Strong normalization in core type theory

David Ripley
Monash University
davewripley@gmail.com

Abstract

This paper presents a novel typed term calculus and reduction relation for it, and proves that the reduction relation is strongly normalizing—that there are no infinite reduction sequences. The calculus bears a close relation to the $\rightarrow, \neg$ fragment of core logic, and so is called 'core type theory'.

This paper presents a novel typed term calculus and reduction relation for it, and proves that the reduction relation is strongly normalizing—that there are no infinite reduction sequences. The calculus is similar to the simply-typed lambda calculus with an empty type, but with a twist. The simply-typed lambda calculus with an empty type bears a close relation to the $\rightarrow, \bot$ fragment of intuitionistic logic ([Howard, 1980; Scherer, 2017; Sørensen and Urzyczyn, 2006]); the calculus to be presented here bears a similar relation to the $\rightarrow, \neg$ fragment of a logic known as *core logic*. Because of this connection, I'll call the calculus *core type theory*.

Core logic (fka 'intuitionistic relevant logic') has been developed and studied primarily by Neil Tennant, in a series of papers spanning recent decades. (See eg [Petrolo and Pistone, 2019; Tennant, 1979, 2002, 2017].) One interesting feature of core logic is that its valid arguments are not closed under the rule of cut. That is, there are core valid arguments $[\Gamma \succ A]$ and $[A, \Delta \succ B]$ such that $[\Gamma, \Delta \succ B]$ is not core valid. However, in any such case, there is some subsequent of $[\Gamma, \Delta \succ B]$ that is core valid. Tennant calls this latter property *epistemic gain*, and maintains that usual motivations for closure under cut are at least as well served by epistemic gain.

This paper does not directly take a stand on that issue. However, at least one going motivation for cut is its connection to computational properties of a system, and in particular to reductions in related term calculi. For example, this is the connection Girard has in mind in saying that a "sequent calculus without cut-elimination is like a car without [an] engine" [Girard, 1995]. So in evaluating Tennant's defense of core logic via epistemic gain, it would be useful to know what the situation is in related term calculi. This paper aims to shed light on that issue, by exploring some of the properties of core type theory.

1 Core logic

Although core logic is typically presented as a full first-order logic, this paper only studies its propositional $\rightarrow, \neg$ fragment. As such, I won't present core logic in full here,

$$\to\text{I}^n: \quad \dfrac{\begin{matrix}[\varphi]^n \\ \vdots \\ \psi\end{matrix}}{\varphi \to \psi} \qquad \to\text{I!}^n: \quad \dfrac{\begin{matrix}[\varphi]^n \\ \vdots \\ \frownie\end{matrix}}{\varphi \to \psi} \qquad \to\text{E}: \quad \dfrac{\varphi \to \psi \qquad \varphi \qquad \begin{matrix}[\psi]^n \\ \vdots \\ \theta\end{matrix}}{\theta}$$

$$\neg\text{I}^n: \quad \dfrac{\begin{matrix}[\varphi]^n \\ \vdots \\ \frownie\end{matrix}}{\neg\varphi} \qquad \neg\text{E}: \quad \dfrac{\neg\varphi \qquad \varphi}{\frownie}$$

In the rules →I! and ¬I, discharge may not be vacuous. In the rule →I, it may be vacuous.

Figure 1: Core natural deduction for intutionistic logic

just the needed fragment. Similarly, discussions of intuitionistic logic, which is closely related, will also focus on the propositional $\to, \neg$ fragment. I will work with the natural deduction system presented in fig. 1.

Since we're working in a fragment of the language without any falsum connective, there are questions about how to handle negation. We do so via ☹; this is not a formula or connective in its own right (and so cannot be used to form complex formulas), but rather a structural marker that interacts with the connective rules in the specified way. Not all nodes in a proof, then, must be occupied by formulas. Some can be occupied by the structural marker ☹ instead. However, while ☹ may appear in the course of a proof, it may not be assumed; only formulas are eligible for assumption.

For reasons that will become apparent later, I will use the term 'hat' to pick out candidate occupants of proof nodes. That is, every formula is a hat, and ☹ is a hat, and nothing else is a hat. I use Greek letters φ, ψ for formulas, and $\mathfrak{C}, \mathfrak{D}$ for hats. It is useful to consider hats as ordered, with $\mathfrak{C} \leq \mathfrak{D}$ iff either $\mathfrak{C}$ is ☹ or $\mathfrak{C} = \mathfrak{D}$.

With that qualification understood, but otherwise read straightforwardly, this natural deduction system determines not core logic but intuitionistic logic.

Definition 1. For a set Γ of formulas and any $\mathfrak{C}$, we say $\Gamma \vdash \mathfrak{C}$ iff there is a proof of $\mathfrak{C}$ in the system of fig. 1 whose open assumptions are all in Γ.

Theorem 1. *The proof system in fig. 1 determines intuitionistic logic. That is,* $\Gamma \vdash \varphi$ *iff* $\Gamma \vdash_{Int} \varphi$*; and* $\Gamma \vdash$ ☹ *iff* $\Gamma \vdash_{Int}$.

Proof. It should be clear that the system does not prove anything that is intuitionistically unprovable. Note for later in the proof: this means that there is no proof of ☹ without open assumptions, since such a proof would require proofs with no open assumptions of both $\neg\varphi$ and φ for some φ, but intuitionistic logic is consistent. It remains to show that the system proves enough.

→I and →E together are usual rules for intuitionistic implication. ¬I and ¬E together are *almost* usual rules for intuitionistic negation; the difference is the prohibition on vacuous discharge in ¬I. So it is enough to show that an unrestricted version of ¬I is derivable in this system.

