_\Gamma$.

To obtain a compositional interpretation of types, each type constructor such as implication $A \to B$ is interpreted by a suitable operation $\mathcal{A} \to \mathcal{B}$ on semantic types. For pure implicational truth table natural deduction, types are formed from uninterpreted base types o (propositional variables) and function space: $A, B ::= o \mid A \to B$. Types are interpreted as the following semantic types:

$$\begin{array}{lcl} [\![o]\!]_\Gamma & = & \mathsf{SN}(\Gamma \vdash o) \\ [\![A \to B]\!]_\Gamma & = & ([\![A]\!] \to [\![B]\!])_\Gamma \end{array}$$

The main structure of the normalization proof then proceeds as follows: Contexts Γ are interpreted as families of sets of substitutions.

$$\begin{array}{lcl} [\![\varepsilon]\!]_\Delta & = & \Delta \vdash \varepsilon \quad (= \{\sigma \mid \sigma : \Delta \vdash \varepsilon\}) \\ [\![\Gamma.A]\!]_\Delta & = & \{\sigma.a \mid \sigma \in [\![\Gamma]\!]_\Delta \text{ and } a \in [\![A]\!]_\Delta\} \end{array}$$

Thanks to the requirement that the variables inhabit the semantic types, each context can be valuated by the identity substitution:

▶ **Lemma 1** (Identity substitution). $\mathbb{1} \in [\![\Gamma]\!]_\Gamma$.

Proof. By induction on Γ. In case $\Gamma.A$, we have $\mathbb{1} \in [\![\Gamma]\!]_\Gamma$ by induction hypothesis, thus, by weakening, $\uparrow \in [\![\Gamma]\!]_{\Gamma.A}$. Further, the 0th de Bruijn index $\mathsf{x}_0 \in [\![A]\!]_{\Gamma.A}$. Thus $(\uparrow.\mathsf{x}_0) = \mathbb{1} \in [\![\Gamma.A]\!]_{\Gamma.A}$. ◀

The main theorem shows that each well-typed term inhabits the corresponding semantic type:

▶ **Theorem 2** (Fundamental theorem of logical predicates). *If $a : \Gamma \vdash A$ and $\sigma \in [\![\Gamma]\!]_\Delta$ then $a\sigma \in [\![A]\!]_\Delta$.*

Normalization is then a direct consequence:

▶ **Corollary 3** (Strong normalization). *If $a : \Gamma \vdash A$ then $a \in \mathsf{SN}$.*

Proof. By Theorem 2 with Lemma 1, $a\,\mathbb{1} = a \in [\![A]\!]_\Gamma$, thus, $a \in \mathsf{SN}$ since each semantic type contains only strongly normalizing terms. ◀

The definition of the semantic types such as $\mathcal{A} \to \mathcal{B}$ needs be crafted such as to allow us to prove Theorem 2. In the next section we identify the necessary properties.

3.3 Modelling the inference rules

To formulate the properties that allow us to prove Theorem 2 we introduce an auxiliary construction $\boxed{\mathcal{C}[\mathcal{A}]}$, "*abstraction*", given semantic types $\mathcal{A}$ and $\mathcal{C}$, where $\mathcal{A}$ classifies terms of type A and $\mathcal{C}$ terms of type C.

$$\mathcal{C}[\mathcal{A}]_\Gamma = \{t \in \Gamma.A \vdash C \mid t(\tau.a) \in \mathcal{C}_\Delta \text{ for all } \tau : \Delta \leq \Gamma \text{ and } a \in \mathcal{A}_\Delta\}.$$

The abstraction[7] $\mathcal{C}[\mathcal{A}]$ is a presheaf via the weakening with the lifted OPE:

▶ **Lemma 4.** *If $\tau : \Delta \leq \Gamma$ and $t \in \mathcal{C}[\mathcal{A}]_\Gamma$ then $t(\Uparrow \tau) : \mathcal{C}[\mathcal{A}]_\Delta$.*

Proof. Assume $\tau' : \Phi \leq \Delta$ and $a \in \mathcal{A}_\Phi$ and show $t(\Uparrow \tau)(\tau'.a) \in \mathcal{C}_\Phi$. Since $(\Uparrow \tau)(\tau'.a) = \tau\tau'.a$ this follows by definition of $t \in \mathcal{C}[\mathcal{A}]_\Gamma$. ◀

Using abstraction, the properties of the semantic connective can be mechanically obtained from the inference rules for the syntactic connective. In the formulation of these properties, a judgement $a : \Gamma \vdash A$ turns into statement $a \in \mathcal{A}_\Gamma$ and a judgement $t : \Gamma.A \vdash C$ into $t \in \mathcal{C}[\mathcal{A}]_\Gamma$. In case of semantic implication $\mathcal{A} \to \mathcal{B}$, we obtain the following four requirements, one for each rule:

($\mathsf{in}^{00}_{\to}$) If $t \in (\mathcal{A} \to \mathcal{B})[\mathcal{A}]$ and $u \in (\mathcal{A} \to \mathcal{B})[\mathcal{B}]$ then $\mathsf{in}^{00}_{\to}(t, u) \in \mathcal{A} \to \mathcal{B}$.
($\mathsf{in}^{01}_{\to}$) If $t \in (\mathcal{A} \to \mathcal{B})[\mathcal{A}]$ and $b \in \mathcal{B}$ then $\mathsf{in}^{01}_{\to}(t, b) \in \mathcal{A} \to \mathcal{B}$.
($\mathsf{in}^{11}_{\to}$) If $a \in \mathcal{A}$ and $b \in \mathcal{B}$ then $\mathsf{in}^{11}_{\to}(a, b) \in \mathcal{A} \to \mathcal{B}$.
($\mathsf{el}^{10}_{\to}$) If $f \in \mathcal{A} \to \mathcal{B}$ and $a \in \mathcal{A}$ and $t \in \mathcal{C}[\mathcal{B}]$ then $f \cdot \mathsf{el}^{01}_{\to}(a, t) \in \mathcal{C}$.

Given these properties of semantic implication, we can show that semantic types model the inference rules:

Proof of Theorem 2. By induction on $t : \Gamma \vdash C$, prove $t\sigma \in [\![C]\!]_\Delta$ for all $\sigma \in [\![\Gamma]\!]_\Delta$. In case of a variable $t = x$, we have $x\sigma \in [\![\Gamma(x)]\!]_\Delta$ by assumption on σ.

The other cases are covered by the assumptions on semantic implication. For instance, consider:

$$\frac{t : \Gamma.A \vdash A \to B \qquad b : \Gamma \vdash B}{\mathsf{in}^{01}_{\to}(t, b) : \Gamma \vdash A \to B}$$

By induction hypothesis (2) $b\sigma \in [\![B]\!]_\Delta$ and (1) $t(\sigma\tau.a) \in [\![A \to B]\!]_\Phi$ for arbitrary $\tau : \Phi \leq \Delta$ and $a \in [\![A]\!]_\Phi$, since then $\sigma\tau \in [\![\Gamma]\!]_\Phi$. Hence, $t(\Uparrow \sigma) \in ([\![A \to B]\!])[[\![A]\!]]_\Delta$ by definition of abstraction. By property ($\mathsf{in}^{01}_{\to}$), it follows that $\mathsf{in}^{01}_{\to}(t, b)\sigma = \mathsf{in}^{01}_{\to}(t(\Uparrow \sigma), b\sigma) \in [\![A \to B]\!]_\Delta$. ◀

This completes the description of our framework for strong normalization proofs. We now turn our attention to ways how to instantiate this framework.

[7] Matthes [25, Sec. 6.2] uses the notation $\mathsf{S}_x(\mathcal{A}, \mathcal{C})$ for abstraction (in a setting with named variables x).

3.4 Flavors of semantic types

We are familiar with three principal methods how to construct semantic types for strong normalization proofs.

1. *Saturated sets* following Tait [30], see e.g. the exposition by Luo [23]. This technique requires semantic types to be closed under weak head expansion and is only known to work for deterministic weak head reduction. While it has been applied [13] to the *if-then-else* instance of ITTND with optimized rules, it does not cover the general case of TTND with non-deterministic and even non-confluent weak head reduction.
2. *Reducibility candidates* following Girard [17, 19]. We apply this method in Section 4. It covers β-reduction but not $\beta\pi$.
3. *Biorthogonals* that have been used in SN proofs for λ-calculi for classical logic, e.g. by Parigot [27], and in SN proofs for the monadic meta-language by Lindley and Stark [22]. These cover even $\beta\pi$, and we shall turn to these in Section 6.

4 Reducibility Candidates

Girard's reducibility candidates are a flavor of semantic types that can show strong normalization also for non-confluent rewrite relations such as reduction in truth-table natural deduction.

When defining the semantic versions of the logical connectives such as $\mathcal{A} \to \mathcal{B}$, we have the choice to base the definition either on the introduction rules or the elimination rules.[8] We will study both approaches, but first, we recapitulate the definition of reducibility candidates.

Let Intro be the term set of introductions, i.e., the terms of the form $\mathsf{in}_c^{\vec{b}}(\vec{t})$. This set is clearly closed under weakening and anti-weakening.

A *reducibility candidate* $\mathcal{A}$ for a type A is a term set family with the following properties:

CR1 $\mathcal{A}_\Gamma \subseteq \mathsf{SN}$.

CR2 If $a \in \mathcal{A}_\Gamma$ and $a \longrightarrow a'$ then $a' \in \mathcal{A}_\Gamma$.

CR3 For $a : \Gamma \vdash A$, if $a \notin \mathsf{Intro}$ and $(a \longrightarrow \_) \subseteq \mathcal{A}_\Gamma$, then $a \in \mathcal{A}_\Gamma$.

We write $\boxed{\mathcal{A} \in \mathsf{CR}}$ if $\mathcal{A}$ is a term set family satisfying CR1-3. It is easy to see that $\mathsf{SN} \in \mathsf{CR}$. If $\mathcal{A}$ satisfies only CR1/2, it shall be called a *precandidate.*

Term set abstraction operates on precandidates:

▶ **Lemma 5** (Abstraction). *Let $\mathcal{A}_\Gamma$ be inhabited for any Γ. If $\mathcal{C}$ is a precandidate, so is $\mathcal{C}[\mathcal{A}]$.*

Proof. CR1 holds by non-emptiness of $\mathcal{A}$: Given $t \in \mathcal{C}[\mathcal{A}]_\Gamma$ and arbitrary $a \in \mathcal{A}_\Gamma$ we have $t[a] \in \mathcal{C}_\Gamma$. In particular, $t[a] \in \mathsf{SN}$, and thus, $t \in \mathsf{SN}$.

