Modified Realizability Toposes

and

Strong Normalization Proofs

(Extended Abstract)[1]

J. M. E. Hyland[2] C.-H. L. Ong[3]

University of Cambridge, England

Abstract

This paper is motivated by the discovery that an appropriate quotient SN_* of the strongly normalising untyped $\lambda*$-terms (where $*$ is just a formal constant) forms a partial applicative structure with the inherent application operation. The quotient structure satisfies all but one of the axioms of a partial combinatory algebra (PCA). We call such partial applicative structures *conditionally partial combinatory algebras* (C-PCA). Remarkably, an arbitrary *right-absorptive* C-PCA gives rise to a *tripos* provided the underlying intuitionistic predicate logic is given an interpretation in the style of Kreisel's *modified realizability*, as opposed to the standard Kleene-style realizability. Starting from an arbitrary right-absorptive C-PCA U, the tripos-to-topos construction due to Hyland *et al.* can then be carried out to build a *modified realizability topos* $\mathbb{TOP}_{\mathrm{m}}(U)$ of non-standard sets equipped with an equality predicate. Church's Thesis is internally valid in $\mathbb{TOP}_{\mathrm{m}}(\mathsf{K}_1)$ (where the PCA K_1 is "Kleene's first model" of natural numbers) but not Markov's Principle. There is a topos inclusion of $\mathbb{SET}$ — the "classical" topos of sets — into $\mathbb{TOP}_{\mathrm{m}}(U)$; the image of the inclusion is just sheaves for the $\neg\neg$-topology. Separated objects of the $\neg\neg$-topology are characterized. We identify the appropriate notion of PERs (partial equivalence relations) in the modified realizability setting and state its completeness properties. The topos $\mathbb{TOP}_{\mathrm{m}}(U)$ has enough completeness property to provide a category-theoretic semantics for a family of higher type theories which include Girard's System F and the Calculus of Constructions due to Coquand and Huet. As an important application, by interpreting type theories in the topos $\mathbb{TOP}_{\mathrm{m}}(\mathsf{SN}_*)$, a clean semantic explanation of the Tait-Girard style strong normalization argument is obtained. We illustrate how a strong normalization proof for an impredicative and dependent type theory may be assembled from two general "stripping arguments" in the framework of the topos $\mathbb{TOP}_{\mathrm{m}}(\mathsf{SN}_*)$. This opens up the possibility of a "generic" strong normalization argument for an interesting class of type theories.

1 Introduction

A celebrated result at the junction of proof theory and theoretical computer science is the strong normalization of System F [Gir72, Gir86]. This result is notable not only because of the impact it

[1]An earlier version appeared in Proc. Typed Lambda Calculus Applications Conference, Utrecht, March 1993, Springer LNCS Vol. 664.

[2]Dept. of Pure Maths. and Mathematical Statistics, 16 Mill Lane, Cambridge CB2 1SB, UK; `jmeh1@phx.cam.ac.uk`.

[3]Computer Laboratory, Pembroke Street, Cambridge CB2 3QG, UK; `chlo1@cl.cam.ac.uk`. On leave from the National University of Singapore and supported by a fellowship from Trinity College, Cambridge.

has in proof theory (*e.g.* proof of the syntactic version of Takeuti's conjecture) but also because the proof is notoriously hard. To get a feel of how intrinsically difficult it is, it is helpful to recall Girard's observation that the strong normalization (s.n.) of System F implies the consistency of $\mathbf{PA}_2$ (second order Peano Arithmetic). The system $\mathbf{PA}_2$ is highly expressive. In Girard's words, "it suffices for everyday mathematics". By Gödel's Second Incompleteness Theorem, the consistency of $\mathbf{PA}_2$ is not provable in $\mathbf{PA}_2$. In view of Girard's observation, the s.n. of System F is therefore also *not* provable in $\mathbf{PA}_2$. This says something about the complexity of the s.n. proof. Remarkably, Girard succeeded in proving it by using a powerful induction technique known as *reducibility candidates* which is based on an earlier method of Tait [Tai67, Tai75]; see [Gal90] for a careful exposition and [Sce89] for a semantic approach. System F, also known as Second Order Polymorphic Lambda Calculus was reinvented by Reynolds [Rey74].

Other higher type theories have emerged over the past two decades. Martin-Löf introduced a series of intuitionistic dependent type theories *e.g.* [ML73, ML84]. More recently, Coquand and Huet introduced the Calculus of Constructions [CH88] which is both a dependent as well as impredicative type theory. Strong normalization holds for all of these theories. The proof in each case, being essentially an appropriate extension of the Tait-Girard method, is invariably hard. It would therefore be highly desirable if a "generic" s.n. proof could be invented which not only sheds light on the Tait-Girard argument but also reduces the s.n. property of a class of type theories to a couple of sufficient conditions. It is this dream of a "generic" s.n. argument which provided the initial motivation to our work.

A Key Idea It is well known (see e.g. [LS86]) that there is an equivalence between cartesian closed categories (CCC) and the simply-typed λ-calculi with surjective pairing. Consider the interpretation of $\boldsymbol{\lambda}^{\rightarrow}$, the pure simply-typed λ-calculus in a particular (class of) CCC $\mathbb{PER}(U)$, the category of partial equivalence relations (PERs) over a partial combinatory algebra (PCA) U. Recall that objects of this category are just PERs *i.e.* symmetric and transitive relations over U. For any PERs R and S over U, a morphism $F : R \to S$ is a function F from $[R]$ (the R-equivalence classes) to $[S]$ which is *realised*[4] (or *tracked*) by some element of U; that is to say, for some realiser $f \in U$, whenever $r\,R\,r'$, then $(fr)\;S\;(fr')$ and $F([r]_R) = [fr]_S$. (We assume throughout this paper that relations defined over a partial applicative structure are *strict* *i.e.* whenever we write $(fr)\;S\;(fr')$, we are implicitly asserting that fr and fr' are defined.) Categories constructed in this way have morphisms which are *by definition* realised by elements of the underlying PCA. We shall refer to such categories informally as "realizability categories".

Consider the standard interpretation of $\boldsymbol{\lambda}^{\rightarrow}$ in $\mathbb{PER}(U)$ (see e.g. [LS86]). For any derivable type-assignment sequent $x_1 : \sigma_1, \cdots, x_n : \sigma_n \vdash s : \tau$ (assuming $\{\,\vec{x}\,\} \supseteq \mathsf{FV}(s)$, the free variables of s), the types $\sigma_1, \cdots, \sigma_n, \tau$ are interpreted as objects of $\mathbb{PER}(U)$, and s the term in question is interpreted as the morphism $[\![\, s \,]\!] : [\![\, \mathbf{1} \,]\!] \times [\![\, \sigma_1 \,]\!] \times \cdots \times [\![\, \sigma_n \,]\!] \to [\![\, \tau \,]\!]$ which is realised by some element of the underlying PCA U. This interpretation makes sense in the class of CCCs $\mathbb{PER}(U)$ where U is *any* PCA. Now, *suppose* the following statement is valid.

Assumption 0 *An appropriate quotient of the s.n. untyped λ-terms yields a* PCA, *call it* SN. $\square$

As before, we may interpret the calculus $\boldsymbol{\lambda}^{\rightarrow}$ in the CCC $\mathbb{PER}(\mathsf{SN})$. We can now demonstrate how a s.n. "proof" may be assembled from the following **"stripping" arguments**.