Suppose, then, that we have some proof Π of ☹, with an aim to proving $\neg\varphi$ regardless of whether φ is among the open assumptions of Π. As we've observed, Π must have some open assumption or other; say ψ is one. Let Π' be the proof of $\psi \to \neg\varphi$ arrived at by extending Π with a step of $\to$I!, discharging the occurrences of ψ open in Π. Then we can proceed as follows:

$$\to\mathrm{E}^n\!: \quad \dfrac{\begin{matrix}\Pi' \\ \psi \to \neg\varphi\end{matrix} \qquad \psi \qquad [\neg\varphi]^n}{\neg\varphi}$$

The overall proof arrived at has exactly the same open assumptions as Π, and is a proof of $\neg\varphi$, regardless of whether φ is among the open assumptions of Π. □

Why give such a strange proof system for good old intuitionistic logic? Because this system makes it particularly simple to reach core logic as well. To do this, we impose an additional restriction, which I will call the *core restriction*.

Definition 2. A proof meets the *core restriction* iff in each application of $\to$E and $\neg$E in the proof, the major premise of the application is itself assumed, rather than following from another rule.[1] A proof is a *core proof* iff it meets the core restriction.

For a set Γ of formulas and a formula φ, we say $\Gamma \vdash^{-} \varphi$ iff there is a core proof of φ whose open assumptions are all in Γ.

Not everything provable in the total system has a core proof. (Note that the crucial derivation invoked in the proof of theorem 1 is not core.) Core logic is the logic determined by core proofs.

Example 1. $\neg\varphi, \varphi \vdash \psi$, but $\neg\varphi, \varphi \nvdash^{-} \psi$. Here is a proof establishing the first claim:

$$\to\mathrm{E}^2\!: \quad \dfrac{\to\mathrm{I}!^1\!: \dfrac{\neg\mathrm{E}\!: \dfrac{\neg\varphi \qquad [\varphi]^1}{\frownie}}{\varphi \to \psi} \qquad \varphi \qquad [\psi]^2}{\psi}$$

Note that the proof is not core, since the major premise for $\to$E is not an assumption.

To see that there is no core proof of the same, note first that there are no implications in the conclusion of this proof. Since no implication introduced in the course of a core proof can ever be eliminated, this must mean that the rules $\to$I and $\to$I! are not involved in any core proof with this conclusion. Similar reasoning shows that $\neg$I cannot be involved either. But if $\to$I! and $\neg$I are neither of them involved, then $\neg$E cannot be involved, since it would bring a ☹ into the proof, and $\to$I! and $\neg$I are the only rules that can continue on from a ☹. So any purported core proof for this argument must consist entirely of $\to$E, and as such must leave some assumption open of the form $\rho \to \theta$. But neither premise of this argument has such a form; so there is no such proof.

It should be noted that this proof system for core logic is not the exact system presented and studied by Tennant in eg [Tennant, 2017]. In Tennant's system, any occurrence of any assumption that can be discharged by a rule application *must* be discharged

[1] In $\to$E, the major premise is the displayed $\varphi \to \psi$; and in $\neg$E, the major premise is the displayed $\neg\varphi$.

by that rule application. I have not imposed this restriction. This means that core proofs as Tennant defines them are not closed under substitution, since a proof that violates this restriction can be a substitution instance of a proof that meets it. For this reason, I have here dropped the restriction. However, this does not affect which arguments have core proofs; it only affects how many proofs they have. This is because while *proofs* are not closed under substitution when Tennant's restriction is imposed, *provability* still is. So closing proofs themselves under substitution, which is the effect of relaxing this restriction, does not affect provability.[2,3]

Finally, it's worth noting a key relation between intuitionistic logic and core logic, and between these proof systems for the logics. (For more, see [Tennant, 2002, 2015].)

Theorem 2. *Any proof of* $\mathfrak{C}$ *with open assumptions* Γ *can be normalized into a core proof of* $\mathfrak{D}$ *with open assumptions* Δ*, for some* $\mathfrak{D}, \Delta$ *with* $\mathfrak{D} \leq \mathfrak{C}$ *and* $\Delta \subseteq \Gamma$.

It follows from this that whenever $\Gamma \vdash \varphi$, either $\Gamma \vdash^{-} \varphi$ or $\Gamma \vdash^{-} ☹$, and moreover that $\Gamma \vdash ☹$ iff $\Gamma \vdash^{-} ☹$. So core logic matches intuitionistic logic on the consequences of consistent sets, and it matches intuitionistic logic in its understanding of which sets are consistent in the first place. The only differences between intuitionistic validity and core validity are in what follows from inconsistent sets. Intuitionistically, everything follows; this is not so in core logic.

2 Core type theory

2.1 Types and hats

The propositions of core logic will serve as the types of core type theory. There will also be need of a slight generalisation of types, what I will call *hats*. A *hat* is either a type or else ☹.[4] I will continue to use lowercase Greek letters to indicate propositions (and so types); for hats I use $\mathfrak{C}, \mathfrak{D}$. Hats are considered to be ordered: $\mathfrak{C} \leq \mathfrak{D}$ iff either $\mathfrak{C} = \mathfrak{D}$ or $\mathfrak{C} = ☹$.

Each term in core type theory wears a (unique) hat.[5] If the term's hat is a type, the term is *typed*; if the hat is ☹, the term is *exceptional*. Following usual interpretations of the Curry-Howard correspondence (eg [Sørensen and Urzyczyn, 2006]), terms can be understood as programs. When the term's hat is a type φ, this indicates that if the program is successfully run its output will be data of that type. When the term's hat is ☹, this indicates that if the program is run it will not be successful.