CR2 relies on the closure of reduction under substitution: Assume $\mathcal{C}[\mathcal{A}]_\Gamma \ni t \longrightarrow t'$ and $\tau : \Delta \leq \Gamma$ and $a \in \mathcal{A}_\Delta$. To show $t'(\tau.a) \in \mathcal{C}_\Delta$ observe that $t(\tau.a) \in \mathcal{C}_\Delta$ and that CR2 holds for $\mathcal{C}$. ◀

▶ Remark 6 (On emptiness of RCs). In untyped presentations of RCs, CR3 guarantees non-emptiness of any $\mathcal{A} \in \mathsf{CR}$, since automatically all variables will inhabit $\mathcal{A}$ by virtue of CR3. In our case, $\mathcal{A}_\Gamma$ may be empty since there may be no variables $x : \Gamma \vdash A$ of the correct type A. We thus have to be a bit careful when carrying over the textbook proofs [19] to our intrinsically-typed setting.

[8] See Matthes' [25, Section 6.2] systematic exposition of introduction-based vs. elimination-based definition of semantic types (in the context of the saturated sets method).

4.1 Elimination-based approach

Geuvers and Hurkens [14] base the semantic definition of the logical connective on the elimination rules. A term inhabits a semantic type if it can be soundly eliminated by all possible eliminations for that type. In case of implication,

$$f \in (\mathcal{A} \to \mathcal{B})_\Gamma \iff \forall \mathcal{C} \in \mathsf{CR},\, \tau : \Delta \leq \Gamma,\, a \in \mathcal{A}_\Delta,\, t \in \mathcal{C}[\mathcal{B}]_\Delta.\ f\tau \cdot \mathsf{el}^{10}_{\to}(a,t) \in \mathcal{C}_\Delta.$$

Due to our intrinsic typing, in contrast to Geuvers and Hurkens [14], we need *Kripke-style function space*, i.e., quantify over all extensions Δ of Γ with their respective embeddings $\tau : \Delta \leq \Gamma$. Still, this definition can be mechanically derived from the elimination rules of implication, which is the single rule:

$$\frac{f : \Gamma \vdash A \to B \qquad a : \Gamma \vdash A \qquad t : \Gamma.B \vdash C}{f \cdot \mathsf{el}^{10}_{\to}(a,t) : \Gamma \vdash C}$$

In case of several elimination rules, the definition of the semantic type has to require the closure under all rules [14].

Note the impredicative quantification over all reducibility candidates $\mathcal{C}$, which requires an impredicative meta-theory to formalize this definition. Such an impredicative quantification is not required in the introduction-based approach that we study in Section 4.3.

The elimination-based approach gives us the soundness of the elimination rules for free.

▶ **Lemma 7** (Elimination). *If $f \in \mathcal{A} \to \mathcal{B}$ and $a \in \mathcal{A}$ and $t \in \mathcal{C}[\mathcal{B}]$ then $f \cdot \mathsf{el}^{10}_{\to}(a,t) \in \mathcal{C}$. (Property* ($\mathsf{el}^{10}_{\to}$)*.)*

Proof. By definition of $\mathcal{A} \to \mathcal{B}$ using $\tau = \mathbb{1}$. ◀

Soundness of the introduction rules requires some work.

▶ **Lemma 8** (Introduction). *Properties* ($\mathsf{in}^{00}_{\to}$)*,* ($\mathsf{in}^{01}_{\to}$) *and* ($\mathsf{in}^{11}_{\to}$) *hold for $\mathcal{A} \to \mathcal{B}$.*

Proof. We show property ($\mathsf{in}^{01}_{\to}$), the others are analogous. Assume $t \in (\mathcal{A} \to \mathcal{B})[\mathcal{A}]$ and $b \in \mathcal{B}$ and show $\mathsf{in}^{01}_{\to}(t,b) \in \mathcal{A} \to \mathcal{B}$. To this end, assume $\mathcal{C} \in \mathsf{CR}$ and $\tau : \Delta \leq \Gamma$ and $a \in \mathcal{A}_\Delta$ and $u \in \mathcal{C}[\mathcal{B}]_\Delta$ and show $v := \mathsf{in}^{01}_{\to}(t,b)\tau \cdot \mathsf{el}^{10}_{\to}(a,u) \in \mathcal{C}_\Delta$ by induction on $t(\Uparrow \tau), b\tau, a, u \in \mathsf{SN}$ (obtained by CR1).

Since v is not an introduction we shall utilize CR3 for $\mathcal{C}$. Therefore, we have to show that all reducts of v are already in $\mathcal{C}_\Delta$.

If reduction happens in subterm $b\tau$, so $b\tau \longrightarrow b'$, we can apply the induction hypothesis on $b' \in \mathsf{SN}$, since $b' \in \mathcal{B}_\Delta$ by CR2. Reduction in one of the other subterms t, a, u of v is treated analogously.

It remains to cover the β-reductions at the root, which are $v \longrightarrow u[b\tau]$ and $v \longrightarrow t(\tau.a) \cdot \mathsf{el}^{10}_{\to}(a,u)$. We have $u[b\tau] \in \mathcal{C}_\Delta$ by assumptions on u and b. Further, since $t(\tau.a) \in (\mathcal{A} \to \mathcal{B})_\Delta$, by definition $t(\tau.a) \cdot \mathsf{el}^{10}_{\to}(a,u) \in \mathcal{C}_\Delta$. ◀

Let us not forget to verify that $\mathcal{A} \to \mathcal{B}$ is indeed a reducibility candidate.

▶ **Lemma 9** (Function space). *If $\mathcal{A}, \mathcal{B} \in \mathsf{CR}$ then $(\mathcal{A} \to \mathcal{B}) \in \mathsf{CR}$.*

Proof. First, $\mathcal{A} \to \mathcal{B}$ needs to be a term set family. This is facilitated by the Kripke-style definition of the function space: Assume $f \in (\mathcal{A} \to \mathcal{B})_\Gamma$ and $\tau : \Delta \leq \Gamma$ and show $f\tau \in (\mathcal{A} \to \mathcal{B})_\Delta$. To this end assume $\mathcal{C} \in \mathsf{CR}$ and $\tau' \in \Phi \leq \Delta$ and $a \in \mathcal{A}_\Phi$ and $t \in \mathcal{C}[\mathcal{B}]_\Phi$ and show $f\tau\tau' \cdot \mathsf{el}^{10}_{\to}(a,t) \in \mathcal{C}_\Phi$. This follows from the assumption on f with OPE $\tau\tau' : \Phi \leq \Gamma$.

For CR1, assume $f \in (\mathcal{A} \to \mathcal{B})_\Gamma$ and show $f \in \mathsf{SN}$. Let $\mathcal{C} = \mathcal{A}$ (this choice is simplest, but any RC would do) and $\Delta = \Gamma.A$. Clearly $a := (\mathsf{x}_0 : \Delta \vdash A) \in \mathcal{A}_\Delta$ and $t := (\mathsf{x}_1 : \Delta.B \vdash A) \in \mathcal{C}[\mathcal{B}]_\Delta$. Thus $f\tau \cdot \mathsf{el}^{10}_{\to}(a, t) \in \mathcal{C}_\Delta \subseteq \mathsf{SN}$. This implies $f \in \mathsf{SN}$.

Closure under reduction (CR2) follows because reduction is closed under weakening and elimination.

For CR3, assume $f : \Gamma \vdash A \to B$ that is not an introduction and whose reducts are in $(\mathcal{A} \to \mathcal{B})_\Gamma$. To show $f \in (\mathcal{A} \to \mathcal{B})_\Gamma$, assume $\mathcal{C} \in \mathsf{CR}$ and $\tau : \Delta \leq \Gamma$ and $a \in \mathcal{A}_\Delta$ and $t \in \mathcal{C}[B]_\Delta$ and show $f\tau \cdot E \in \mathcal{C}_\Delta$ where $E = \mathsf{el}^{10}_{\to}(a, t)$. We proceed by CR3 for $\mathcal{C}$, exploiting that $f\tau \cdot E$ is not an introduction either. It is sufficient to show that all reducts of $f\tau \cdot E$ are in $\mathcal{C}_\Delta$. We proceed by induction on $a, t \in \mathsf{SN}$. Since f is not an introduction, we can only reduce in f or in E. Reductions in f are covered by the assumption on f. Reductions in E are either $a \longrightarrow a'$ or $t \longrightarrow t'$ and covered by the respective induction hypothesis, since a' and t' stay in their respective RCs by virtue of CR2. ◀

Strong normalization now follows according to Section 3.

4.2 A gap in the original proof by Geuvers and Hurkens, and its fix

In their elimination-based SN proof, Geuvers and Hurkens [14, Section 6.1] use for semantic types saturated sets with the expansion closure modified to liken CR3. To explain their approach, let us first introduce weak head reduction[9] $I \cdot E \cdot \vec{E} \rhd_\beta v \cdot \vec{E}$ where β-redex $I \cdot E$ contracts to v and the elimination sequence $\vec{E}$ is arbitrary (can be empty). Any SN term that is neither an introduction nor a $\rhd_\beta$-redex is called neutral (set Neut).

In Def. 57.3 [14] a set of terms $\mathcal{X}$ is defined to be saturated ($\mathcal{X} \in \mathsf{SAT}$) if

a. (SAT1) $\mathcal{X} \subseteq \mathsf{SN}$,

b. (SAT2) $\mathsf{Neut} \subseteq \mathcal{X}$, and

c. (SAT3′) $\mathcal{X}$ is closed under $\rhd_\beta$-expansion, namely if $t \in \mathsf{SN}$ and $(t \rhd_\beta \_) \subseteq \mathcal{X}$ (*) then $t \in \mathcal{X}$.

In the original formulation (SAT3) of the saturated sets method,[10] the requirement (*) is that $(t \rhd_\beta \_) \cap \mathcal{X}$ is inhabited, meaning that t is the weak-head expansion of some term that is already in $\mathcal{X}$. In the new formulation the requirement is that all weak-head reducts of t are in $\mathcal{X}$. It is easy to see that now SAT2 is subsumed under SAT3′, since neutrals have no weak-head reducts, and the condition (*) is trivially satisfied. The modification of SAT3 towards CR3-style SAT3′ was perhaps undertaken to account for the non-determinism of $\rhd_\beta$ in ITTND.