[4] *Realizability* is a notion primarily associated with proofs of propositions. We use it in a broader sense of "witnessing" a property, not necessarily in the context of formal logic.

1 **Realiser** *For any derivable sequent* $x_1 : \sigma_1, \cdots, x_n : \sigma_n \vdash s : \tau$, *the morphism* $[\![\, \vec{x} : \vec{\sigma} \vdash s : \tau \,]\!]$ *is realised by* $\lambda\xi.\lambda x_1 \cdots x_n.\lceil s \rceil$ *where* $\lceil s \rceil$ *is obtained from* s *by "stripping off" (or erasing) all embedded type expressions.* (Since $\lceil s \rceil \in \mathsf{SN}$, $\lceil s \rceil$ is s.n.) $\square$

2 **Reflection** *For any well-typed term* s, *if* $\lceil s \rceil$ *is s.n. in* $\mathbf{\Lambda}$ *then* s *is s.n. in the typed regime.* $\square$

The two stripping arguments above are easily seen to be valid in the case of the calculus $\boldsymbol{\lambda}^{\rightarrow}$. *Provided* Assumption 0 is valid, the proof of the s.n. of $\boldsymbol{\lambda}^{\rightarrow}$ is now complete.

A "Generic" Strong Normalization Argument Does the argument "scale up"? Does an appropriate extrapolation of this argument establish s.n. of say, System F or even better, the Calculus of Constructions? This approach hinges upon two things:

- there is a realizability category $\mathbb{C}$ with the untyped s.n. λ-terms as realisers,
- this category $\mathbb{C}$ is a model of the type theory in question.

We know from the works of Seely [See87], Pitts [Pit87] and Hyland [HP89] that the category-theoretic interpretation of such sophisticated type theories as System F or the Calculus of Constructions places heavy demands on the structure of categories. For example, in the case of System F, we essentially need a cloven fibration $\begin{smallmatrix}\mathbb{E}\\ \downarrow p\\ \mathbb{B}\end{smallmatrix}$ (see *e.g.* [B85]) such that:

(i) the base category $\mathbb{B}$ has finite products,

(ii) $\begin{smallmatrix}\mathbb{E}\\ \downarrow p\\ \mathbb{B}\end{smallmatrix}$ is a fibred CCC *i.e.* each fibre is a CCC and reindexing is a *strict* CCC-morphism,

(iii) there is a generic object $G \in \mathbb{E}_P$ for some distinguished object $P \in \mathbb{B}$,

(iv) $\begin{smallmatrix}\mathbb{E}\\ \downarrow p\\ \mathbb{B}\end{smallmatrix}$ has P-indexed product *i.e.* for each $I \in \mathbb{B}$, the reindexing functor $\pi^*_{P,I}$ has a right-adjoint $\Pi_{P,I}$ satisfying the Beck-Chevalley condition where $\pi_{P,I} : P \times I \rightarrow I$ is the projection morphism.

Happily, realizability categories satisfying the above requirements are available as appropriate sub-structures of *realizability toposes* [Hyl82, Hyl88] (see also [HRR90]). Hyland shows that any PCA U gives rise in a systematic way to a Kleene-style realizability topos $\mathbb{TOP}_s(U)$ which has more than sufficient completeness properties for interpreting at least the class of impredicative and dependent type theories [Pit87, HP89].

To carry our programme through, the first step is to verify Assumption 0.

2 Strongly Normalising Untyped $\lambda*$-Terms

Our immediate task is the following:

To construct a PCA *of strongly normalising untyped λ-terms (or an appropriate quotient thereof) using the inherent application operator of the calculus.*

We begin by searching for an equivalence relation on $\mathbf{SN}$ (the collection of s.n. pure untyped λ-terms), say $\sim$ which is *compatible* with application (so that the associated quotient structure has a well-defined partial application). That is to say, for $M, M', N, N' \in \mathbf{SN}$, whenever $M \sim M'$ and $N \sim N'$, then

- *either* both MN and $M'N'$ are not s.n.,
- *or* both are s.n. and $MN \sim M'N'$.

First Attempt The most natural candidate for $\sim$ is β-equivalence (which we denote as $=_\beta$). Unfortunately, it is not compatible with application. It is instructive to see why this is so. Consider the s.n. λ-terms: $M \equiv \lambda z.(\lambda x.\mathbf{i})(z(\lambda y.yy)) =_\beta \lambda z.\mathbf{i} \equiv N$ where $\mathbf{i}$ is the identity. Take $P \equiv (\lambda y.yy)$. Clearly NP is s.n. However MP is not s.n. because the free occurrence of the variable z in the redex-subterm $\Delta \equiv (\lambda x.\mathbf{i})(z(\lambda y.yy))$ of M allows "offending" terms (like P in this case) to be introduced as a result of the application MP. This situation will not arise in the case of NP simply because z does not occur free in N.

The above example leads us to consider the equivalence relation generated by a reduction scheme that contracts *only* those β-redexes which do not contain any free variables. More formally, we define *closed β-reduction* on $\mathbf{\Lambda}_*$ (the collection of λ-terms generated from a distinguished formal constant $*$) denoted $\to_{\mathrm{cl}}$, as the relation inductively defined by the following rules:

$$\frac{}{(\lambda x.P)Q \to_{\mathrm{cl}} P[Q/x]} \quad \mathsf{FV}((\lambda x.P)Q) = \varnothing$$

$$\frac{M \to_{\mathrm{cl}} N}{PM \to_{\mathrm{cl}} PN \qquad MP \to_{\mathrm{cl}} NP \qquad \lambda x.M \to_{\mathrm{cl}} \lambda x.N}$$

We further define $\twoheadrightarrow_{\mathrm{cl}}$ as the reflexive, transitive closure of $\to_{\mathrm{cl}}$, and $\sim_{\mathrm{cl}}$ as the symmetric closure of $\twoheadrightarrow_{\mathrm{cl}}$. For example, $\lambda z.z((\lambda x.z)\mathbf{i}) \not\to_{\mathrm{cl}} \lambda z.zz$ but $\lambda z.z((\lambda x.x)\mathbf{i}) \to_{\mathrm{cl}} \lambda z.z\mathbf{i}$.

The main result of this section is the following theorem. We define $\mathbf{SN}_*$ to be the subset of $\mathbf{\Lambda}_*$ consisting of all s.n. terms. Note that there are no δ-rules associated with the constant $*$.

Theorem 2.1 (Compatibility) *Let $M, M', N, N' \in \mathbf{SN}_*$ with $M \sim_{\mathrm{cl}} M'$ and $N \sim_{\mathrm{cl}} N'$. Then,*

(i) $MN \in \mathbf{SN}_* \iff M'N' \in \mathbf{SN}_*$,

(ii) $MN \in \mathbf{SN}_* \implies MN \sim_{\mathrm{cl}} M'N'$.