This requires interpretations of the complex types $\varphi \to \psi$ and $\neg\varphi$. Implications are interpreted as function types. A function of type $\varphi \to \psi$ awaits an input of type φ, and

[2] Thanks to Neil Tennant (pc) for discussion on this point.

[3] A preview and a conjecture: this means that the corresponding restriction in the term system to follow would not affect which types are inhabited, but only how many inhabitants they have. I would conjecture that the term calculus that corresponds to Tennant's actual system, with this extra discharge restriction imposed, is the fragment of the system presented in section 2 involving only one variable of each type, rather than denumerably many.

[4] Just as in the proof system of fig. 1, note that $\varphi \to ☹$, $\neg ☹$, and so on are not well-formed. The only way ☹ can appear in a hat is alone. $\to$ and $\neg$ operate on *types*, and ☹ is not a type.

[5] This is thus a 'Church-style' and not a 'Curry-style' calculus, in the language of [Sørensen and Urzyczyn, 2006, p. 63].

if run successfully with such an input, it produces an output of type ψ. Negations are interpreted as failures triggered by the presence of some other data. A term of type $\neg\varphi$ awaits an input of type φ, and if it receives such an input it fails to run successfully.

For now, these explanations are just intuitive indications. They will be made precise in sections 2.2 and 2.4.

2.2 Terms

Terms (with their hats) are defined inductively as follows. Here and throughout, where I omit a hat on a term, either it can be inferred or I am speaking in generality. For a term M, $\texttt{FV}(M)$ is the set of free variables in M; this is defined as usual. These term-forming clauses are directly determined by copying the proof rules of fig. 1, with variables standing for assumptions.

Definition 3 (Terms)**.**

- There's a countable infinity of variables $x^\varphi, y^\varphi, \ldots$ of each type φ.
- Given $M^{\varphi\to\psi}$ and N^φ, we have $(M\,N)^\psi$.
- Given $M^{\neg\varphi}$ and N^φ, we have $(M\,N)^{☹}$
- Given x^φ and M^ψ, we have $(\lambda x.M)^{\varphi\to\psi}$, in which any and all free occurrences of x in M are bound.
- Given x^φ and $M^{☹}$ with x free, we have $(\lambda x.M)^{\varphi\to\psi}$ and $(\lambda x.M)^{\neg\varphi}$, in which all free occurrences of x in M are bound.

Some comments on this definition are in order. First, note that there are no variables with ☹ as a hat. Variables must be *typed*, not merely hatted. Second, note that there is never any restriction on binding multiple occurrences of the same variable; this is always fine. Third, note that *vacuous* binding is sometimes allowed and sometimes not. Vacuously binding into a *typed* term is fine, but vacuously binding into an exceptional term is not possible. Fourth, note that $(\lambda x.M)^{\varphi\to\psi}$ and $(\lambda x.M)^{\neg\varphi}$ are distinct terms (when they are well-formed), even though they differ only in their hats.

In everything that follows, terms are everywhere identified up to α-conversion (relettering of bound variables). These term-formation rules can be seen as analogous to the natural deduction rules of fig. 1, with the difference that I've here chosen the term-formation rule analogous to a more usual formulation of →E.

2.3 Substitution

Substitution (of a term for a variable) is defined as usual. It is well-defined iff the term's hat matches the type of the variable it is being substituted for. Since there are no exceptional variables, exceptional terms cannot be substituted for anything. I write $M[x \mapsto N]$ to indicate the term that results from substituting N for each free occurrence of x in M.

2.4 Reduction

2.4.1 Redexes and reducts

A *redex* is a term of the form $(\lambda x.M)N$, a lambda abstract applied to an argument. In any redex, the hat on N matches the hat on x, and so $M[x \mapsto N]$ is defined; this is the *reduct* of the redex.

There are two things to notice here:

- The free variables in a redex are a superset of the free variables in its reduct. The superset is possibly proper, owing to the possibility of vacuous binding: if x is not free in M, then N's free variables may not occur at all in $M[x \mapsto N]$.
- The hat on a redex is $\geq$ the hat on its reduct. The order is possibly proper: $((\lambda x.M^{☹})^{\varphi\to\psi} N)^{\psi}$ has as its reduct $(M^{☹}[N \mapsto x])^{☹}$.

The second remark here reveals that all is not as usual. Already we can see that core type theory fails to exhibit one usual property of type term calculi, variously called 'preservation' or 'subject reduction'. (See eg [Barthe and Melliès, 1996; Harper, 2016].) Typed redexes can have exceptional reducts. However, the second remark also shows that the situation is not entirely unconstrained, at least for redexes and their reducts. We can never move from one type to another, or from ☹ to a type.

Definition 4. In a redex $(\lambda x.M)N$, if x does not occur free in M, the redex is a *vacuous* redex. If M is $M^{☹}$, the redex is an *explosive* redex.

Note that no redex can be both vacuous and explosive, although some are neither.

2.4.2 One-step reduction

This subsubsection defines the relation $\rhd_{1\beta}$ of *one-step* reduction between terms. To begin: if M is a redex and M' its reduct, then $M \rhd_{1\beta} M'$.

In more usual calculi, such as the simply-typed lambda calculus, reduction is a *compatible* relation; if $M \rhd_{1\beta} M'$, then $O(M) \rhd_{1\beta} O(M')$. In such calculi, then, we can reduce a complex term containing a redex simply by reducing the redex itself, leaving the rest alone. Indeed, this is required for a calculus to be a term rewriting system, in the sense of [Baader and Nipkow, 1998; Terese, 2003].