Unfortunately, with SAT3′ it is not clear how to show the equivalent of Lemma 9, $(\mathcal{A} \to \mathcal{B}) \in \mathsf{SAT}$ [14, Lemma 58]. In the formulation based on untyped terms, $\mathcal{A} \to \mathcal{B}$ is defined by

$$f \in (\mathcal{A} \to \mathcal{B}) \iff \forall \mathcal{C} \in \mathsf{SAT},\ a \in \mathcal{A},\ t \in \mathcal{C}[\mathcal{B}].\ f \cdot \mathsf{el}^{10}_{\to}(a, t) \in \mathcal{C}.$$

To attempt to show SAT3′ for $\mathcal{A} \to \mathcal{B}$, assume $f \in \mathsf{SN}$ with $(f \rhd_\beta \_) \subseteq \mathcal{A} \to \mathcal{B}$ and derive $f \in \mathcal{A} \to \mathcal{B}$. To this end, assume $\mathcal{C} \in \mathsf{SAT}$ and $a \in \mathcal{A}$ and $t \in \mathcal{C}[\mathcal{B}]$ and show $f \cdot E \in \mathcal{C}$ with $E = \mathsf{el}^{10}_{\to}(a, t)$. Since $\mathcal{C}$ is arbitrary, we have to rely on SAT3′ to introduce elements into $\mathcal{C}$. Thus, we need to show (1) $f \cdot E \in \mathsf{SN}$ and (2) $t' \in \mathcal{C}$ whenever $f \cdot E \rhd_\beta t'$. For both goals we need to analyze the reducts of $f \cdot E$. The problem is that f could be an introduction and,

[9] Weak head reduction is called *key reduction* in *loc. cit.*.
[10] See for instance the exposition by Luo [23].

hence, $f \cdot E$ a β-redex reducing to some v. We lack assumptions to show $v \in \mathcal{C}$ and even $v \in \mathsf{SN}$, since v is not of the same form as $f \cdot E$. Were it either $f' \cdot E$ (with $f \longrightarrow f'$) or $f \cdot E'$ (with $E \longrightarrow E'$) there would be some hope to use the assumptions, in particular $f, E \in \mathsf{SN}$.

Note that with the original SAT3 the relevant part of the proof goes in the other direction, we can exploit the closure of weak head reduction under elimination, namely if $f \rhd_\beta f'$ then $f \cdot E \rhd_\beta f' \cdot E$. It seems that this direction is employed in the proof sketch [14, Lemma 58.c], not matching the new requirement SAT3′.

Pointed to the gaps in their argument Geuvers and Hurkens published a revision [15] with two amendments to the definitions:

1. Closure condition SAT3′ now applies only to *weak head redexes* t. Only strongly normalizing weak head redexes t whose weak head reducts are in saturated set $\mathcal{X}$ are forced into $\mathcal{X}$. The thus relativized SAT3′ no longer subsumes SAT2 which forces *neutrals* into $\mathcal{X}$.
2. The semantic connectives are relativized to SN terms. E.g., $f \in (\mathcal{A} \to \mathcal{B})$ stipulates also $f \in \mathsf{SN}$.

The second amendment fixes a problem with connectives that have no eliminations, like *truth*, but does not add anything for connectives with at least one elimination, like $\mathcal{A} \to \mathcal{B}$.

Yet the first amendment allows us now to analyse the reducts of $f \cdot E$ in the proof of SAT3′ for $\mathcal{A} \to \mathcal{B}$. Since f is not an introduction, the only weak head redexes of $f \cdot E$ are of the form $f' \cdot E$ with $f \rhd_\beta f'$. To show $(f \cdot E \rhd_\beta \_) \subseteq \mathcal{C}$, we can thus utilize the assumption $(f \rhd_\beta \_) \subseteq \mathcal{A} \to \mathcal{B}$. This repairs the proof; in Appendix A.1 we will see a variant of the amended proof be spelled out in detail.

In the following section, we can get rid of the impredicative definition of $\mathcal{A} \to \mathcal{B}$ and use an inductive definition instead. We study this introduction-based approach to type interpretation in the context of Girard's method, but conjecture that it could be utilized in the arguably more structured method of Geuvers and Hurkens as well.

4.3 Introduction-based approach

Instead of the impredicative *elimination*-based definition of semantic types like $\mathcal{A} \to \mathcal{B}$, we can base their definition on the *introduction* rules. The rough idea is that elements of $\mathcal{A} \to \mathcal{B}$ can be introduced by any of $\mathsf{in}^{00}_{\to}$, $\mathsf{in}^{01}_{\to}$, and $\mathsf{in}^{11}_{\to}$ – this is a union of reducibility candidates. However, since the first two of these need already the implication they introduce, the construction of a least fixed-point is required.

Note that the union $\mathcal{A} \cup \mathcal{B}$ of two reducibility candidates $\mathcal{A}$ and $\mathcal{B}$ preserves CR1/2, but not CR3. However, property CR3 can be forced by the following closure operation $\boxed{\overline{\mathcal{A}}}$ on a term set $\mathcal{A} \subseteq (\Gamma \vdash A)$.

$$\textsc{emb}\ \frac{a \in \mathcal{A}}{a \in \overline{\mathcal{A}}} \qquad \textsc{exp}\ \frac{a : \Gamma \vdash A \qquad a \notin \mathsf{Intro} \qquad (a \longrightarrow \_) \subseteq \overline{\mathcal{A}}}{a \in \overline{\mathcal{A}}}$$

The closure operation lifts pointwise to families $\mathcal{A}_\Gamma \subseteq \Gamma \vdash A$ of term sets.

▶ **Lemma 10.** *If $a \in \overline{\mathcal{A}}_\Gamma$ and $\tau : \Delta \leq \Gamma$ then $a\tau \in \overline{\mathcal{A}}_\Delta$.*

Proof. By induction on $a \in \overline{\mathcal{A}}_\Gamma$. In case $a \in \mathcal{A}_\Gamma$ (EMB) use the functoriality of $\mathcal{A}$ and EMB. In case EXP, i.e., $a \in \mathsf{SN}(\Gamma \vdash A) \setminus \mathsf{Intro}$ and $(a \longrightarrow \_) \subseteq \overline{\mathcal{A}}_\Delta$ we first have $a\tau \in \mathsf{SN}(\Delta \vdash A) \setminus \mathsf{Intro}$. If $a\tau \longrightarrow b'$ then there is b with $a \longrightarrow b$ and $b' = b\tau$, and by induction hypothesis $b\tau \in \overline{\mathcal{A}}_\Delta$. Thus $a\tau \in \overline{\mathcal{A}}_\Delta$ by EXP. ◀

▶ **Lemma 11** (Saturation). *$\overline{\mathcal{A}}$ is a reducibility candidate for any precandidate $\mathcal{A}$.*

Proof. CR3 is forced by the closure operation. Closure under reduction (CR2) and preservation of SN (CR1) are proven by induction on $a \in \overline{\mathcal{A}}$, the latter using that $a \in \mathsf{SN}$ when all of a's reducts are. ◀

We may now define a notion of function space on reducibility candidates based on the introduction rules for implication. Since introduction rules are "recursive" in general, i.e., may mention the principal formula in the subsequent of a premise, we need to employ the least fixed-point operation μ for monotone operators on the lattice of reducibility candidates. We define $\mathcal{A} \to \mathcal{B} = \mu\mathcal{F}$ where

$$\mathcal{F}(\mathcal{X})_\Gamma = \overline{\{\mathsf{in}^{00}_{\to}(t,u), \mathsf{in}^{01}_{\to}(t,b), \mathsf{in}^{11}_{\to}(a,b) \mid a \in \mathcal{A}_\Gamma, b \in \mathcal{B}_\Gamma, t \in \mathcal{X}[\mathcal{A}]_\Gamma, u \in \mathcal{X}[\mathcal{B}]_\Gamma\}}$$

This operation acts on reducibility candidates:

▶ **Lemma 12** (Function space)**.** *If $\mathcal{A}$ and $\mathcal{B}$ are reducibility candidates, so is $\mathcal{A} \to \mathcal{B}$.*

Proof. It is sufficient to show that $\mathcal{F}$ acts on reducibility candidates. Since CR3 is forced, it is sufficient that $\mathcal{F}(\mathcal{X})$ is a precandidate for any candidate $\mathcal{X}$, and this follows mostly from Lemma 5 and the candidateship of $\mathcal{A}$ and $\mathcal{B}$. CR1 follows since any reduction of an introduction needs to happen in one of the arguments of in, which are SN. CR2 follows by the same observation. ◀

By definition, $\mathcal{A} \to \mathcal{B}$ models the introduction rules for implication: properties ($\mathsf{in}^{00}_{\to}$), ($\mathsf{in}^{01}_{\to}$) and ($\mathsf{in}^{11}_{\to}$). For the elimination rule, property ($\mathsf{el}^{10}_{\to}$), we have to do a bit of work.

▶ **Lemma 13** (Function elimination)**.** *Let $\mathcal{A}, \mathcal{B}, \mathcal{C}$ be candidates. If $f \in \mathcal{A} \to \mathcal{B}$ and $a \in \mathcal{A}$ and $u \in \mathcal{C}[\mathcal{B}]$ then $f \cdot E \in \mathcal{C}$ where $E = \mathsf{el}^{10}_{\to}(a,u)$.*

Proof. By main induction on $f \in \mathcal{A} \to \mathcal{B}$.

Case (exp) $f \notin \mathsf{Intro}$ and $f \longrightarrow f'$ implies $f' \in \mathcal{A} \to \mathcal{B}$. We show $f \cdot E \in \mathcal{C}$ by side induction on $E \in \mathsf{SN}$ via CR3. First, $f \cdot E \notin \mathsf{Intro}$. Assume $f \cdot E \longrightarrow c$. Since f is not a introduction, we have either $f \longrightarrow f'$ or $E \longrightarrow E'$. In the first case, by main induction hypothesis, $f' \cdot E \in \mathcal{C}$. In the second case, $f \cdot E' \in \mathcal{C}$ by side induction hypothesis. In any case, $c \in \mathcal{C}$. Since c was arbitrary, $f \cdot E \in \mathcal{C}$ by CR3.