Hence, the quotient structure $\langle\, \mathbf{SN}_*/{\sim_{\mathrm{cl}}}, \cdot/{\sim_{\mathrm{cl}}} \,\rangle$ is a well-defined partial applicative structure. $\square$

We sketch an outline of the proof. In general, we follow the notational conventions of [Bar84] with the notable exception of substitution; we write $M[N/x]$ to mean "in M, substitute N for every occurrence of x" taking care to follow the substitution convention in [Bar84, p. 26]. We let Δ, Δ_i

range over β-redexes. Let $\Delta \equiv (\lambda x.A)B$. By convention, we write $\underline{\Delta} \equiv A[B/x]$ (similarly for $\underline{\Delta_i}$). The binary relation β on $\mathbf{\Lambda}_*$ is defined as the collection of pairs of the shape $\langle\,(\lambda x.P)Q, P[Q/x]\,\rangle$ with P, Q ranging over $\mathbf{\Lambda}_*$. We write $\rightarrow$ as the compatible closure of β and $\twoheadrightarrow$ the reflexive, transitive closure of $\rightarrow$.

Multi-holed Linear Contexts In the following, we shall work with a sub-collection of what Barendregt calls "multiple numbered contexts" (see [Bar84, p. 375]) known as *multi-holed linear contexts*. We write them typically as $C[[]_1, \cdots, []_n]$ where the $[]_i$'s serve as place-markers for the "holes". Note that all $[]_i$'s are distinct and each hole $[]_i$ occurs exactly once (hence the adjective "linear").

Definition 2.2 For $U, V \in \mathbf{\Lambda}_*$, we say that $U \twoheadrightarrow V$ is an *innocuous reduction* if for some $n \geqslant 1$ there are redexes Δ_i for $1 \leqslant i \leqslant n$ and an n-holed linear context $C[[]_1, \cdots, []_n]$ satisfying the *non-interference* condition

"no free variables in any of the Δ_i becomes bound in $C[\Delta_1, \cdots, \Delta_n]$"

and that $U \equiv C[\Delta_1, \cdots, \Delta_n]$ and $V \equiv C[\underline{\Delta_1}, \cdots, \underline{\Delta_n}]$. The point of the non-interference condition is to ensure that for fresh variables $\xi_1, \cdots, \xi_n$, the term $C[\Delta_1, \cdots, \Delta_n]$ is the same as $C[\xi_1, \cdots, \xi_n][\vec{\Delta}/\vec{\xi}]$.

For example, with $C[\,] \equiv \lambda z.[\,]$ and $\Delta \equiv (\lambda x.\mathbf{i})(z(\lambda y.yy))$, the reduction $C[\Delta] \rightarrow C[\underline{\Delta}]$ is not innocuous because the non-interference condition is violated. Closed reduction is immediately seen to be innocuous *i.e.* for $U, V \in \mathbf{\Lambda}_*$, whenever $U \rightarrow_{\mathrm{cl}} V$, there is a 1-holed linear context $C[\,]$ and a *closed* redex Δ such that $U \equiv C[\Delta] \rightarrow_{\mathrm{cl}} C[\underline{\Delta}] \equiv V$.

It is easy to see that β-reduction preserves s.n. property *i.e.* assuming $U \rightarrow V$, if $U \in \mathbf{SN}_*$ then $V \in \mathbf{SN}_*$. However, the converse *i.e.*

$$(\dagger) \qquad U \rightarrow V \;\;\&\;\; V \in \mathbf{SN}_* \quad \Longrightarrow \quad U \in \mathbf{SN}_*$$

is not true in general; just consider $U \equiv (\lambda x.y)\Omega \rightarrow y \equiv V$ where Ω is any unsolvable term. We establish sufficient conditions for the above implication $(\dagger)$ in the following proposition. This result is also a crucial step (but stronger than is necessary) in the proof of the Compatibility Theorem.

Proposition 2.3 (Crucial) *For $U, V \in \mathbf{\Lambda}_*$ such that $U \equiv C[\Delta_1, \cdots, \Delta_n] \twoheadrightarrow C[\underline{\Delta_1}, \cdots, \underline{\Delta_n}] \equiv V$ is an innocuous reduction with $\Delta_1, \cdots, \Delta_n \in \mathbf{SN}_*$. If $V \in \mathbf{SN}_*$, then $U \in \mathbf{SN}_*$.* $\square$

The proposition is a corollary of a Technical Lemma which we omit. We are now in a position to prove the Compatibility Theorem which is actually valid for any λ-calculus (including the *pure* calculus) generated from a set (possibly empty) of formal constants with no δ-rules.

Proof of the Theorem (i) Since s.n. is preserved by closed β-reduction, it suffices to prove: for $M, N, P \in \mathbf{SN}_*$,

(1) $M \rightarrow_{\mathrm{cl}} N \;\;\&\;\; NP \in \mathbf{SN}_* \quad \Longrightarrow \quad MP \in \mathbf{SN}_*$;

(2) $M \rightarrow_{\mathrm{cl}} N \;\;\&\;\; PN \in \mathbf{SN}_* \quad \Longrightarrow \quad PM \in \mathbf{SN}_*$.

Now, to prove (1), note that $MP \to_{\rm cl} NP$. For some 1-holed linear context $C[\,]$ and for some closed redex Δ, $MP \equiv C[\Delta] \to C[\Delta] \equiv NP$. Δ is s.n. since it is a subterm of M — a s.n. term. The result then follows by an appeal to the Crucial Proposition. The argument for (2) is entirely similar. Part (ii) of the theorem is an easy consequence of the fact that the equivalence relation $\sim_{\rm cl}$ is by definition a compatible closure. $\square$

In the following, we shall often need to reason with the s.n. property of $\lambda*$-terms. We gather some useful arguments in the following proposition to this end.

Proposition 2.4 (Strong Normalization Arguments) *The following arguments are valid:*

(1)	**subterm**	*If $M \in \mathbf{SN}_*$ and N is a subterm of M, then $N \in \mathbf{SN}_*$;*
(2)	**reduction**	*If $M \in \mathbf{SN}_*$ and $M \twoheadrightarrow N$, then $N \in \mathbf{SN}_*$;*
(3)	**abstraction**	*$M \in \mathbf{SN}_*$ iff $\lambda x.M \in \mathbf{SN}_*$;*
(4)	**substitution**	*If $M[N/x] \in \mathbf{SN}_*$ for some N, then $M \in \mathbf{SN}_*$;*
(5)	**redex**	*$Q, P[Q/x] \in \mathbf{SN}_*$ iff $(\lambda x.P)Q \in \mathbf{SN}_*$;*
(6)	**head variable**	*Let $\nu \equiv *$ or a variable. Then, $\vec{L} \subseteq \mathbf{SN}_*$ iff $\nu\vec{L} \in \mathbf{SN}_*$;*
(7)	**application**	*Let $\nu \equiv *$ or a variable. Then, $M, \vec{L} \subseteq \mathbf{SN}_*$ iff $M(\nu\vec{L}) \in \mathbf{SN}_*$;*
(8)	**anti-reduction**	*If $M, N \in \mathbf{SN}_*$ and $MN \equiv C[\Delta] \to C[\Delta] \in \mathbf{SN}_*$ with Δ and $C[\,]$ satisfying the non-interference condition, then $MN \in \mathbf{SN}_*$.*

The converse of each of the above arguments, where applicable, is not valid. $\square$

Is SN_* a partial combinatory algebra? Let SN_* denote the quotient structure $\langle\, \mathbf{SN}^o_*/\!\sim_{\rm cl}, \cdot/\!\sim_{\rm cl}\,\rangle$ where $\mathbf{SN}^o_*$ is the collection of closed s.n. untyped $\lambda*$-terms. We shall very often confuse SN_* with the underlying set. Let $\mathbf{s}$ and $\mathbf{k}$ denote the (respective $\sim_{\rm cl}$-equivalence classes of the) standard combinators $\lambda xyz.xz(yz)$ and $\lambda xy.x$. For any partial applicative structure U, denote the formal applicative algebra freely generated from U and Var as $\mathcal{T}(U)$. We shall call elements of $\mathcal{T}(U)$ *polynomials* over U.