In core type theory, however, this is not possible.[6] There are two reasons for this. First, we can have $M \rhd_{1\beta} M'^{☹}$ where $x \notin \mathtt{FV}(M')$ and either $x \in \mathtt{FV}(M)$ or M is M^{φ}. In either case, $\lambda x.M$ is well-formed but $\lambda x.M'$ is not. In $\lambda x.M$ either the binding is not vacuous or M is not exceptional, so there is no problem. But $\lambda x.M'$ attempts to vacuously bind into an exceptional term, which is not possible. So we cannot reduce terms underneath a lambda without exercising some care.

Second, in terms of the form MN, both M and N must be typed. If $M \rhd_{1\beta} M'^{☹}$, then $M'N$ is not well-formed; and if $N \rhd_{1\beta} N'^{☹}$, then MN' is not well-formed. So we

[6] And so core type theory, despite involving terms with familiar-seeming structure, is not a term rewriting system. Despite this, I have borrowed some language, such as 'redex', from the theory of term rewriting systems, since this language applies just as well to core type theory. Core type theory is still an abstract reduction system in the sense of [Baader and Nipkow, 1998; Terese, 2003].

cannot reduce either term in an application without exercising some care. As a result of these situations, the needed definition of one-step reduction is less straightforward than usual, and is given by recursion on the structure of the term being reduced.

Definition 5 (One-step reduction)**.**

- If M is a redex and M' its reduct, then $M \rhd_{1\beta} M'$
- Reducing M in MN:
  - If $M^{\varphi} \rhd_{1\beta} M'^{\varphi}$, then $MN \rhd_{1\beta} M'N$
  - If $M \rhd_{1\beta} M'^{\frownie}$, then $MN \rhd_{1\beta} M'$
- Reducing N in MN:
  - If $N^{\varphi} \rhd_{1\beta} N'^{\varphi}$, then $MN \rhd_{1\beta} MN'$
  - If $N \rhd_{1\beta} N'^{\frownie}$, then $MN \rhd_{1\beta} N'^{\frownie}$
- Reducing M in $\lambda x.M$:
  - If $M^{\varphi} \rhd_{1\beta} M'^{\varphi}$, then $\lambda x.M \rhd_{1\beta} \lambda x.M'$
  - If $M \rhd_{1\beta} M'^{\frownie}$,
    - if $x \in \mathtt{FV}(M')$, then $\lambda x.M \rhd_{1\beta} \lambda x.M'$ (preserving hat[7])
    - if $x \notin \mathtt{FV}(M')$, then $\lambda x.M \rhd_{1\beta} M'$

The strategy of this definition is straightforward: if it is possible to reduce a subterm in place without changing the context, then that's what's done. So when $M \rhd_{1\beta} M'$, if $O(M)$ and $O(M')$ are both well-formed, then indeed $O(M) \rhd_{1\beta} O(M')$. That much of compatibility stands. When this is not possible, because the result would not be well-formed, then the subterm being reduced is retained, and its immediate context discarded. There are no choices in this process, other than the initial choice of a redex to reduce. So given a term with a redex in it, there is a unique result of reducing the term at that redex.

It can be verified by inspection of this definition that the two preservation properties indicated above for redexes and their reducts extend to $\rhd_{1\beta}$. That is, where $M^{\mathfrak{C}} \rhd_{1\beta} N^{\mathfrak{D}}$, then $\mathtt{FV}(M) \supseteq \mathtt{FV}(N)$ and $\mathfrak{C} \geq \mathfrak{D}$. (That these preservation properties hold is required for definition 5 to work, but it is straightforward to see that they do.)

Some examples will help give the flavour of this definition.

Example 2. $\left((\lambda y^{\varphi}.(x^{\neg\varphi} y^{\varphi})^{\frownie})^{\varphi\to\theta} z^{\varphi}\right)^{\theta}$ is a redex, and it reduces in one step to $(x^{\neg\varphi} z^{\varphi})^{\frownie}$.

[7] If $x^{\varphi} \in \mathtt{FV}(M'^{\frownie})$, then $(\lambda x^{\varphi}.M'^{\frownie})^{\varphi\to\psi}$ and $(\lambda x^{\varphi}.M'^{\frownie})^{\neg\varphi}$ are both well-formed, and differ only in their hat. This clause should be understood as saying $(\lambda x.M)^{\varphi\to\psi} \rhd_{1\beta} (\lambda x.M')^{\varphi\to\psi}$ and $(\lambda x.M)^{\neg\varphi} \rhd_{1\beta} (\lambda x.M')^{\neg\varphi}$. We do *not* have $(\lambda x.M)^{\varphi\to\psi} \rhd_{1\beta} (\lambda x.M')^{\neg\varphi}$ or $(\lambda x.M)^{\neg\varphi} \rhd_{1\beta} (\lambda x.M')^{\varphi\to\psi}$; changing hats here is disallowed.

Example 3. Let M be the redex from example 2, and let M' be its reduct. Then $(\lambda w^{\rho}.M^{\theta})^{\rho\to\theta} \rhd_{1\beta} M'^{\frownie}$.

Note that while $(\lambda w^{\rho}.M^{\theta})^{\rho\to\theta}$ is well-formed, despite the fact that $w \notin \mathtt{FV}(M)$, the same would not be true of $\lambda w.M'^{\frownie}$. Accordingly, the λw is dropped entirely in this step of reduction, and we reach M' by itself.

Example 4. With the same M and M', we have $\big(\lambda z^{\varphi}.(\lambda w^{\rho}.M^{\theta})^{\rho\to\theta}\big)^{\varphi\to\rho\to\theta} \rhd_{1\beta} (\lambda z^{\varphi}.M'^{\frownie})^{\varphi\to\rho\to\theta}$. While the inner vacuous lambda has dropped out, as we saw in example 3, the outer λz is not vacuous, and so it can bind into the exceptional M'. Accordingly, it is retained.[8]

Example 5. With the same M and M', we have $\big((\lambda w^{\rho}.M^{\theta})^{\rho\to\theta}v^{\rho}\big)^{\theta} \rhd_{1\beta} M'^{\frownie}$. As in example 3, the vacuous binding must vanish. Here, the application too must vanish: $M'v$ would not be well-formed, so M' alone is retained.