Case $f = \mathsf{in}^{00}_{\to}(t_1, t_2)$ where $t_1 \in (\mathcal{A} \to \mathcal{B})[\mathcal{A}]$ and $t_2 \in (\mathcal{A} \to \mathcal{B})[\mathcal{B}]$. We show $f \cdot E \in \mathcal{C}$ by side induction on $t_1, t_2, E \in \mathsf{SN}$ via CR3. Given $f \cdot E \longrightarrow c$, there are three cases. Either $c = f' \cdot E$ with $f \longrightarrow f'$ or $c = f \cdot E'$ with $E \longrightarrow E'$ or $c = t_1[a] \cdot E$. The first two cases are handled by the side induction hypotheses, the last case by main induction hypothesis on $t_1[a] \in \mathcal{A} \to \mathcal{B}$.

Case $f = \mathsf{in}^{01}_{\to}(t_1, b)$ where $t \in (\mathcal{A} \to \mathcal{B})[\mathcal{A}]$ and $b \in \mathcal{B}$. We show $f \cdot E \in \mathcal{C}$ by side induction on $t, b, E \in \mathsf{SN}$ via CR3. Given $f \cdot E \longrightarrow c$, there are four cases. Either $c = f' \cdot E$ with $f \longrightarrow f'$ or $c = f \cdot E'$ with $E \longrightarrow E'$ or $c = t[a] \cdot E$ or $c = u[b]$. The first two cases are handled by the side induction hypotheses, the but-last case by main induction hypothesis on $t[a] \in \mathcal{A} \to \mathcal{B}$, and the last case by assumption $u \in \mathcal{C}[\mathcal{B}]$.

Case $f = \mathsf{in}^{11}_{\to}(a', b)$ where $a' \in \mathcal{A}$ and $b \in \mathcal{B}$. We show $f \cdot E \in \mathcal{C}$ by side induction on $a', b, E \in \mathsf{SN}$ via CR3.

Given $f \cdot E \longrightarrow c$, there are three cases. Either $c = f' \cdot E$ with $f \longrightarrow f'$ or $c = f \cdot E'$ with $E \longrightarrow E'$ or $c = u[b]$. The first two cases are handled by the side induction hypotheses and the last case by assumption $u \in \mathcal{C}[\mathcal{B}]$. ◀

The pattern outlined here for implication generalizes to arbitrary connectives given by truth tables. Each connective is interpreted as an operation on candidates, using the least fixed-point of the closure of the term set generated by the introductions. Each elimination then has to be proven sound in a lemma similar to Lemma 13.

This concludes our study of reducibility candidates to show SN for ITTND. In the remaining technical sections, we study the extension of the normalization argument to permutations.

5 Permutation Reductions

In previous sections, we have studied the reduction β of detours $I \cdot E$ stemming from an elimination E of a via I just introduced connective. In ITTND, even an elimination E followed by another elimination E', thus, a term of the form $f \cdot E \cdot E'$, constitutes a detour and can be π-reduced.

For the sake of defining and studying π-reduction, let us introduce eliminations E and evaluation contexts $\vec{E}$, aka *spines*, as syntactic classes separate from terms. Eliminations E from type A into type C are typed by judgement $\boxed{E : \Gamma \mid A \vdash C}$. In the case of implication, we have:

$$\frac{a : \Gamma \vdash A \qquad u : \Gamma.B \vdash C}{\mathsf{el}^{10}_{\to}(a, u) : \Gamma \mid A \to B \vdash C}$$

Sequences of eliminations form spines $\vec{E}$, where we denote the empty spine as id and spine construction by a centered dot.

$$\frac{}{\mathsf{id} : \Gamma \mid A \vdash A} \qquad \frac{E : \Gamma \mid A \vdash B \qquad \vec{E} : \Gamma \mid B \vdash C}{E \cdot \vec{E} : \Gamma \mid A \vdash C}$$

Spine construction straightforwardly extends to spine concatenation $\vec{E} \cdot \vec{E}'$. Weakening $\vec{E}\tau$ and substitution $\vec{E}\sigma$ are defined in the obvious way.

Since the target type C of an elimination can be freely chosen, one can structure a proof to always eliminate a hypothesis $x : A$ directly into the goal C. Thus, a sequence $x \cdot E \cdot E'$ of two eliminations $E : \Gamma \mid A \vdash B$ and $E' : \Gamma \mid B \vdash C$, going via an intermediate formula B, can be considered a detour.

This detour is removed by a permutation contraction $\boxed{E \cdot E' \mapsto_\pi E\{E'\}}$ that shifts ("permutes") the outer elimination E' into the negative branches of the inner elimination E. The composition[11] $\boxed{E\{E'\}}$ of eliminations moves a weakened version of E' to the negative branches of E. In the case of implication, we have

$$\mathsf{el}^{10}_{\to}(a, u)\{E'\} = \mathsf{el}^{10}_{\to}(a, u \cdot E'{\uparrow}) \tag{1}$$

where $E'{\uparrow}$ shall denote the weakening of elimination E' by $\uparrow : \Gamma.B \leq \Gamma$. In particular, $\mathsf{el}^{10}_{\to}(a', u'){\uparrow} = \mathsf{el}^{10}_{\to}(a'{\uparrow}, u'(\Uparrow\uparrow))$.

▶ Remark 14. If in Equation (1) term u is an introduction, it may β-react with E' to eliminate further detours. Thus, π-reductions can lead to significant further normalization.

[11] The notation $E\{E'\}$ is due to Joachimski and Matthes [20].

Now a one-step π-*reduction* $\boxed{t \longrightarrow_\pi t'}$ shall be a π-contraction in some spine within term t. Let us further define *spine reduction* $\boxed{\vec{E} \rhd_\pi \vec{E}'}$ as π-contraction within a spine at the root, i.e., inductively by the axiom

$$\vec{E} \cdot E_1 \cdot E_2 \cdot \vec{E}' \rhd_\pi \vec{E} \cdot E_1\{E_2\} \cdot \vec{E}'.$$

Since a spine reduction shortens the length of the spine by 1, spine reduction is SN. For π-reduction, the situation is slightly more complicated since a π-reduction can create new π-redexes: for instance, if in Equation (1) the term u is an elimination. However, these π-redexes have moved deeper into the term, thus, by ranking π-redexes by their depth we can easily construct a termination order. Consequently, π-reduction alone is also SN [14, Thm. 55]. Since elimination composition is associative, i.e., $(E_1\{E_2\})\{E_3\} = E_1\{E_2\{E_3\}\}$, spine and π-reduction are confluent.

5.1 Permutations are harmless

For β-reduction alone, we have the following closure property of SN: If all proper sub-terms and all $\rhd_\beta$-reducts of a term are β-SN, so is the term itself. This is Lemma 2.3. of Geuvers and Hurkens' addendum [15]. We reprove it here for $\beta\pi$-SN. Note that the requirements are not extended to include the $\rhd_\pi$-reducts! So, the addition of permutation reduction is actually "harmless".

From now, let "reduction" be $\beta\pi$-reduction and SN be understood w.r.t. this reduction relation.

▶ **Lemma 15** (Weak head expansion). *Assume $a, b, t, u, a', u' \in \mathsf{SN}$, where mentioned. Let $E = \mathsf{el}^{10}_{\rightarrow}(a', u')$.*

1. *If $t[a'] \cdot E \cdot \vec{E} \in \mathsf{SN}$ then $\mathsf{in}^{00}_{\rightarrow}(t, u) \cdot E \cdot \vec{E} \in \mathsf{SN}$.*
2. *If $t[a'] \cdot E \cdot \vec{E} \in \mathsf{SN}$ and $u'[b] \cdot \vec{E} \in \mathsf{SN}$ then $\mathsf{in}^{01}_{\rightarrow}(t, b) \cdot E \cdot \vec{E} \in \mathsf{SN}$.*
3. *If $u'[b] \cdot \vec{E} \in \mathsf{SN}$ then $\mathsf{in}^{11}_{\rightarrow}(a, b) \cdot E \cdot \vec{E} \in \mathsf{SN}$.*

Proof. We demonstrate statment 2 in detail, the others are similar. For $\mathsf{in}^{01}_{\rightarrow}(t, b) \cdot \mathsf{el}^{10}_{\rightarrow}(a', u') \cdot \vec{E} \in \mathsf{SN}$, we show that all its one-step reducts are SN. To this end, we induct on our two main hypotheses (i) and (ii). The induction on (i) $t[a'] \cdot E \cdot \vec{E} \in \mathsf{SN}$ immediately covers reductions in t, E, and $\vec{E}$, and the induction on (ii) $u'[b] \cdot \vec{E} \in \mathsf{SN}$ covers the remaining inner reductions, namely in b.

Besides inner reductions, we have two $\rhd_\beta$-reductions, yet they are directly implied by our two main hypotheses. It remains to show that the π-contraction of $E \cdot \vec{E}$ is also benign, meaning $I \cdot E' \cdot \vec{E}' \in \mathsf{SN}$, where $I = \mathsf{in}^{01}_{\rightarrow}(t, b)$ and $E' = \mathsf{el}^{10}_{\rightarrow}(a', u' \cdot E_1 \uparrow)$ and $\vec{E} = E_1 \cdot \vec{E}'$. To tackle this by induction hypothesis, we need to show the two new main hypotheses, which are now (i') $t[a'] \cdot E' \cdot \vec{E}' \in \mathsf{SN}$ and (ii') $(u' \cdot E_1 \uparrow)[b] \cdot \vec{E}' \in \mathsf{SN}$. But (i') is just a π-reduct of (i), and (ii') is identical to (ii), once we distribute the substitution $[b]$. The inductive step is thus justified by the first induction hypothesis.

Statement 1 is very similar, only that the second induction is on $(u, u') \in \mathsf{SN}$, to cover reductions in u and u'.

Statement 3 needs a main induction on the length of $\vec{E}$ to cover the case of $\rhd_\pi$-reduction. Further side inductions are needed on $a, a' \in \mathsf{SN}$. ◀

Similar arguments to Lemma 15 can be found in the work of Joachimski and Matthes [21, Sect. 5 and 6]. I have also formalized that argument in Agda, albeit for a simpler case: simply-typed combinatory algebra with conditionals.[12]

[12] `https://github.com/andreasabel/truthtable/blob/1a7a01fd28ffb327e9c91a3722e49b467d05a79d/agda/SK-Bool-ortho.agda`

5.2 Failure of the CR method for $\beta\pi$

Our goal is now a model-theoretic proof of the SN of $\beta\pi$-reduction. Unfortunately, just throwing permutation reductions into the mix and replaying the CR proof for SN-β does not work, despite the "harmless" character of permutations. The proof of Lemma 13 relies on the fact that if $f \cdot E \longrightarrow c$ and $f \notin \mathsf{Intro}$ then either $f \longrightarrow f'$ or $E \longrightarrow E'$, and the structure of the elimination $f \cdot E$ is preserved. However, with permutations, in case $f = f_0 \cdot E_0$ it could be that $c = f_0 \cdot E_0\{E\}$, changing the structure of the elimination. Such reductions are not covered by any of the induction hypotheses.