Definition 2.5 A *conditionally partial combinatory algebra* (C-PCA) is a partial applicative structure $\langle\, U, \cdot\,\rangle$ where U is a set with at least two elements; there are distinguished elements $\mathbf{k}$, $\mathbf{s} \in U$ satisfying the following axioms: for any $f, g, a \in U$

$$\begin{array}{lrcl} (\mathbf{S}) & \mathbf{s}fga & \simeq & fa(ga), \\ (\mathbf{K}) & \mathbf{k}ab & = & a, \end{array}$$

where $t\!\downarrow$ means "t is defined" and $\simeq$ is *Kleene equality* i.e. either both sides are defined and are equal, or both are undefined. We shall assume that application is strict *i.e.* to assert $st\!\downarrow$ is to assert implicitly both $s\!\downarrow$ and $t\!\downarrow$ for polynomials s and t. Also, the assertion $u = v$ has the force of $u\!\downarrow$ and

$v\downarrow$. Note that the following axioms are valid in a C-PCA: for any $f, g, a \in U$, we have $(\mathbf{K}_1)$: $\mathbf{k}a\downarrow$ and

$$(\mathbf{S}_2^-) \qquad \exists a \in U.fa(ga)\downarrow \quad \Longrightarrow \quad \mathbf{s}fg\downarrow.$$

It is easy to check that **skk** which we shall call **i** is always defined in a C-PCA. The stipulation $\mathbf{s} \neq \mathbf{k}$ is equivalent to $\exists a, b \in U.a \neq b$. If, in addition, the axiom $(\mathbf{S}_2)$: $\forall f, g \in U.\mathbf{s}fg\downarrow$ holds in a C-PCA U, then U is by definition, a *partial combinatory algebra.* Of course, if the axiom $(\mathbf{S}_2)$ holds, then so does the axiom $(\mathbf{S}_1)$: $\forall f \in U.\mathbf{s}f\downarrow$; but the converse is not true.

As an important corollary of Proposition 2.4, we have the following theorem.

Theorem 2.6 (S.N. Realisers) *The quotient structure* SN_* *is a* C-PCA *in which* $(\mathbf{S}_1)$ *is valid but not* $(\mathbf{S}_2)$. *Hence,* SN_* *is not a* PCA.

Proof (Sketch) To see why the axiom $(\mathbf{S}_2)$ fails[5]: just consider $f = g = \lambda z.(\lambda x.xx)$. We will just show the validity of $(\mathbf{S})$ for illustration. First for "$\Rightarrow$", for any $f, g, a \in \mathsf{SN}_*$, observe that:

$$\mathbf{s}fga \rightarrow_{\mathrm{cl}} [\lambda yz.fz(yz))g]_2 a \rightarrow_{\mathrm{cl}} [(\lambda z.fz(gz))a]_1 \rightarrow_{\mathrm{cl}} fa(ga).$$

If $\mathbf{s}fga \in \mathsf{SN}_*$, then so does $fa(ga)$, by the reduction argument. To prove the other direction "$\Leftarrow$", suppose $fa(ga) \in \mathsf{SN}_*$. Note that $(fz(gz))[a/z] \equiv fa(ga)$. By the redex argument, $[(\lambda z.fz(gz))a]_1 \in \mathsf{SN}_*$. Now, by the subterm argument, $(\lambda z.fz(gz)) \in \mathsf{SN}_*$; and so, by the redex argument, the closed redex $[(\lambda yz.fz(yz))g]_2 \in \mathsf{SN}_*$. Take $C[\,] \equiv [\,]a$, by the Crucial Proposition, $[\lambda yz.fz(yz))g]_2 a \equiv C[\lambda yz.fz(yz))g] \in \mathsf{SN}_*$. By an entirely similar argument, we have $\mathbf{s}fga \in \mathsf{SN}_*$. $\square$

The relevance of PCAs to constructive logic is well-known, see *e.g.* [Bee85, Ch. VI]; not so in the case of C-PCAs. As far as we know, the notion of C-PCA is new. Schönfinkel showed that combinatory algebras may be characterised as precisely those (total) applicative structures U which are *combinatory complete i.e.* every polynomial t over U is *internally representable* which means that for any fixed $\{\vec{x}\}$ containing $\mathsf{Var}(t)$, we have

$$\exists u \in U.\forall \vec{a} \subseteq U.t[\vec{a}/\vec{x}] = u\vec{a}.$$

Of course, for the simultaneous substitution $(-)[\vec{a}/\vec{x}]$ to make sense, we require the two sequences $\vec{a}$ and $\vec{x}$ to be compatible *i.e.* they have the same length. In a similar vein, Bethke [Bet87] recently established a characterization result for PCAs. She showed that a partial applicative structure U is a PCA iff for any $t \in \mathcal{T}(U)$ and for $\mathsf{Var}(t) \subseteq \{x_0, \cdots, x_{n+1}\}$, U satisfies the following:

$$\exists y \in U.\forall a_0, \cdots, a_{n+1} \subseteq U.[ta_0 \cdots a_n\downarrow \;\&\; ya_0 \cdots a_{n+1} \simeq t[a_0, \cdots, a_{n+1}/x_0, \cdots, x_{n+1}]].$$

Can C-PCAs be characterised along similar lines? For any partial applicative structure U, we say that U is *conditionally combinatory complete* iff for any $t \in \mathcal{T}(U)$ with $\mathsf{Var}(t) \subseteq \{\vec{x}\}$, we have:

$$(\textbf{c-cc}) \qquad \exists \vec{b} \subseteq U.t[\vec{b}/\vec{x}]\downarrow \quad \Longrightarrow \quad \exists y \in U.\forall \vec{a} \subseteq U.y\vec{a} \simeq t[\vec{a}/\vec{x}].$$

[5]We are grateful to E. Robinson for pointing this example out to us.