Example 6. With the same M, we have $\big((\lambda w^{\rho}.M^{\theta})^{\rho\to\theta}v^{\rho}\big)^{\theta} \rhd_{1\beta} M^{\theta}$. This starts from the same term as example 5, but reduces it at the outer (vacuous) redex, rather than the inner one. Since w does not occur free in M, this means that $M[w \mapsto v]$ is just M itself.

These examples start to reveal some of the complexity of one-step reduction in core type theory. They also show a bit about how the preservation properties operate in practice.

With one-step reduction in hand, we can give a standard definition of normal form:

Definition 6. A term M is in *normal form* iff there is no M' with $M \rhd_{1\beta} M'$; or equivalently, iff it does not contain a redex.

2.4.3 Reduction

Finally, *reduction* $\rhd_{\beta}$ is the reflexive transitive closure of $\rhd_{1\beta}$. Again, it can be verified that the two preservation properties apply to $\rhd_{\beta}$ as well: where $M^{\mathfrak{C}} \rhd_{\beta} N^{\mathfrak{D}}$, then $\mathtt{FV}(M) \supseteq \mathtt{FV}(N)$ and $\mathfrak{C} \geq \mathfrak{D}$. Both of these properties will be appealed to repeatedly in what follows. I will also talk of 'reduction paths' in the usual way.

Example 7. With the same M and M' from examples 5 and 6, we can see two reduction paths from $\big((\lambda w^{\rho}.M^{\theta})^{\rho\to\theta}v^{\rho}\big)^{\theta}$ to $M'^{\frownie}$. The first path is one step long, and is the reduction in example 5. The second path is two steps long: its first step is the reduction in example 6, and its second is the reduction in example 2.

2.4.4 Reduction and substitution

There's enough here to prove a key lemma about the interaction between reduction and substitution that will be important later.

[8] Although $(\lambda z^{\varphi}.M'^{\frownie})^{\neg\varphi}$ is well-formed, it cannot be reached by reduction from this term, as discussed in footnote 7.

Lemma 1 (qv [Hindley and Seldin, 2008, Lemma A1.12, p. 280])**.** *If x and y are distinct variables and y does not occur free in N, then $Q[y \mapsto P][x \mapsto N]$ is $Q[x \mapsto N][y \mapsto P[x \mapsto N]]$.*

Proof. The only things that could have gone wrong are ruled out by assumption. □

Lemma 2. *If $M \rhd_\beta M'$ and $N \rhd_\beta N'$, and $M[x \mapsto N]$ and $M'[x \mapsto N']$ are both defined, then $M[x \mapsto N] \rhd_\beta M'[x \mapsto N']$.*

Proof. Since terms are identified up to α-conversion, we are free to assume that that no variable occurring bound in M is free in N, and that x is not bound in M.

If $M[x \mapsto N]$ and $M'[x \mapsto N']$ are both defined, then x^φ, N^φ, and N'^φ, for some type φ.[9] It follows that $O[x \mapsto N]$ and $O[x \mapsto N']$ are defined for any term O; the latter will be appealed to below.

First we worry about the reduction path from N to N'. For any step $N_i \rhd_{1\beta} N_j$ in this path, we must have neither N_i nor N_j exceptional, since N' is not exceptional. It follows that $M[x \mapsto N_i]$ and $M[x \mapsto N_j]$ are both defined. Because of this, $M[x \mapsto N_i] \rhd_{1\beta} M[x \mapsto N_j]$, since one-step reduction happens without changing its context whenever this is possible, and we have seen it is possible in this case. So $M[x \mapsto N] \rhd_\beta M[x \mapsto N']$.

Now we worry about the reduction path from M to M'. For any step $M_i \rhd_{1\beta} M_j$ in this path, $M_i[x \mapsto N']$ and $M_j[x \mapsto N']$ are both defined, as mentioned above. This step must occur at a redex $(\lambda y.Q)P$ in M_i with reduct $Q[y \mapsto P]$ in M_j—call this the *key* redex. We work by induction on the formation of M_i around the key redex, to show $M_i[x \mapsto N'] \rhd_{1\beta} M_j[x \mapsto N']$.

- If M_i just is the key redex $(\lambda y.Q)P$, then $M_i[x \mapsto N']$ is $(\lambda y.(Q[x \mapsto N']))(P[x \mapsto N'])$. (It's important here that y is not x, but as y is bound in M we have this.) Thus, $M_i[x \mapsto N'] \rhd_{1\beta} (Q[x \mapsto N'])[y \mapsto P[x \mapsto N']]$; call this latter $M^\star$.

  In this case, M_j is just the reduct $Q[y \mapsto P]$, and so $M_j[x \mapsto N']$ is $Q[y \mapsto P][x \mapsto N']$. By lemma 1, this is $M^\star$, since we have what that lemma needs about bound variables.

- If M_i is OR, with the key redex in O, then $O \rhd_{1\beta} O'$ at the key redex. So M_j is either $O'R$ if O' is typed or else O' if O' is exceptional. Either way, what we need follows from the induction hypothesis and definition 5.

- If M_i is OR, with the key redex in R, the reasoning is just the same as the previous case.