We cannot arbitrarily tighten the restriction $\_ \notin \mathsf{Intro}$ in the formulation of CR3, since CR3 is used in Lemma 13 to introduce terms of the shape $f \cdot E$ into a reducibility candidate $\mathcal{C}$. Such terms need to satisfy the restriction, therefore we cannot exclude π-redexes in general: a priori, $f \cdot E$ could be a π-redex.

6 Orthogonality

Since the reducibility candidate method does not immediately extend to permutations, we turn to a more powerful technique: (bi)orthogonals [6, 29, 8, 18, 32, 1]. Lindley and Stark [22] have observed that biorthogonals ("$\top\top$-lifting") deal well with the permutation reduction for the monadic bind in a strong normalization proof for the monadic meta-language. We shall thus adapt this technique, although it is more demanding on our meta-theory, requiring greatest fixed-points of non-strictly positive operators. This is covered by Knaster and Tarski's fixed-point theorem [31], but not readily available in type-theoretic proof assistants like Coq [7] and Agda [2].

In the following, when we speak of context-indexed families, we implicitly assume that the family is closed under weakening.

Semantic types $\mathcal{A}$ shall now be context-indexed families of sets of spines $\vec{E}$, and we write $\boxed{a \perp \mathcal{A}_\Gamma}$ to characterize a term $a : \Gamma \vdash A$ as classified by semantic type $\mathcal{A}$. The orthogonality relation $\perp$ is defined as

$$a \perp \mathcal{A}_\Gamma :\Longleftrightarrow \boxed{a \in \mathcal{A}_\Gamma^\perp} :\Longleftrightarrow a \cdot \vec{E} \in \mathsf{SN} \text{ for all } \vec{E} \in \mathcal{A}_\Gamma.$$

We demand of semantic types that they contain the empty spine id and only contain strongly normalizing spines. Reductions $\boxed{\vec{E} \longrightarrow \vec{E}'}$ in spines $\vec{E}$ can either be $\beta\pi$-reductions in the subterms of the eliminations or can be π-contractions along the spine.

More formally, a semantic type $\mathcal{A}_\Gamma$ for syntactic type A at context Γ is a set of *pairs* $(C, (\vec{E} : \Gamma \mid A \vdash C))$. Then $a \perp \mathcal{A}_\Gamma$ is defined as $a \cdot \vec{E} \in \mathsf{SN}(\Gamma \vdash C)$ for all $(C, \vec{E} : \Gamma \mid A \vdash C) \in \mathcal{A}_\Gamma$. However, we typically suppress the type component C which is implicitly determined by $\vec{E}$.

▶ **Lemma 16** (Semantic types). *Let $\mathcal{A}$ be a semantic type for A.*

1. *If $x : \Gamma \vdash A$ is a variable, then $x \perp \mathcal{A}_\Gamma$.*
2. *$\mathcal{A}^\perp \subseteq \mathsf{SN}$.*
3. *$\mathcal{A}^\perp$ is closed under reduction.*

Proof.

1. Given $(C, \vec{E}) \in \mathcal{A}_\Gamma$ show $x \cdot \vec{E} \in \mathsf{SN}$. This holds since the only reductions are in $\vec{E}$, which is required to be SN by definition of semantic types.
2. Given $t \perp \mathcal{A}_\Gamma$ show $t \in \mathsf{SN}$. Since $\mathsf{id} \in \mathcal{A}_\Gamma$, we have $t \cdot \mathsf{id} = t \in \mathsf{SN}$.
3. Given $t \perp \mathcal{A}_\Gamma$ and $t \longrightarrow t'$ and $\vec{E} \in \mathcal{A}_\Gamma$ we have $t' \cdot \vec{E} \in \mathsf{SN}$ since $t \cdot \vec{E} \in \mathsf{SN}$ and $t \cdot \vec{E} \longrightarrow t' \cdot \vec{E}$. ◀

Symmetrically to $\mathcal{A}^\perp$, given a set of terms $\mathcal{T}_\Gamma \subseteq (\Gamma \vdash A)$ we define

$$\mathcal{T}_\Gamma^\perp = \{(C, (\vec{E} : \Gamma \mid A \vdash C)) \mid a \cdot \vec{E} \in \mathsf{SN}(\Gamma \vdash C) \text{ for all } a \in \mathcal{T}_\Gamma\}.$$

Taking the orthogonal $\mathcal{T}^\perp$ of a non-empty SN term set $\mathcal{T}$ is one way to construct a semantic type:

▶ **Lemma 17** (Orthogonals are semantic types). *If $\mathcal{T}$ is a family of non-empty sets of strongly normalizing terms of type A, then $\mathcal{T}^\perp$ is a semantic type for type A.*

Proof. First, $\mathsf{id} \in \mathcal{T}^\perp$ since $\mathcal{T} \subseteq \mathsf{SN}$. Then $\mathcal{T}^\perp \subseteq \mathsf{SN}$ since $\mathcal{T}$ is non-empty. ◀

By definition, orthogonality gives rise to the Galois connection

$$\mathcal{T}^\perp \supseteq \mathcal{A} \iff \mathcal{T} \subseteq \mathcal{A}^\perp$$

(both sides of $\iff$ expand to the same statement $\forall t \in \mathcal{T}, \vec{E} \in \mathcal{A}.\ t \cdot \vec{E} \in \mathsf{SN}$). As a consequence, biorthogonality $\_^{\perp\perp}$ is a closure operator both on sets of terms, $\mathcal{T} \subseteq \mathcal{T}^{\perp\perp}$, and evaluation contexts, $\mathcal{A} \subseteq \mathcal{A}^{\perp\perp}$.

The abstraction type $\mathcal{X}[\mathcal{A}]$ is now defined by

$$\mathcal{X}[\mathcal{A}]_\Gamma = \{(C, (\vec{E} : \Gamma.A \mid X \vdash C)) \mid \vec{E}(\tau.a) \in \mathcal{X}_\Delta \text{ for all } \tau : \Delta \leq \Gamma \text{ and } a \perp \mathcal{A}_\Delta\}.$$

Abstraction operates on semantic types:

▶ **Lemma 18** (Abstraction, revisited). *If $\mathcal{A}$ and $\mathcal{X}$ are semantic types for A and X, then $\mathcal{X}[\mathcal{A}]$ is a semantic type for X.*

Proof. We first show that $(X, (\mathsf{id} : \Gamma.A \mid X \vdash X)) \in \mathcal{X}[\mathcal{A}]_\Gamma$. To this end, assume $\tau : \Delta \leq \Gamma$ and $a \in \mathcal{A}_\Delta$ and show $\mathsf{id}(\tau.a) \in \mathcal{X}_\Delta$. This is trivial, since $\mathsf{id}(\tau.a) = \mathsf{id}$ and $\mathcal{X}$ is a semantic type.

Then, assume $(C, (\vec{E} : \Gamma.A \mid X \vdash C)) \in \mathcal{X}[\mathcal{A}]_\Gamma$ and show $\vec{E} \in \mathsf{SN}$. Choose $\tau = \uparrow : \Gamma.A \leq \Gamma$ and $a = \mathsf{x}_0 \in \mathcal{A}_{\Gamma.A}$ the 0th de Bruijn index, then $\vec{E}(\uparrow, \mathsf{x}_0) = \vec{E} \in \mathcal{X}_{\Gamma.A}$ and hence SN. ◀

Given two semantic types $\mathcal{A}$ and $\mathcal{B}$, the function space $\mathcal{A} \to \mathcal{B}$ is defined as the *greatest fixpoint* $\nu\mathcal{F}^\perp$ of the pointwise orthogonal $\mathcal{F}^\perp$ of the operator

$$\mathcal{F}(\mathcal{X})_\Gamma = \{\mathsf{in}^{00}_\to(t, u), \mathsf{in}^{01}_\to(t, b), \mathsf{in}^{11}_\to(a, b) \mid a \perp \mathcal{A}_\Gamma, b \perp \mathcal{B}_\Gamma, t \perp \mathcal{X}[\mathcal{A}]_\Gamma, u \perp \mathcal{X}[\mathcal{B}]_\Gamma\}.$$

In comparison with the reducibility candidate version in Section 4, the closure operation has been replaced by biorthogonalization, and we converted $\mu(\mathcal{F}^{\perp\perp})$ to $(\nu(\mathcal{F}^\perp))^\perp$. We dropped the outer orthogonalization since we now compute sets of evaluation contexts, but note that $\mathcal{F}$ applies orthogonalization on $\mathcal{X}$. Due to the double "negation", $\mathcal{F}^\perp$ is a non-strictly positive operator which has a (greatest) fixpoint thanks to its monotonicity, yet, this fixpoint is not directly obtainable in meta-theories that only accept *strictly* positive coinductive definitions, such as the type theories of Agda [2] and Coq [7].