For $t \in \mathcal{T}(U)$ and x a variable, define $\lambda^* x.t$ by structural induction as follows:

$$\begin{array}{llll} \lambda^* x.x & \stackrel{\text{def}}{=} & \mathbf{skk}; & \\ \lambda^* x.t & \stackrel{\text{def}}{=} & \mathbf{k}t & \text{if } x \notin \mathsf{FV}(t); \\ \lambda^* x.st & \stackrel{\text{def}}{=} & \mathbf{s}(\lambda^* x.s)(\lambda^* x.t). & \text{if } x \in \mathsf{FV}(st). \end{array}$$

We write $\lambda^* \vec{x}.t$ for $\lambda^* x_1.(\cdots(\lambda^* x_n.t)\cdots)$. This algorithm is known as the *Curry abstraction algorithm.* Note that for any $t \in \mathcal{T}(U)$ with $\mathsf{Var}(t) \subseteq \{x\}$, the polynomial $\lambda^* x.t$ is not necessarily defined in U. For example, in any C-PCA U where there are elements $a, b \in U$ such that $a \cdot b$ is undefined, the polynomial $\lambda^* x.ab \stackrel{\text{def}}{=} \mathbf{k}(ab)$ is undefined. We can show:

Theorem 2.7 (Constructive Characterization) *A partial applicative structure U is a* C-PCA *iff conditional combinatory completeness is valid in U.* □

As an important corollary, we obtain an axiom useful for many "realiser calculations" in the sequel:

(abs) $$\exists a_1, \cdots, a_n \in U.t[\vec{a}/\vec{x}]\downarrow \quad \Longrightarrow \quad \lambda^* \vec{x}.t\downarrow.$$

3 Right-Absorptive C-PCA and Modified Realizability

Recall that our programme to produce a "generic" s.n. proof relies crucially on Hyland's construction which builds a Kleene-style realizability topos $\mathbb{TOP}_s(U)$ out of an arbitrary PCA U. It is helpful to understand the construction from a logical perspective. The topos $\mathbb{TOP}_s(U)$ may be thought of as a constructive set theory according to the Kleene-style realizability interpretation of truth, and the underlying PCA U is just the collection of "realisers". For instance, in the case of the *effective topos* $\mathcal{E}\!f\!f$, the "canonical" realizability topos over the PCA K_1 — "Kleene's first model" of natural numbers, a sentence of Heyting Arithmetic is recursively realised if and only if it is "internally" true of the natural number object of the topos $\mathcal{E}\!f\!f$ (see [Hyl82]).

Hyland's PCA-to-topos construction is actually an instance of a more general construction that yields a class of toposes as studied in Tripos Theory [HJP80]. Formally, a *tripos* (which is an acronym for "Topos Representing Indexed Pre-Ordered Sets") is a structure couched in the language of category theory which ressembles Lawvere's hyperdoctrines. It provides a semantics for typed intuitionistic predicate logic *without* equality. The Fundamental Theorem of Tripos Theory states that:

Every tripos P *gives rise to a topos* P-$\mathbb{SET}$ *of non-standard sets.*

Logically, the passage from a tripos P to the associated topos P-$\mathbb{SET}$ corresponds to the addition of equality and the axiom of extensionality. In essence and this can be made precise, the logic of a tripos P is an "external" (and hence arguably more convenient) but equivalent presentation of the *internal* logic of the associated topos P-$\mathbb{SET}$. In light of Tripos Theory, the PCA-to-topos construction may be re-organised in terms of two stages:

I. Every PCA U yields a "standard" Kleene-style realizability tripos $\mathsf{P}_s(U)$ (subscript "s" for "standard").

II. Every standard realizability tripos $\mathsf{P}_{\mathrm{s}}(U)$ gives rise to an associated standard realizability topos $\mathbb{TOP}_{\mathrm{s}}(U)$, by the Fundamental Theorem of Tripos Theory.

We have established that SN_* — the quotient structure of central interest to our programme — is a C-PCA but not a PCA. If the prescription of stage I above is applied to SN_*, does the process of construction yield a tripos (and in turn, a topos)? Unfortunately, the answer is no and this is because we need the full "structure" of a PCA in order to use its elements as "realisers" for a *Kleene*-style realizability interpretation of intuitionistic predicate logic (which is what stage I is all about). We will now explain why this is so.

Scott Implication Let U be a C-PCA. We define *Scott implication*, a binary operation $\to$ on the powerset of U as follows: for $P, Q \subseteq U$,

$$(P \to Q) \quad \stackrel{\text{def}}{=} \quad \{\, u \in U : \forall a \in P. ua{\downarrow} \ \& \ ua \in Q \,\}.$$

Reading subsets of U as "propositions", Scott implication is the precise semantic counterpart of Kleene's realizability interpretation of implication. Now assume that the axiom $(\mathbf{S}_2)$ is not valid in U. We claim that U is inadequate as realisers for a Kleene-style realizability interpretation of intuitionistic predicate logic. To show this, it suffices to show that Scott implication over U does not model minimal logic. Suppose, for a contradiction, it does. Then for any $P, Q, R \subseteq U$, the following subset

$$V \quad \stackrel{\text{def}}{=} \quad (P \to Q \to R) \to (P \to Q) \to (P \to R)$$

is non-empty and contains the element $\mathbf{s}$. Take $P \equiv \varnothing$ and V degenerates to $U \to U \to U$. Clearly, $\mathbf{s} \in U \to U \to U$ if and only if $(\mathbf{S}_2)$ is valid. The following lemma gives further properties of Scott implication over C-PCAs: note the extent to which they are weaker (*vide* non-emptyness assumption in (iii)) than those of the same notion defined over PCAs.

Lemma 3.1 *For any* C-PCA U *and for any* $P, Q, R \subseteq U$,

(i) $P = \varnothing \implies (P \to Q) = U$. *Suppose there are some* $a, b \in U$ *for which* ab *is undefined and that the axiom* $(\mathbf{S}_2)$ *holds, then the converse is also valid.*

(ii) $\mathbf{k} \in P \to (Q \to P)$.

(iii) $P, Q \neq \varnothing \implies \mathbf{s} \in (P \to (Q \to R)) \to ((P \to Q) \to (P \to R))$.

The non-emptyness assumption in (iii) is indispensable. □

This above observation leads us to consider a more intensional variant of the "standard" realizability interpretation; that of *modified realizability* in the style of Kreisel [Kre59, Tro73]. In the following, we shall present modified realizability in the general framework of a *right-absorptive* C-PCA.

Definition 3.2 Let $\langle U, \cdot \rangle$ be a partial applicative structure. For any non-empty subset Θ of U, we say that Θ is *right-absorptive* if $\forall \theta \in \Theta. \forall u \in U. \theta u{\downarrow} \ \& \ \theta u \in \Theta$. Informally, the subset Θ is a right-ideal of U *i.e.* $\Theta \cdot U \subseteq \Theta$. We call a C-PCA U *right-absorptive* if U has a right-absorptive subset.

The point of right-absorptiveness is this: supersets of any right-absorptive subset Θ are closed under the operation of Scott implication. More precisely, let Θ be a non-empty subset of a C-PCA U. Then

$$\Theta \text{ is right-absorptive} \quad \iff \quad \forall Q, P \subseteq U.[\Theta \subseteq Q \implies \Theta \subseteq (P \to Q)].$$

Clearly, if a C-PCA U has a *right-absorptive element* θ *i.e.* $\forall u \in U.\theta u{\downarrow}$ & $\theta u = \theta$; then the singleton set $\{\theta\}$ is a right-absorptive subset of U.

Example A C-PCA may have more than one right-absorptive subset or it may have none. Consider the C-PCA of closed β-equivalent untyped λ-terms (which is actually a λ-model and so, is *a fortiori* a total combinatory algebra): it has a right-absorptive element $\mathbf{YK}$ where $\mathbf{Y}$ is the paradoxical combinator $\lambda f.(\lambda x.f(xx))(\lambda x.f(xx))$. It may be helpful to think of $\mathbf{YK}$ as the "solution" to the recursive equation $\mathsf{X} = \lambda x.\mathsf{X}$ in meta-variable X. The collection of all elements with *unbounded order*[6] forms a further right-absorptive subset.