- If M_i is $\lambda z.O$, with the key redex in O, then $O \rhd_{1\beta} O'$ at the key redex. So M_j is either O' if O' is exceptional and does not contain z free, or else $\lambda z.O'$ otherwise. Either way, what we need follows from the induction hypothesis and definition 5,

[9] Usual statements of this lemma for typed lambda calculi (such as [Hindley and Seldin, 2008, Lemma A1.15, p. 281]) do not need to assume that $M'[x \mapsto N']$ is defined, since this follows in those settings from the other assumptions of the lemma. Here, though, it does not follow. Fortunately, everywhere we need to apply this lemma the extra assumption will be justified.

so long as $O'[x \mapsto N']$ is exceptional and does not contain z free iff the same is true of O'. For this, it suffices that z is not x and does not occur free in N'; since z is bound in M_i and so in M, this is taken care of.

□

3 Strong normalisation

In core type theory, every reduction path reaches a normal form; reduction in core type theory is *strongly normalising*. This section proves this claim. I will proceed closely following the strategy of [Hindley and Seldin, 2008, Appendix A3], which itself draws on [Tait, 1967].[10] Key to the proof is the interplay between two properties of terms: *strong normalizability* and *strong computability*.

Definition 7. A term is *strongly normalizing* (SN) iff every reduction path beginning from the term is finite.

Definition 8. A term is *strongly computable* (SC) as follows (by induction on hat):

- If M is a term of atomic type or an exceptional term, then M is SC iff it is SN.
- $M^{\varphi \to \psi}$ is SC iff for all SC terms N^{φ}, the term $(M\, N)^{\psi}$ is SC.
- $M^{\neg\varphi}$ is SC iff for all SC terms N^{φ}, the term $(M\, N)^{☹}$ is SC.

It will emerge over the course of the proof that every term is both SN and SC. The proof begins with a series of small lemmas, before moving to three larger lemmas. The eventual theorem—that every term is SN, and so that $\rhd_{\beta}$ is strongly normalizing—follows quickly from two of these larger lemmas.

3.1 Smaller lemmas

First, two immediate consequences of definition 8.

Lemma 3. *If M and N are both SC, and $M\, N$ is well-formed, then $M\, N$ is SC.*

Proof. Immediate from definition 8. □

In the next lemma and a few places to come, I'll make use of the fact that every type has the form $\mathfrak{C}_1 \to \ldots \to \mathfrak{C}_n \to \theta$, for some $n \geq 0$ and θ either atomic or $\neg\sigma$ for some type σ.

Lemma 4. *$M^{\mathfrak{C}}$ is SC iff:*

- *where $\mathfrak{C}$ is $\mathfrak{C}_1 \to \ldots \to \mathfrak{C}_n \to \theta$ and θ is atomic: for all SC $N_1^{\mathfrak{C}_1}, \ldots, N_n^{\mathfrak{C}_n}$, the term $(M\, N_1 \ldots N_n)^{\theta}$ is SC.*

[10] See also [Troelstra and Schwichtenberg, 2000, §6.8, 6.12.2] and [Sørensen and Urzyczyn, 2006, §5.3.2–5.3.6], both also cited in [Hindley and Seldin, 2008] in connection with this proof.

- *where $\mathfrak{C}$ is $\mathfrak{C}_1 \to \ldots \to \mathfrak{C}_n \to \neg\sigma$: for all SC $N_1^{\mathfrak{C}_1}, \ldots, N_n^{\mathfrak{C}_n}, O^\sigma$, the term $(M N_1 \ldots N_n O)^{☹}$ is SC.*

Proof. Definition 8. □

Now, two lemmas that allow us to infer SN for some terms from SN for others:

Lemma 5. *If M is SN, and N is a subterm of M, then N is SN as well.*

Proof. By noting that any infinite reduction sequence for N would give rise to an infinite reduction sequence for M. □

Lemma 6. *If $M[x \mapsto N]$ is SN, then M is SN as well.*

Proof. By noting that any infinite reduction sequence for M would give rise to an infinite reduction sequence for $M[x \mapsto N]$. □

3.2 Bigger lemmas and the result

That's enough to step to the three bigger lemmas.

Lemma 7 (qv [Hindley and Seldin, 2008, Lemma A3.10, p. 295])**.** *Let $\mathfrak{C}$ be any hat. Then:*

1. *if $M^{\mathfrak{C}}$ is of the form $(aX_1 \ldots X_n)^{\mathfrak{C}}$ (with $0 \leq n$) where a is a variable and all X_i are SN, then M is SC, and*

2. *every SC term with hat $\mathfrak{C}$ is SN.*

Proof. Proof is by induction on $\mathfrak{C}$.

- $\mathfrak{C}$ is atomic or ☹: since $M^{\mathfrak{C}}$ is of the form $(aX_1 \ldots X_n)^{\mathfrak{C}}$ (with $0 \leq n$) where a is a variable and all X_i are SN, M itself is also SN. (For M to have an infinite reduction sequence, some X_i would need to have one.) But then by Definition 8, M is SC. In this case, clause (2) is immediate from Definition 8.

- $\mathfrak{C}$ is $\rho \to \sigma$:

  - For (1): take any SC term Y^ρ. By IH(2), Y is SN. Now consider $(MY)^\sigma$; by IH(1) this is SC. But Y was arbitrary, so M too is SC by Definition 8.

  - For (2): suppose $M^{\mathfrak{C}}$ is SC, and take some variable x^ρ not occurring at all in M. By IH(1), x is SC. So $(Mx)^\sigma$ is SC too, by Lemma 3. By IH(2), then, Mx is SN as well; and so M is SN by Lemma 5.

- $\mathfrak{C}$ is $\neg\rho$:

  - For (1): take any SC term Y^ρ. By IH(2), Y is SN. Now consider $(MY)^{☹}$; by the base case this is SC. But Y was arbitrary, so M too is SC by Definition 8.