▶ **Lemma 19** (Function space, revisited). *If $\mathcal{A}$ is a semantic type for A and $\mathcal{B}$ one for B, then $\mathcal{A} \to \mathcal{B}$ is a semantic type for $A \to B$.*

Proof. Applying Lemma 17, it is sufficient to show that $\mathcal{F}(\mathcal{X})$ is a family of non-empty sets of SN terms for semantic types $\mathcal{X}$. This is the case by assumptions on $\mathcal{A}$, $\mathcal{B}$, and $\mathcal{X}$. ◀

▶ **Lemma 20** (Function introduction). *Given $a \perp \mathcal{A}_\Gamma$ and $b \perp \mathcal{B}_\Gamma$ and $t \perp (\mathcal{A} \to \mathcal{B})[\mathcal{A}]_\Gamma$ and $u \perp (\mathcal{A} \to \mathcal{B})[\mathcal{B}]_\Gamma$, we have $\mathsf{in}^{00}_\to(t, u), \mathsf{in}^{01}_\to(t, b), \mathsf{in}^{11}_\to(a, b) \perp (\mathcal{A} \to \mathcal{B})_\Gamma$.*

Proof. For any of the mentioned introductions I we have $I \in \mathcal{F}(\mathcal{A} \to \mathcal{B})_\Gamma$ by definition of $\mathcal{F}$. Since biorthogonalization is a closure operator, we have $I \in \mathcal{F}(\mathcal{A} \to \mathcal{B})_\Gamma^{\perp\perp}$ and thus $I \perp \mathcal{F}(\mathcal{A} \to \mathcal{B})_\Gamma^{\perp} = (\mathcal{A} \to \mathcal{B})_\Gamma$, since $\mathcal{A} \to \mathcal{B}$ is a fixed point of $\mathcal{F}^\perp$. ◀

It seems now logical to prove the following soundness statement for eliminations:

▶ **Lemma 21** (Function elimination, preliminary). *Let $\mathcal{A}, \mathcal{B}, \mathcal{C}$ be semantic types for A, B, C, resp. If $a \perp \mathcal{A}_\Gamma$ and $u \perp \mathcal{C}[\mathcal{B}]_\Gamma$ then $E = \mathsf{el}^{10}_{\to}(a, u) \in (\mathcal{A} \to \mathcal{B})_\Gamma$.*

However, such a lemma is not strong enough to justify the implication elimination rule, as from $f \perp (\mathcal{A} \to \mathcal{B})_\Gamma$ and $E \in (\mathcal{A} \to \mathcal{B})_\Gamma$ we only get $f \cdot E \in \mathsf{SN}$, but we need the stronger $f \cdot E \in \mathcal{C}_\Gamma$. Thus, we prove the following stronger lemma.

▶ **Lemma 22** (Function elimination, revisited). *Let $\mathcal{A}, \mathcal{B}, \mathcal{C}$ be semantic types for A, B, C, resp. If $a \perp \mathcal{A}_\Gamma$ and $u \perp \mathcal{C}[\mathcal{B}]_\Gamma$ and $E = \mathsf{el}^{10}_{\to}(a, u)$ and $\vec{E} \in \mathcal{C}_\Gamma$ then $E \cdot \vec{E} \in (\mathcal{A} \to \mathcal{B})_\Gamma$.*

Proof. Let $\mathcal{X}_\Gamma = \{E \cdot \vec{E} \mid E = \mathsf{el}^{10}_{\to}(a, u)$ for some $a \perp \mathcal{A}_\Gamma$ and $u \perp \mathcal{C}[\mathcal{B}]_\Gamma$, and $\vec{E} \in \mathcal{C}_\Gamma\}$. To show $\mathcal{X} \subseteq \mathcal{A} \to \mathcal{B}$, by coinduction it is sufficient that $\mathcal{X}$ is a post-fixpoint of $\mathcal{F}^\perp$. So assume $E \cdot \vec{E} \in \mathcal{X}$ and $I \in \mathcal{F}(\mathcal{X})$ and show $v := I \cdot E \cdot \vec{E} \in \mathsf{SN}$ by Lemma 15. To this end, we have to show that all $\rhd_\beta$-redexes of v are SN. We distinguish the different introduction forms I.

Case $I = \mathsf{in}^{00}_{\to}(t, u')$ with $t \perp \mathcal{X}[\mathcal{A}]_\Gamma$ and $u' \perp \mathcal{X}[\mathcal{B}]_\Gamma$. We have $t[a] \perp \mathcal{X}_\Gamma$ by assumption on t and $E \cdot \vec{E} \in \mathcal{X}_\Gamma$, thus, $t[a] \cdot E \cdot \vec{E} \in \mathsf{SN}$.

Case $I = \mathsf{in}^{11}_{\to}(a, b)$ with $a \perp \mathcal{A}_\Gamma$ and $b \perp \mathcal{B}_\Gamma$. We have $u[b] \perp \mathcal{C}_\Gamma$ and $\vec{E} \in \mathcal{C}_\Gamma$, thus $u[b] \cdot \vec{E} \in \mathsf{SN}$.

Case $I = \mathsf{in}^{01}_{\to}(t, b)$. In this case we have two weak head β-redexes which we handle as in the previous cases. ◀

Plugging these lemmata into the framework of Section 3, we obtain a new proof of $\beta\pi$-SN for ITTND.

7 Conclusion

We have successfully applied Girard's method, in its original form, to prove β-SN of ITTND, and the orthogonality method to prove $\beta\pi$-SN. The applicability of established methods is reassuring that ITTND does not offer a new form of computation asking for new theoretical justifications.

Our proof using orthogonality places rather high demands on the meta-theory: non-strictly positive coinductive definitions. Neither Coq nor Agda directly support those; in Coq, though, we can always fall back to impredicativity to construct the necessary fixed-point in the lattice of term or spine sets ordered by inclusion. In Martin-Löf Type Theory (MLTT) [24], the basis of Agda, such backups do not exist. This begs the question whether non-strictly positive (co)inductive types could be added in some form to MLTT without jeopardizing its soundness.

In the appendix (Appendix A), we investigate how the SN-method of Joachimski and Matthes [21, 26] can be applied to ITTND to prove $\beta\pi$-SN without the need for impredicativity nor non-strict positivity nor CPS-translation. Whether even an arithmetical proof à la David and Nour [9, 10] works for unoptimized ITTND is unclear, since already the introduction rules for implication are recursive and thus make implication semantically an inductive type.

A further question is the computational content of the normalization arguments presented here. The double negation on the meta level employed in the biorthogonals superficially resembles the CPS translation by Geuvers, van der Giessen, and Hurkens [16], and perhaps the latter can be extracted from our normalization proof.

Finally, the classical version of TTND has been little explored so far. It is unclear whether it has a computational interpretation that enjoys the strong normalization property.

References

1 Andreas Abel. *A Polymorphic Lambda-Calculus with Sized Higher-Order Types*. PhD thesis, Ludwig-Maximilians-Universität München, 2006.

2 Agda developers. *Agda 2.6.1 documentation*, 2020. URL: `http://agda.readthedocs.io/en/v2.6.1/`.

3 Thorsten Altenkirch and Bernhard Reus. Monadic presentations of lambda terms using generalized inductive types. In Jörg Flum and Mario Rodríguez-Artalejo, editors, *Computer Science Logic, 13th Int. Wksh., CSL '99, 8th Annual Conf. of the EACSL*, volume 1683 of *Lect. Notes in Comput. Sci.*, pages 453–468. Springer, 1999. `doi:10.1007/3-540-48168-0_32`.

4 Franco Barbanera and Stefano Berardi. A symmetric lambda calculus for classical program extraction. *Inf. Comput.*, 125(2):103–117, 1996. `doi:10.1006/inco.1996.0025`.

5 Nick Benton, Chung-Kil Hur, Andrew Kennedy, and Conor McBride. Strongly typed term representations in Coq. *J. of Autom. Reasoning*, 49(2):141–159, 2012. `doi:10.1007/s10817-011-9219-0`.

6 Garrett Birkhoff. *Lattice Theory*. Amer. Math. Soc., Providence, RI, USA, 3rd edition, 1967.

7 Coq developers. The Coq proof assistant, version 8.12.0, 2019. `doi:10.5281/zenodo.2554024`.

8 Vincent Danos and Jean-Louis Krivine. Disjunctive tautologies as synchronisation schemes. In Peter Clote and Helmut Schwichtenberg, editors, *Computer Science Logic, 14th Int. Wksh., CSL 2000, 9th Annual Conf. of the EACSL*, volume 1862 of *Lect. Notes in Comput. Sci.*, pages 292–301. Springer, 2000. `doi:10.1007/3-540-44622-2_19`.

9 René David. Normalization without reducibility. *Ann. Pure Appl. Logic*, 107(1–3):121–130, 2001. `doi:10.1016/S0168-0072(00)00030-0`.

10 René David and Karim Nour. Arithmetical proofs of strong normalization results for the symmetric lambda-mu-calculus. In Pawel Urzyczyn, editor, *Proc. of the 7th Int. Conf. on Typed Lambda Calculi and Applications, TLCA 2005*, volume 3461 of *Lect. Notes in Comput. Sci.*, pages 162–178. Springer, 2005. `doi:10.1007/11417170_13`.

11 N. G. de Bruijn. Lambda calculus notation with nameless dummies, a tool for automatic formula manipulation, with application to the Church-Rosser theorem. *Indagationes Mathematicae*, 75(5):381–392, 1972. `doi:10.1016/1385-7258(72)90034-0`.

12 Gerhard Gentzen. Untersuchungen über das logische Schließen. *Mathematische Zeitschrift*, 39:176–210, 405–431, 1935. URL: `http://gdz.sub.uni-goettingen.de/`.

13 Herman Geuvers and Tonny Hurkens. Deriving natural deduction rules from truth tables. In Sujata Ghosh and Sanjiva Prasad, editors, *Proc. of the 7th Indian Conference on Logic and Its Applications*, volume 10119 of *Lect. Notes in Comput. Sci.*, pages 123–138. Springer, 2017. `doi:10.1007/978-3-662-54069-5_10`.

14 Herman Geuvers and Tonny Hurkens. Proof terms for generalized natural deduction. In Andreas Abel, Fredrik Nordvall Forsberg, and Ambrus Kaposi, editors, *23rd Int. Conf. on Types for Proofs and Programs, TYPES 2017*, volume 104 of *Leibniz Int. Proc. in Informatics*, pages 3:1–3:39. Schloss Dagstuhl, 2017. `doi:10.4230/LIPIcs.TYPES.2017.3`.

15 Herman Geuvers and Tonny Hurkens. Addendum to "Proof terms for generalized natural deduction", 2020. URL: `http://www.cs.ru.nl/~herman/PUBS/addendum_to_TYPES.pdf`.

16 Herman Geuvers, Iris van der Giessen, and Tonny Hurkens. Strong normalization for truth table natural deduction. *Fundam. Inform.*, 170(1-3):139–176, 2019. `doi:10.3233/FI-2019-1858`.

17 Jean-Yves Girard. *Interprétation fonctionnelle et élimination des coupures dans l'arithmétique d'ordre supérieur*. Thèse de Doctorat d'État, Université de Paris VII, 1972.

18 Jean-Yves Girard. Locus solum: From the rules of logic to the logic of rules. *Math. Struct. in Comput. Sci.*, 11(3):301–506, 2001. doi:10.1017/S096012950100336X.

19 Jean-Yves Girard, Yves Lafont, and Paul Taylor. *Proofs and Types*, volume 7 of *Cambridge Tracts in Theoret. Comput. Sci.* Cambridge University Press, 1989.