Not every C-PCA is right-absorptive.

Proposition 3.3 *(i) The pure untyped s.n. λ-terms quotiented with $\sim_{\mathrm{cl}}$ is not right-absorptive.*

(ii) SN_* *has a right-absorptive subset* $\Theta \stackrel{\mathrm{def}}{=} \{ *\vec{u} : \vec{u} \subseteq \mathsf{SN}_* \}$. □

Definition 3.4 Given a C-PCA U with a right-absorptive subset Θ, a *proof-extension pair* is a pair $P \equiv \langle P_0, P_1 \rangle$ with $P_0, P_1 \subseteq U$ satisfying $\Theta \subseteq P_1$ and $P_0 \subseteq P_1$. Note that by definition $\Theta \neq \varnothing$, and so $P_1 \neq \varnothing$.

We may read a proof-extension pair P as a non-standard proposition with the first component P_0 containing the set of (codes for the) "actual proofs" of the proposition P and the second component P_1 the set of (codes for the) "potential proofs" or "proof extensions" of the proposition. The notion of right-absorptiveness was introduced because the failure of axiom $(\mathbf{S}_2)$ places a serious restriction on the availability and use of the crucial realiser $\mathbf{s}$. This constraint is connected with the non-emptyness assumption in propositions of certain shapes: see Lemma 3.1(iii). We circumvent this problem by modifying the way we model propositions: instead of a set of realisers we think of a proposition as a *pair* of sets of realisers, and *crucially* the second component of each pair is designed to be a superset of Θ and so, it is necessarily non-empty. For this reason, we are forced to consider *right-absorptive* C-PCAs. Now the *pure* s.n. λ-terms are not right-absorptive whereas the s.n. $\lambda*$-terms are (Proposition 3.3) — this is precisely why our programme is built on a quotient of s.n. $\lambda*$-terms (as opposed to the pure terms).

Let $\mathsf{Prf}(U)$ denote the collection of proof-extension pairs over a right-absorptive C-PCA U (w.r.t. a fixed Θ) and we use meta-variables P, Q, R *etc.* to range over $\mathsf{Prf}(U)$. An important property of proof-extension pairs is that they are closed under (component-wise) intersection. For any collection of proof-extensions $\{ A(i) \in \mathsf{Prf}(U) : i \in \mathcal{I} \}$, we define the *intersection* as:

$$\bigcap_{i \in \mathcal{I}} A(i) \quad \stackrel{\mathrm{def}}{=} \quad \langle \bigcap_{i \in \mathcal{I}} A(i)_0, \bigcap_{i \in \mathcal{I}} A(i)_1 \rangle.$$

It is easy to check that $\bigcap_{i \in \mathcal{I}} A(i)$ thus defined is a proof-extension pair.

[6] A λ-term M has *unbounded order* if for any natural number n, however large, there exists a term N such that $M =_\beta \lambda x_1 \cdots x_n.N$. Such a term is always unsolvable, see *e.g.* [Bar84].

Definition 3.5 Let U be a right-absorptive C-PCA. We define *Kreisel implication* $\stackrel{\circ}{\to}$ which is a binary operation on $\mathsf{Prf}(U)$ as follows: for any two proof-extension pairs P and Q,

$$(P \stackrel{\circ}{\to} Q) \quad \stackrel{\text{def}}{=} \quad \langle\, (P_0 \to Q_0) \cap (P_1 \to Q_1), \quad (P_1 \to Q_1)\,\rangle.$$

It is a property of the right-absorptive subset that $(P \stackrel{\circ}{\to} Q)$ thus defined is a proof-extension pair.

Kreisel implication is the precise semantic counterpart of the Kreisel-style modified realizability interpretation of implication, of which more anon.

Modified Realizability Triposes Our aim for the rest of this section is to show that a new class of *modified* realizability triposes $\mathsf{P}_{\mathrm{m}}(U)$ may be systematically constructed from an arbitrary right-absorptive C-PCA U. We shall assume familiarity with the basic notions of Tripos Theory (including the respective definitions of a tripos P and its associated topos P-$\mathbb{SET}$ of non-standard sets) of which the most accessible reference is [HJP80]. For any set I, define $\mathsf{P}_{\mathrm{m}}(I)$ to be $\langle\, \mathsf{Prf}(U)^I, \vdash_I \rangle$, the set of all functions from I to $\mathsf{Prf}(U)$ which is to be thought of as a collection of proof-extension pairs indexed over the set I. The pre-order $\vdash_I$ is defined as

$$A \vdash_I B \quad \stackrel{\text{def}}{=} \quad \bigcap_{i \in I} (A(i) \stackrel{\circ}{\to} B(i))_0 \neq \varnothing.$$

In the case of $I \equiv \varnothing$, we decree that the intersection of a collection of proof-extension pairs indexed over the empty set is $\langle\, U, U\,\rangle$, the largest (w.r.t. inclusion) such pair, as is consistent with convention. If a is a member of the above intersection, we say that a *realises* or *witnesses* $A \vdash_I B$.

We define a binary operation $\stackrel{\circ}{\to}$ on $\mathsf{Prf}(U)^I$ by point-wise extension of $\stackrel{\circ}{\to}$: given $A, B \in \mathsf{Prf}(U)^I$, the map $A \stackrel{\circ}{\to} B$ is defined as $i \mapsto (A(i) \stackrel{\circ}{\to} B(i))$. The structure $\langle\, \mathsf{Prf}(U)^I, \vdash_I \rangle$ is a pre-ordered set: we prove this fact as a corollary of the following lemma.

Lemma 3.6 *Kreisel implication on proof-extension pairs of a right-absorptive* C-PCA *models minimal logic i.e. intuitionistic implication.* □

A bottom element of the preorder $\langle\, \mathsf{Prf}(U)^I, \vdash_I \rangle$ is a map $i \mapsto \langle\, \varnothing, X_i \,\rangle$ for any $X_i \supseteq \Theta$ and for any $i \in I$; a top element is the constant map $i \mapsto \langle\, U, U\,\rangle$; another is the map $i \mapsto \langle\, \{\,\mathbf{i}\,\}, \{\,\mathbf{i}\,\} \cup \Theta\,\rangle$.

We will next show how the universal quantifier is to be interpretated. The interpretation of the other connectives of the logic may then be defined in terms of the interpretation for the implication and the universal quantifier, using a definability result in [HJP80, Theorem 1.4]. Though cast in category-theoretic language, the result in *op. cit.* is essentially the inter-definability result of second order logical connectives which is attributed to Russell, see e.g. [Pra65].