  - For (2): suppose $M^{\mathfrak{C}}$ is SC, and take some variable x^ρ not occurring at all in M. By IH(1), x is SC. So $(Mx)^{☹}$ is SC too, by Lemma 3. By Definition 8, then, Mx is SN as well; and so M is SN by Lemma 5.

□

It follows immediately from Lemma 7 that all variables are SC; I'll appeal to this a few times as we go on.

Lemma 8 (qv [Hindley and Seldin, 2008, Lemma A3.11, p. 295])**.** *For any types ρ and σ,*

1. *if $M^{\sigma}[x^{\rho} \mapsto N^{\rho}]$ is SC, and if either N^{ρ} is SC or x is free in M, then $((\lambda x.M)^{\rho\to\sigma}N^{\rho})^{\sigma}$ is SC;*

2. *if $M^{\circledcirc}[x^{\rho} \mapsto N^{\rho}]$ is SC and x occurs free in M, then $((\lambda x.M)^{\rho\to\sigma}N^{\rho})^{\sigma}$ is SC; and*

3. *if $M^{\circledcirc}[x^{\rho} \mapsto N^{\rho}]$ is SC and x occurs free in M, then $((\lambda x.M)^{\neg\rho}N^{\rho})^{\circledcirc}$ is SC.*

Proof.

1. Recall that σ is $\tau_1 \to \ldots \to \tau_n \to \theta$, where θ is either atomic or $\neg\psi$.

   (a) If θ is atomic, take any SC $M_1^{\tau_1}, \ldots, M_n^{\tau_n}$. Since $M[x \mapsto N]$ is SC, it follows from Lemma 4 that $\big((M[x \mapsto N])M_1 \ldots M_n\big)^{\theta}$ is SC, and so (since θ is atomic) SN.

   Since this term is SN, by Lemma 5 so are all its subterms, among them $M[x \mapsto N]$ and all the M_is. By Lemma 6, M itself is SN. If x occurs free in M, then N is a subterm of $M[x \mapsto N]$, so N is SN. If x does not occur free in M, then we have by assumption than N is SC, so by Lemma 7 N is still SN.

   Now, suppose toward a contradiction that $\big((\lambda x.M)NM_1 \ldots M_n\big)^{\theta}$ is not SN, that it has an infinite reduction sequence. This sequence cannot consist entirely of reductions within $M, N, M_1, \ldots, M_n$, since we know all of these are SN.

   So it must look like this:

$$
\begin{aligned}
(\lambda x.M)NM_1 \ldots M_n &\rhd_{\beta} (\lambda x.M')N'M_1' \ldots M_n' \\
&\rhd_{1\beta} (M'[x \mapsto N'])M_1' \ldots M_n' \\
&\rhd_{\beta} \ldots
\end{aligned}
$$

   By lemma 2, however, $M[x \mapsto N] \rhd_{\beta} M'[x \mapsto N']$,[11] and so we can construct an infinite reduction sequence

$$
\begin{aligned}
(M[x \mapsto N])M_1 \ldots M_n &\rhd_{\beta} (M'[x \mapsto N'])M_1' \ldots M_n' \\
&\rhd_{\beta} \ldots
\end{aligned}
$$

[11] We can see that $M'[x \mapsto N']$ is defined, as the lemma requires, since it occurs as a subterm in the reduction sequence.

But this is impossible, since we know $(M[x \mapsto N])M_1 \ldots M_n$ is SN. Thus, $\big((\lambda x.M)NM_1 \ldots M_n\big)^\theta$ is itself SN. Since θ is atomic, this means $\big((\lambda x.M)NM_1 \ldots M_n\big)^\theta$ is SC. Since $M_1, \ldots, M_n$ were arbitrary, it follows by lemma 4 that $(\lambda x.M)N$ is SC.

(b) If θ is $\neg\psi$, take any SC $M_1^{\tau_1}, \ldots, M_n^{\tau_n}, O^\psi$. Since $M[x \mapsto N]$ is SC, it follows from Lemma 4 that $\big((M[x \mapsto N])M_1 \ldots M_n O\big)^{☹}$ is SC, and so by Definition 8 SN as well.

From here, the reasoning continues just as for the atomic case, but with O hanging out on the right.

2. The reasoning is exactly parallel to the previous case, except slightly simpler, since we are now sure x occurs free in M.

3. The reasoning is a simplified version of the previous cases. Since $M^{☹}[x^\rho \mapsto N^\rho]$ is SC, it follows from Definition 8 that is is SN as well. From this, it follows by lemma 6 that $M^{☹}$ is SN, and by lemma 5 that N is SN.

   Now, suppose towards a contradiction that $(\lambda x.M)^{\neg\rho}N$ is not SN, that it has an infinite reduction sequence. This sequence cannot consist entirely of reductions in M and N, since these are both SN. So it must look like this:

$$
\begin{aligned}
(\lambda x.M)^{\neg\rho}N &\rhd_\beta (\lambda x.M')^{\neg\rho}N' \\
&\rhd_{1\beta} M'[x \mapsto N'] \\
&\rhd_\beta \ldots
\end{aligned}
$$

   where $M \rhd_\beta M'$ and $N \rhd_\beta N'$.

   By lemma 2, however, $M[x \mapsto N] \rhd_\beta M'[x \mapsto N']$, and so we can construct an infinite reduction sequence:

$$
\begin{aligned}
M[x \mapsto N] &\rhd_\beta M'[x \mapsto N'] \\
&\rhd_\beta \ldots
\end{aligned}
$$

   But this is impossible, since we know $M[x \mapsto N]$ is SN. Thus, $((\lambda x.M)^{\neg\rho}N^\rho)^{☹}$ is itself SN; since it has hat ☹, this makes it SC as well.