20 Felix Joachimski and Ralph Matthes. Standardization and confluence for a lambda calculus with generalized applications. In Leo Bachmair, editor, *Rewriting Techniques and Applications, RTA 2000, Norwich, UK*, volume 1833 of *Lect. Notes in Comput. Sci.*, pages 141–155. Springer, 2000. doi:10.1007/10721975_10.

21 Felix Joachimski and Ralph Matthes. Short proofs of normalization for the simply-typed lambda-calculus, permutative conversions and Gödel's T. *Archive of Mathematical Logic*, 42(1):59–87, 2003. doi:10.1007/s00153-002-0156-9.

22 Sam Lindley and Ian Stark. Reducibility and $\top\top$-lifting for computation types. In Pawel Urzyczyn, editor, *Proc. of the 7th Int. Conf. on Typed Lambda Calculi and Applications, TLCA 2005*, volume 3461 of *Lect. Notes in Comput. Sci.*, pages 262–277. Springer, 2005. doi:10.1007/11417170_20.

23 Zhaohui Luo. *ECC: An Extended Calculus of Constructions.* PhD thesis, University of Edinburgh, 1990. URL: https://www.cs.rhul.ac.uk/home/zhaohui/ECS-LFCS-90-118.pdf.

24 Per Martin-Löf. *Intuitionistic Type Theory.* Bibliopolis, 1984.

25 Ralph Matthes. Characterizing strongly normalizing terms of a calculus with generalized applications via intersection types. In José D. P. Rolim, Andrei Z. Broder, Andrea Corradini, Roberto Gorrieri, Reiko Heckel, Juraj Hromkovic, Ugo Vaccaro, and J. B. Wells, editors, *Intersect. Types and Related Sys. (ITRS 2000), ICALP Satellite Wksh.*, pages 339–354. Carleton Scientific, Waterloo, ON, Canada, 2000.

26 Ralph Matthes. Non-strictly positive fixed-points for classical natural deduction. *Ann. Pure Appl. Logic*, 133(1–3):205–230, 2005. doi:10.1016/j.apal.2004.10.009.

27 Michel Parigot. Proofs of strong normalization for second order classical natural deduction. *J. Symb. Logic*, 62(4):1461–1479, 1997. doi:10.2307/2275652.

28 Michel Parigot. Strong normalization of second order symmetric λ-calculus. In Sanjiv Kapoor and Sanjiva Prasad, editors, *FST TCS 2000: Foundations of Software Technology and Theoretical Computer Science*, volume 1974 of *Lect. Notes in Comput. Sci.*, pages 442–453. Springer, 2000. doi:10.1007/3-540-44450-5_36.

29 Andrew M. Pitts. Parametric polymorphism and operational equivalence. *Math. Struct. in Comput. Sci.*, 10(3):321–359, 2000. URL: http://journals.cambridge.org/action/displayAbstract?aid=44651.

30 William W. Tait. Intensional interpretations of functionals of finite type I. *J. Symb. Logic*, 32(2):198–212, 1967. doi:10.2307/2271658.

31 Alfred Tarski. A lattice-theoretical fixpoint theorem and its applications. *Pacific Journal of Mathematics*, 5:285–309, 1955.

32 Jérôme Vouillon and Paul-André Melliès. Semantic types: A fresh look at the ideal model for types. In Neil D. Jones and Xavier Leroy, editors, *Proc. of the 31st ACM Symp. on Principles of Programming Languages, POPL 2004*, pages 52–63. ACM Press, 2004. doi:10.1145/964001.964006.

A Saturated Sets

In this appendix, we show how to adapt the original *saturated sets* method to IITND, first just for β-SN, then including π-reductions.

A.1 Saturated Sets for Computation Reductions

In the following, we adapt Tait's method of saturated sets to show β-SN for ITTND. This is a variation of the proof by Geuvers and Hurkens [14].

We first observe that the set SN contains a weak-head redex already when (1) all of its reducts are SN and (2) its *lost terms* are SN, where a lost term is a subterm that could get dropped by all of the weak-head reductions. This fact is made precise by the following lemma:

▶ **Lemma 23.** *The following implications, written as rules, are valid closure properties of* SN*:*

$$\frac{t_1[a] \cdot \mathsf{el}^{10}_{\to}(a,u) \cdot \vec{E} \in \mathsf{SN} \qquad t_2 \in \mathsf{SN}}{\mathsf{in}^{00}_{\to}(t_1,t_2) \cdot \mathsf{el}^{10}_{\to}(a,u) \cdot \vec{E} \in \mathsf{SN}}$$

$$\frac{t[a] \cdot \mathsf{el}^{10}_{\to}(a,u) \cdot \vec{E} \in \mathsf{SN} \qquad u[b] \cdot \vec{E} \in \mathsf{SN} \qquad b \in \mathsf{SN}}{\mathsf{in}^{01}_{\to}(t,b) \cdot \mathsf{el}^{10}_{\to}(a,u) \cdot \vec{E} \in \mathsf{SN}} \qquad \frac{u[b] \cdot \vec{E} \in \mathsf{SN} \qquad a_1, a_2, b \in \mathsf{SN}}{\mathsf{in}^{11}_{\to}(a_1,b) \cdot \mathsf{el}^{10}_{\to}(a_2,u) \cdot \vec{E} \in \mathsf{SN}}$$

(Spine $\vec{E}$ may be empty in all cases.)

Proof. Each of these implications is proven by induction on the premises, establishing that the possible reducts of the term in the conclusion are SN. The weak-head reduct(s) are covered by the premises in each case. Reductions in lost terms are covered by the extra SN hypotheses. Reductions in preserved terms are covered by the main SN hypotheses. (This includes reductions in the spine $\vec{E}$.)

For example, consider the case for $\mathsf{in}^{00}_{\to}$: By induction on $t_1[a] \cdot \mathsf{el}^{10}_{\to}(a,u) \cdot \vec{E} \in \mathsf{SN}$ and $t_2 \in \mathsf{SN}$ show $t' \in \mathsf{SN}$ given $\mathsf{in}^{00}_{\to}(t_1,t_2) \cdot \mathsf{el}^{10}_{\to}(a,u) \cdot \vec{E} \longrightarrow t'$.

Case $t' = t_1[a] \cdot \mathsf{el}^{10}_{\to}(a,u) \cdot \vec{E}$. Then $t' \in \mathsf{SN}$ by assumption.

Case $t' = \mathsf{in}^{00}_{\to}(t_1,t_2') \cdot \mathsf{el}^{10}_{\to}(a,u) \cdot \vec{E}$ where $t_2 \longrightarrow t_2'$. Then $t' \in \mathsf{SN}$ by induction hypothesis $t_2' \in \mathsf{SN}$.

Case $t' = \mathsf{in}^{00}_{\to}(t_1',t_2) \cdot \mathsf{el}^{10}_{\to}(a',u') \cdot \vec{E}'$ where $(t_1,a,u,\vec{E}) \longrightarrow (t_1',a',u',\vec{E}')$ (a single reduction in one of these subterms). Then $t_1[a] \cdot \mathsf{el}^{10}_{\to}(a,u) \cdot \vec{E} \longrightarrow^{+} t_1'[a'] \cdot \mathsf{el}^{10}_{\to}(a',u') \cdot \vec{E}'$ (several steps possible, e.g., if reduction was in a and t_1 mentions the 0th de Bruijn index). Thus, $t' \in \mathsf{SN}$ by induction hypothesis on $t_1'[a'] \cdot \mathsf{el}^{10}_{\to}(a',u') \cdot \vec{E}' \in \mathsf{SN}$. ◀

Mimicking Lemma 23, the *saturation* $\overline{\mathcal{A}}$ of a term set is – in the case of the implicational fragment of ITTND – defined inductively as follows:

$$\frac{t \in \mathcal{A}_\Gamma}{t \in \overline{\mathcal{A}}_\Gamma} \qquad \frac{t_1[a] \cdot \mathsf{el}^{10}_{\to}(a,u) \cdot \vec{E} \in \overline{\mathcal{A}}_\Gamma \qquad t_2 \in \mathsf{SN}}{\mathsf{in}^{00}_{\to}(t_1,t_2) \cdot \mathsf{el}^{10}_{\to}(a,u) \cdot \vec{E} \in \overline{\mathcal{A}}_\Gamma}$$

$$\frac{t[a] \cdot \mathsf{el}^{10}_{\to}(a,u) \cdot \vec{E} \in \overline{\mathcal{A}}_\Gamma \qquad u[b] \cdot \vec{E} \in \overline{\mathcal{A}}_\Gamma \qquad b \in \mathsf{SN}}{\mathsf{in}^{01}_{\to}(t,b) \cdot \mathsf{el}^{10}_{\to}(a,u) \cdot \vec{E} \in \overline{\mathcal{A}}_\Gamma} \qquad \frac{u[b] \cdot \vec{E} \in \overline{\mathcal{A}}_\Gamma \qquad a_1, a_2, b \in \mathsf{SN}}{\mathsf{in}^{11}_{\to}(a_1,b) \cdot \mathsf{el}^{10}_{\to}(a_2,u) \cdot \vec{E} \in \overline{\mathcal{A}}_\Gamma}$$

▶ **Lemma 24.** $\overline{\mathsf{SN}} \subseteq \mathsf{SN}$.

Proof. We show $t \in \mathsf{SN}$ by induction on $t \in \overline{\mathsf{SN}}$, using Lemma 23. ◀

▶ **Corollary 25.** *If* $\mathcal{A} \subseteq \mathsf{SN}$ *then* $\overline{\mathcal{A}} \subseteq \mathsf{SN}$.

Proof. Since closure is a monotone operator, we have $\overline{\mathcal{A}} \subseteq \overline{\mathsf{SN}} \subseteq \mathsf{SN}$ by Lemma 24. ◀

A *saturated set* $\mathcal{A} \in \mathsf{SAT}$ must fulfill the following three properties:
SAT1 $\mathcal{A} \subseteq \mathsf{SN}$ (contains only SN terms).
SAT2 If $\vec{E} \in \mathsf{SN}$ then $x \cdot \vec{E} \in \mathcal{A}$ (contains SN neutrals).
SAT3 $\overline{\mathcal{A}} \subseteq \mathcal{A}$ (closed under SN weak-head expansion).