Definition 3.7 Let $f : I \to J$ be a map between sets. Recall that $\mathsf{P}_{\mathrm{m}}(I) \stackrel{\text{def}}{=} \langle\, \mathsf{Prf}(U)^I, \vdash_I \rangle$. We define functors $\mathsf{P}_{\mathrm{m}}(f) : \mathsf{P}_{\mathrm{m}}(J) \to \mathsf{P}_{\mathrm{m}}(I)$ and $\forall f : \mathsf{P}_{\mathrm{m}}(I) \to \mathsf{P}_{\mathrm{m}}(J)$ as follows: for any $A \in \mathsf{Prf}(U)^J$ and $B \in \mathsf{Prf}(U)^I$, $\mathsf{P}_{\mathrm{m}}(f)$ is just composition with f i.e. $(\mathsf{P}_{\mathrm{m}}(f))A(i) \stackrel{\text{def}}{=} A(f(i))$ for any $i \in I$. For any $j \in J$, $(\forall f)B(j)$ is defined as:

$$(\forall f)B(j) \quad \stackrel{\text{def}}{=} \quad \bigcap_i [|f(i) = j| \stackrel{\circ}{\to} B(i)];$$

where

$$|f(i)=j| \quad \stackrel{\text{def}}{=} \quad \begin{cases} \langle \{\mathbf{i}\}, \Theta \cup \{\mathbf{i}\} \rangle & \text{if } f(i)=j, \\ \langle \varnothing, \Theta \rangle & \text{else.} \end{cases}$$

For the case of $I \equiv \varnothing$, $\mathsf{P}_{\mathrm{m}}(I)$ is just the singleton set, note that $(\forall f)B(j) \stackrel{\text{def}}{=} \langle U, U \rangle$ by convention. It is easy to check that $(\forall f)B(j)$ defines a proof-extension pair for each j. We can show that the conditions of Theorem 1.4 in [HJP80] are satisfied. Hence, we have the following theorem.

Theorem 3.8 (Modified Realizability Topos) *Given any right-absorptive* C-PCA U, $\mathsf{P}_{\mathrm{m}}(U)$ *thus defined is a (canonically presented) tripos. Applying the Fundamental Theorem of Tripos Theory, we can then construct the associated* modified realizability topos $\mathbb{TOP}_{\mathrm{m}}(U)$. □

We give a summary of the various constructions that make up a modified realizability tripos $\mathsf{P}_{\mathrm{m}}(U)$ over a right-absorptive C-PCA U. Let I be a set, for any $A, B \in \mathsf{Prf}(U)^I$ and any set-theoretic function $f : I \to J$:

$$\begin{aligned}
(A \times B)(i) &\stackrel{\text{def}}{=} \textstyle\bigcap_{X \in \mathsf{Prf}(U)}((A(i) \stackrel{\circ}{\to} B(i) \stackrel{\circ}{\to} X) \stackrel{\circ}{\to} X) \\
(A + B)(i) &\stackrel{\text{def}}{=} \textstyle\bigcap_{X \in \mathsf{Prf}(U)}(A(i) \stackrel{\circ}{\to} X) \stackrel{\circ}{\to} (B(i) \stackrel{\circ}{\to} X) \stackrel{\circ}{\to} X), \\
(A \stackrel{\circ}{\to} B)(i) &\stackrel{\text{def}}{=} A(i) \stackrel{\circ}{\to} B(i), \\
(\forall f)A(j) &\stackrel{\text{def}}{=} \textstyle\bigcap_i [|f(i)=j| \stackrel{\circ}{\to} A(i)], \\
(\exists f)A(j) &\stackrel{\text{def}}{=} \textstyle\bigcup_i [|f(i)=j| \times A(i)].
\end{aligned}$$

Since the meaning of $(\exists f)A(j)$ involves indexed union, we decree that union of proof-extension pairs indexed over the emptyset is the least (w.r.t. inclusion) proof-extension pair $\langle \varnothing, \Theta \rangle$.

4 Modified Realizability Toposes

We already know some general properties of P-$\mathbb{SET}$, the topos of non-standard sets associated with an arbitrary tripos P from [HJP80]. In addition, an in-depth study of a particular realizability topos $\mathcal{E}\!f\!f$, the *effective topos* has been carried out in [Hyl82]. This section presents a summary of the properties of $\mathbb{TOP}_{\mathrm{m}}(U)$ where U is any right-absorptive C-PCA.

Embeddings of $\mathbb{SET}$ into $\mathbb{TOP}_{\mathrm{m}}(U)$ The topos $\mathbb{TOP}_{\mathrm{m}}(U)$ is a category of sets equipped with a $\mathsf{Prf}(U)$-valued equality predicate. Unlike the standard realizability toposes, there are two canonical embeddings of $\mathbb{SET}$ into $\mathbb{TOP}_{\mathrm{m}}(U)$ which we shall refer to as type **I** and type **II** embeddings respectively. In particular, the type **II** embedding is a topos inclusion.

Type I Embedding: $\Delta : \mathbb{SET} \to \mathbb{TOP}_{\mathrm{m}}(U)$ Write $\mathbb{T} \stackrel{\text{def}}{=} \langle \{\mathbf{i}\}, \{\mathbf{i}\} \cup \Theta \rangle$ and $\mathbb{F} \stackrel{\text{def}}{=} \langle \varnothing, \Theta \rangle$. For any set X, the image ΔX has X as the underlying set; the equality predicate $=$ is defined as follows: for any $x, y \in X$,

$$[\![x = y]\!] \quad \stackrel{\text{def}}{=} \quad \begin{cases} \mathbb{T} & \text{if } x = y, \\ \mathbb{F} & \text{else.} \end{cases}$$

For any set-theoretic function $f : X \to Y$, we define a functional relation $\Delta f : X \times Y \to \mathsf{Prf}(U)$ by: for any $x \in X$ and $y \in Y$,

$$\Delta f(x,y) \quad \stackrel{\text{def}}{=} \quad \begin{cases} \mathbb{T} & \text{if } f(x) = y, \\ \mathbb{F} & \text{else.} \end{cases}$$

Note that the designated truth values $\mathbb{T}$ and $\mathbb{F}$ are identical to those in Definition 3.7. The data associated with Δ may be cast in tripos-theoretic language: for any map $f : X \to Y$ in $\mathbb{SET}$, ΔX is just the object $\langle X, \exists\Delta_X(\top_X) \rangle$ where $\Delta_X : X \to X \times X$ is the diagonal map, $\top_X$ is the constant map sending $x \in X$ to $\langle U, U \rangle$; and $\Delta f : \Delta X \to \Delta Y$ is equivalent to $\exists(\mathbf{1}_X, f)(\top_X) \in \mathsf{Prf}(U)^{X \times Y}$.

Proposition 4.1 *The functor $\Delta : \mathbb{SET} \to \mathbb{TOP}_{\mathrm{m}}(U)$ is full and faithful, and left-exact. Further, every object $\langle X, = \rangle$ of the topos $\mathbb{TOP}_{\mathrm{m}}(U)$ is a quotient of a subobject of the object ΔX.* $\square$

Type II Embedding: topos inclusion $\nabla : \mathbb{SET} \to \mathbb{TOP}_{\mathrm{m}}(U)$ We spell out the inverse and direct image functors of the geometric morphism: $\Gamma \dashv \nabla$.

Direct Image Functor: $\nabla : \mathbb{SET} \hookrightarrow \mathbb{TOP}_{\mathrm{m}}(U)$ is defined in exactly the same way as the functor Δ except in place of $\mathbb{F}$, we use $\mathbb{F}^+ \stackrel{\text{def}}{=} \langle \varnothing, \Theta \cup \{\, \mathbf{i} \,\} \rangle$. Since adjunction is defined up to isomorphism, replacing the pair $(\mathbb{T}, \mathbb{F}^+)$ in the definition by another equivalent (in $\langle \mathsf{Prf}(U)^{\mathbf{2}}, \vdash_{\mathbf{2}} \rangle$) pair of proof-extension pairs say $(\langle U, U \rangle, \langle \varnothing, U \rangle)$, defines the same direct image functor.