□

Lemma 9 (qv [Hindley and Seldin, 2008, Lemma A3.12, p. 296])**.** *For every term M, for all $x_1^{\rho_1}, \ldots, x_n^{\rho_n}$ (with $n \geq 1$), and all SC terms $N_1^{\rho_1}, \ldots, N_n^{\rho_n}$ such that for all $2 \leq i \leq n$ none of $x_1, \ldots, x_{i-1}$ occurs free in N_i, the term $M^\star := M[x_n \mapsto N_n] \ldots [x_1 \mapsto N_1]$ is SC.*

Proof. Induction on the formation of M.

- If M is x_i for some i, then $M^\star$ is N_i. (This relies on the non-freedom assumption if $i > 1$.) By assumption, then, $M^\star$ is SC.

- If M is some other variable, then $M^\star$ is that variable too. By lemma 7, then, $M^\star$ is SC.

- If M is $M_1 M_2$, then $M^\star$ is $M_1^\star M_2^\star$. By the induction hypothesis, $M_1^\star$ and $M_2^\star$ are both SC. So $M^\star$ is SC by lemma 3.

- If M is $\lambda x^\rho.N^\sigma$, first choose bound variables in M so that x^ρ does not occur free in any of $N_1, \ldots, N_n, x_1, \ldots, x_n$. Then $M^\star$ is $\lambda x^\rho.N^\star$. By definition 8, we can show that $M^\star$ is SC by showing that for all SC O^ρ the term $M^\star O$ is SC. So take any SC O^ρ. Then $N[x_n \mapsto N_n] \ldots [x_1 \mapsto N_1][x \mapsto O]$ is SC by the inductive hypothesis applied to N with the sequence $O, N_1, \ldots, N_n$. But this is $N^\star[x \mapsto O]$. So by lemma 8, $(\lambda x.N^\star)O$ is SC; this is $M^\star O$, so $M^\star$ is indeed SC.

□

Theorem 3. *Every term is SN.*

Proof. Take any term M and variable x. By lemma 9, $M[x \mapsto x]$ is SC; but this is just M itself, so M is SC. By lemma 7, then, M is SN. □

4 Conclusion

Core type theory is a strange beast. Although core logic is very similar to intuitionistic logic, and core type theory bears a similar relationship to core logic that the simply-typed lambda calculus does to intuitionistic logic, many important features of the simply-typed lambda calculus do not hold of core type theory. Although core type theory is inspired by term rewriting systems like the simply-typed lambda calculus, it is not itself a term rewriting system, since reduction in a subterm can change its context. Core type theory is not confluent, and the equivalence relation generated by its reduction relation is trivial, relating every term to every other.

Taking all this into consideration, it is remarkable that core type theory is as well-behaved as it is. Reduction does not preserve free variables, but it never adds any.[12] Reduction does not preserve type, but it never carries a term of one type to a term of any other type, or an exceptional term to a typed one. Finally, the calculus is strongly normalizing: there are many strange reduction paths, but no infinite ones.

[12] This is exactly as in the simply-typed lambda calculus. Note, however, that in the λI calculus, reduction is more precise: reduction leaves the set of free variables exactly the same. For more on λI, see eg [Church, 1941], where it is called simply ‘the calculus of λ-conversion’, with what is now more usual marked as ‘the calculus of λ-K-conversion’.

References

Baader, F. and Nipkow, T. (1998). *Term Rewriting and All That*. Cambridge University Press. 6

Barthe, G. and Melliès, P.-A. (1996). On the subject reduction property for algebraic type systems. In *International Workshop on Computer Science Logic*, pages 34–57. Springer. 6

Church, A. (1941). *The Calculi of Lambda-Conversion*. Princeton University Press, Princeton, New Jersey. 14

Girard, J. (1995). Linear logic: Its syntax and semantics. In Girard, J., Lafont, Y., and Regnier, L., editors, *Advances in Linear Logic*, pages 222–1. Cambridge University Press. 1

Harper, R. (2016). *Practical foundations for programming languages*. Cambridge University Press, 2nd edition. 6

Hindley, J. and Seldin, J. P. (2008). *Lambda-Calculus and Combinators: an Introduction*. Cambridge University Press, Cambridge. 9, 10, 11, 12, 13

Howard, W. H. (1980). The formulae-as-types notion of construction (1969). In *To HB Curry: Essays on combinatory logic, lambda calculus, and formalism*. Academic Press. 1

Petrolo, M. and Pistone, P. (2019). On paradoxes in normal form. *Topoi*, 38(3):605–617. 1

Scherer, G. (2017). Deciding equivalence with sums and the empty type. In *ACM SIGPLAN Notices*, volume 52, pages 374–386. ACM. 1

Sørensen, M. H. and Urzyczyn, P. (2006). *Lectures on the Curry-Howard isomorphism*. Elsevier. 1, 4, 10

Tait, W. W. (1967). Intensional interpretations of functionals of finite type I. *The journal of symbolic logic*, 32(2):198–212. 10

Tennant, N. (1979). Entailment and proofs. *Proceedings of the Aristotelian Society*, 79(1):167–189+viii. 1

Tennant, N. (2002). Ultimate normal forms for parallelized natural deductions. *Logic Journal of the IGPL*, 10(3):299–337. 1, 4

Tennant, N. (2015). The relevance of premises to conclusions of core proofs. *Review of Symbolic Logic*, 8(4):743–784. 4

Tennant, N. (2017). *Core Logic*. Oxford University Press, Oxford. 1, 3

Terese (2003). *Term Rewriting Systems*. Cambridge University Press. 6

Troelstra, A. S. and Schwichtenberg, H. (2000). *Basic Proof Theory*. Cambridge University Press, Cambridge, 2 edition. 10