Semantic implication can now be defined as:

$$f \in (\mathcal{A} \to \mathcal{B})_\Gamma \iff f \in \mathsf{SN} \text{ and } \forall \mathcal{C} \in \mathsf{SAT},\ \tau : \Delta \leq \Gamma,\ a \in \mathcal{A}_\Delta,\ t \in \mathcal{C}[\mathcal{B}]_\Delta.\ f\tau \cdot \mathsf{el}^{10}_{\to}(a, t) \in \mathcal{C}_\Delta.$$

▶ **Lemma 26** (Function space on SAT)**.** *If* $\mathcal{A} \subseteq \mathsf{SN}$ *and* $\mathcal{B} \in \mathsf{SAT}$, *then* $\mathcal{A} \to \mathcal{B} \in \mathsf{SAT}$.

Proof. SAT1 holds by definition. SAT2 holds by SAT2 of $\mathcal{B}$. SAT3 holds by SAT3 of $\mathcal{B}$. ◀

The introductions rules for implication are indeed modeled for the SAT variant of semantic function space. For instance, $\mathsf{in}^{01}_{\to}$:

▶ **Lemma 27** (Introduction ($\mathsf{in}^{01}_{\to}$))**.** *If* $t \in (\mathcal{A} \to \mathcal{B})[\mathcal{A}]_\Gamma$ *and* $b \in \mathcal{B}_\Gamma$ *then* $\mathsf{in}^{01}_{\to}(t, b) \in (\mathcal{A} \to \mathcal{B})_\Gamma$.

Proof. Assume $\mathcal{C} \in \mathsf{SAT}$ and $\tau : \Delta \leq \Gamma$ and $a \in \mathcal{A}_\Delta$ and $u \in \mathcal{C}[\mathcal{B}]_\Delta$ and show $\mathsf{in}^{01}_{\to}(t, b)\tau \cdot \mathsf{el}^{10}_{\to}(a, u) \in \mathcal{C}_\Delta$. Using SAT3 on $\mathcal{C}$, it is sufficient to show that (1) $t(\tau.a) \cdot \mathsf{el}^{10}_{\to}(a, u) \in \mathcal{C}_\Delta$ and (2) $u[b\tau] \in \mathcal{C}_\Delta$ and (3) $b\tau \in \mathsf{SN}$. Subgoals (2) and (3) follow since $b\tau \in \mathcal{B}_\Delta$, and (1) holds since $t(\tau.a) \in (\mathcal{A} \to \mathcal{B})_\Delta$. ◀

A.2 On Permutation Reductions

Ralph Matthes' [26] formulation of saturated sets in the context of π-reductions can also be adapted to ITTND.

First, we observe that Lemma 23 still holds if π-reductions are taken into account. This is because any reduction in the spine of a conclusion can be simulated in the spine of at least one of the premises.

Thus, SAT3 can remain in place, only SAT2 needs to be reformulated, since a neutral $x \cdot \vec{E}$ can be subject to a β-reduction after a π-reduction in $\vec{E}$ has created a new β-redex. Towards a reformulation of SAT2, we observe the following closure properties of SN by neutral terms:

▶ **Lemma 28** (Neutral closure of SN)**.** *The following implications, written as rules, are valid closure properties of* SN*:*

$$\frac{}{x \in \mathsf{SN}} \qquad \frac{a \in \mathsf{SN} \qquad u \in \mathsf{SN}}{x \cdot \mathsf{el}^{10}_{\to}(a, u) \in \mathsf{SN}} \qquad \frac{x \cdot E_1\{E_2\} \cdot \vec{E} \in \mathsf{SN} \qquad E_2 \cdot \vec{E} \in \mathsf{SN}}{x \cdot E_1 \cdot E_2 \cdot \vec{E} \in \mathsf{SN}}$$

The extra assumption $E_2 \cdot \vec{E} \in \mathsf{SN}$ in the third implication is equivalent to $y \cdot E_2 \cdot \vec{E} \in \mathsf{SN}$ for some variable y. In the implicational fragment, this assumption is redundant since the composition $\mathsf{el}^{10}_{\to}(a, u)\{E_2\} = \mathsf{el}^{10}_{\to}(a, u \cdot E_2\uparrow)$ does not lose E_2. In particular, any reduction in $E_2 \cdot \vec{E}$ can be replayed in $x \cdot E_1\{E_2\} \cdot \vec{E}$. However, in general there can be eliminations with only positive premises, such as $\mathsf{el}^{1}_{\neg}(a)$ for negation, where composition $\mathsf{el}^{1}_{\neg}(a)\{E_2\} = \mathsf{el}^{1}_{\neg}(a)$

simply drops E_2. This means that reductions in part $E_2 \cdot \vec{E}$ of $x \cdot E_1 \cdot E_2 \cdot \vec{E}$ cannot necessarily be simulated in $x \cdot E_1\{E_2\} \cdot \vec{E}$. In particular, a reduction $E_2 \cdot E_3 \longrightarrow_\pi E_2\{E_3\}$ could lead to new β-redexes which have no correspondence in $E_1\{E_2\} \cdot E_3$.

Mimicking Lemma 28, we *extend* the definition of saturation $\overline{\mathcal{C}}$ of a semantic type $\mathcal{C}$ for C by the following three clauses:

$$\textsc{var}\ \frac{x : \Gamma \vdash C}{x \in \overline{\mathcal{C}}_\Gamma} \qquad \textsc{el}\ \frac{x : \Gamma \vdash A \to B \qquad a \in \mathsf{SN}(\Gamma \vdash A) \qquad u \in \overline{\mathcal{C}}_{\Gamma.B}}{x \cdot \mathsf{el}^{10}_{\to}(a, u) \in \overline{\mathcal{C}}_\Gamma}$$

$$\textsc{pi}\ \frac{\begin{array}{ccc} x : \Gamma \vdash A & E_1 : \Gamma \mid A \vdash B & x \cdot E_1\{E_2\} \cdot \vec{E} \in \overline{\mathcal{C}}_\Gamma \\ \tau : \Delta \le \Gamma & y : \Delta \vdash B & y \cdot (E_2 \cdot \vec{E})\tau \in \overline{\mathcal{C}}_\Delta \end{array}}{x \cdot E_1 \cdot E_2 \cdot \vec{E} \in \overline{\mathcal{C}}_\Gamma}$$

Note that a premise such as $y \cdot (E_2 \cdot \vec{E})\tau \in \mathsf{SN}$ would be too weak to show that semantic function space is saturated.

We revise the definition of SAT such that SAT3 uses the extended definition of closure, obsoleting SAT2.

▶ **Lemma 29** (Function space on SAT). *If $\mathcal{A} \subseteq \mathsf{SN}$ and $\mathcal{B} \in \mathsf{SAT}$, then $\mathcal{A} \to \mathcal{B} \in \mathsf{SAT}$.*

Proof. We shall focus on the new closure conditions for SAT:

- VAR: Show $x \in (\mathcal{A} \to \mathcal{B})_\Gamma$. Clearly $x \in \mathsf{SN}$. Now assume $\mathcal{C} \in \mathsf{SAT}$ and $\tau : \Delta \le \Gamma$ and $a \in \mathcal{A}_\Delta$ and $u \in \mathcal{C}[\mathcal{B}]_\Delta$ and show $x\tau \cdot \mathsf{el}^{10}_{\to}(a, u) \in \mathcal{C}_\Delta$. By EL, it is sufficient that $a \in \mathsf{SN}$ and $u \in \mathcal{C}_{\Delta.B}$. By VAR we have $\mathsf{x}_0 \in \mathcal{B}_{\Delta.B}$, thus $u(\uparrow.\mathsf{x}_0) = u \in \mathcal{C}_{\Delta.B}$.
- EL: Assume $x : \Gamma \vdash A_0 \to B_0$ and $a_0 \in \mathsf{SN}(\Gamma \vdash A_0)$ and $u_0 \in \overline{\mathcal{A} \to \mathcal{B}}_{\Gamma.B_0}$ and show $x \cdot \mathsf{el}^{10}_{\to}(a_0, u_0) \in \overline{\mathcal{A} \to \mathcal{B}}_\Gamma$. First, $x \cdot \mathsf{el}^{10}_{\to}(a_0, u_0) \in \mathsf{SN}$.
  Further, assume $\mathcal{C} \in \mathsf{SAT}$ and $\tau : \Delta \le \Gamma$ and $a \in \mathcal{A}_\Delta$ and $u \in \mathcal{C}[\mathcal{B}]_\Delta$ and show $(x \cdot \mathsf{el}^{10}_{\to}(a_0, u_0))\tau \cdot \mathsf{el}^{10}_{\to}(a, u) \in \mathcal{C}_\Delta$. Using PI, we first discharge the last subgoal $\mathsf{x}_0 \cdot \mathsf{el}^{10}_{\to}(a, u){\uparrow} \in \mathcal{C}_{\Delta.(A \to B)}$ by EL for $\mathcal{C}$ with $a{\uparrow} \in \mathcal{A}_{\Delta.(A \to B)}$ and $u(\Uparrow{\uparrow}) \in \mathcal{C}_{\Delta.(A \to B).B}$.
  It remains to show that $x\tau \cdot \mathsf{el}^{10}_{\to}(a_0\tau, u_0(\Uparrow \tau) \cdot \mathsf{el}^{10}_{\to}(a, u){\uparrow}) \in \mathcal{C}_\Delta$. Again, we use EL for $\mathcal{C}$. Clearly $a_0\tau \in \mathsf{SN}$, so it remains to show that $u_0(\Uparrow \tau) \cdot \mathsf{el}^{10}_{\to}(a{\uparrow}, u(\Uparrow{\uparrow})) \in \mathcal{C}_{\Delta.B_0}$. Since $u_0(\Uparrow \tau) \in (\mathcal{A} \to \mathcal{B})_{\Delta.B_0}$ and $a{\uparrow} \in \mathcal{A}_{\Delta.B_0}$ and $u(\Uparrow{\uparrow}) \in \mathcal{C}[\mathcal{B}]_{\Delta.B_0}$, this is the case by definition of $\mathcal{A} \to \mathcal{B}$.
- PI: The case PI for $\mathcal{A} \to \mathcal{B}$ is shown by PI for $\mathcal{C}$ (what $\mathcal{C}$ refers to, see the previous cases). This part is a bit tedious to spell out, but completely uninteresting, since just $\vec{E}$ is extended by another $\mathsf{el}^{10}_{\to}$-elimination at the end. ◀

The soundness of the introductions carries over from the previous section (Lemma 27) since the saturated sets are still closed by weak head expansion.

This concludes the $\beta\pi$-SN proof for ITTND using saturated sets.