Inverse Image Functor: $\Gamma : \mathbb{TOP}_{\mathrm{m}}(U) \to \mathbb{SET}$ is just the global sections functor:

- *objects*: for any $\langle X, = \rangle \in \mathbb{TOP}_{\mathrm{m}}(U)$, the image under Γ is the set $\Gamma\langle X, = \rangle \stackrel{\text{def}}{=} \{\, x : [\![x]\!] \neq \varnothing \,\}/\simeq$ where $x \simeq x' \stackrel{\text{def}}{=} [\![x = x']\!] \neq \varnothing$. We write $[x]_\simeq$ for the $\simeq$-equivalence class of x as an element of $\Gamma\langle X, = \rangle$.
- *morphisms*: for any morphism $F : \langle X, = \rangle \to \langle Y, = \rangle \in \mathbb{TOP}_{\mathrm{m}}(U)$, its image under Γ is the set-theoretic function $\Gamma F : \Gamma\langle X, = \rangle \to \Gamma\langle Y, = \rangle$ with $\Gamma F([x]_\simeq) \stackrel{\text{def}}{=} [y]_\simeq$ for any y such that $F(x,y) \neq \varnothing$. Such a y is guaranteed to exist by the requirement of totality on the functional relation F.

Theorem 4.2 *The functor $\nabla : \mathbb{SET} \hookrightarrow \mathbb{TOP}_{\mathrm{m}}(U)$ is a topos inclusion.* $\square$

The above topos inclusion is the canonical inclusion of $\mathbb{SET}$ into the modified realizability topos $\mathbb{TOP}_{\mathrm{m}}(U)$. We know from the work of Hyland *et al.* ([HJP80, Corollary 4.6]) that in general, any arbitrary tripos which is $\exists$-*standard* (which $\mathsf{P}_{\mathrm{m}}(U)$ is) gives rise to just such a topos inclusion which is defined entirely by the logical properties of the tripos.

Double-Negation Topology Given the topos inclusion of $\mathbb{SET}$ into $\mathbb{TOP}_{\mathrm{m}}(U)$, by a theorem of Lawvere and Tierney (see *e.g.* Theorem 4.14 and Proposition 4.15 in [Joh77, pp. 104 – 105]), there is a unique Lawvere-Tierney topology j in $\mathbb{TOP}_{\mathrm{m}}(U)$ such that $\mathbb{SET} \simeq \mathrm{Shv}_j(\mathbb{TOP}_{\mathrm{m}}(U))$, where $\mathrm{Shv}_j(\mathbb{C})$ denotes the category of j-sheaves of the category $\mathbb{C}$. The topology j in question is the double negation topology.

Proposition 4.3 *For any right-absorptive* C-PCA, $\mathbb{SET} \simeq \mathrm{Shv}_{\neg\neg}(\mathbb{TOP}_{\mathrm{m}}(U))$. $\square$

¬¬-Seperated Objects Let j be a Lawvere-Tierney topology over a topos $\mathbb{E}$. Recall the result that the inclusion functor $\nabla : \mathrm{Shv}_j(\mathbb{E}) \hookrightarrow \mathbb{E}$ has a left-adjoint $\mathbf{a} : \mathbb{E} \to \mathrm{Shv}_j(\mathbb{E})$ called the *sheafification functor* which is left-exact.

Recall also the following equivalent characterizations of a j-separated object A.

(1) the diagonal $\Delta_A : A \rightarrowtail A \times A$ is a j-closed subobject of $A \times A$,

(2) the unit of the adjunction $\eta_A : A \to \nabla(\mathbf{a}A)$ is monic,

(3) for any j-dense subobject $E \rightarrowtail X$, whenever the partial map $X \leftarrowtail E \to A$ extends to a total map $X \to A$, the extension is unique.

Let X be a map. A map $R \in \mathsf{Prf}(U)^X$ is said to be *1-stable*, or simply *stable* if for any $x, y \in X$, $R(x)_1 = R(y)_1$. Stable maps characterize strict relations over sheaves in the sense which we will now clarify. For an arbitrary strict relation $R \in \mathsf{Prf}(U)^X$ over the sheaf ∇X, define a new map $\overline{R} \in \mathsf{Prf}(U)^X$ from R by fixing the second component: for each $x \in X$,

$$\overline{R}(x) \quad \stackrel{\mathrm{def}}{=} \quad \langle\, R(x)_0, \bigcup_{y \in X} R(y)_1 \,\rangle.$$

We claim: $\mathsf{P}_{\mathrm{m}}(U) \vDash \forall x \in X. R(x) \leftrightarrow \overline{R}(x)$. Since there is a 1-1 correspondence between monics into an object and strict relations over it, we see that there is a 1-1 correspondence between subobjects of the sheaf ∇X and stable maps $R \in \mathsf{Prf}(U)^X$ for any set X.

Definition 4.4 An object $\langle\, X, = \rangle$ of the topos $\mathbb{TOP}_{\mathrm{m}}(U)$ is said to be *canonically separated* if there is a stable map $R \in \mathsf{Prf}(U)^X$ such that for any $x, y \in X$

$$[\![\, x = y \,]\!] \quad \stackrel{\mathrm{def}}{=} \quad \begin{cases} R(x) & \text{if } x = y, \\ \langle\, \varnothing, R(x)_1 \,\rangle & \text{else.} \end{cases}$$

Note that by definition of stability, $R(x)_1$ is constant as x varies over X. It is not difficult to check that the above data specifies a well-defined object of $\mathbb{TOP}_{\mathrm{m}}(U)$.

Proposition 4.5 *An object of $\mathbb{TOP}_{\mathrm{m}}(U)$ is ¬¬-separated iff it is isomorphic to a canonically separated object.* □

Validity of Constructive Principles Modified realizability was introduced by Kreisel [Kre59, Tro73] as an intensional variant of the Kleene-style realizability interpretation. The most distinctive feature of modified realizability is that it provides a setting in which the *Markov Principle* ($\mathbf{MP}_{\mathrm{pr}}$)

($\mathbf{MP}_{\mathrm{pr}}$) $\qquad \neg\neg\exists x \in \mathbb{N}.A \quad \to \quad \exists x \in \mathbb{N}.A \qquad A$ is primitive recursive.

is invalidated.

Theorem 4.6 *(i) The* Independence of Premise (**IP**) *axiom is internally valid in $\mathbb{TOP}_{\mathrm{m}}(U)$ for any right-absorptive* C-PCA *U: for any B, and A in which y is not free,*

(**IP**) $\qquad \neg A \to \exists y \in \mathbb{N}.B \quad \to \quad \exists y \in \mathbb{N}.(\neg A \to B)$

(ii) Church's Thesis ($\mathbf{CT}_0$) *is internally valid in* $\mathbb{TOP}_{\mathrm{m}}(\mathsf{K}_1)$, *where the* PCA K_1 *is "Kleene's first model" of natural numbers and where* T *and* U *are Kleene's* T*-predicate and output function respectively:*

$$(\mathbf{CT}_0) \qquad \forall x.\exists y.B(x,y) \quad \rightarrow \quad \exists e.\forall x.\exists z.[\mathrm{T}(e,x,z) \wedge B(x,\mathrm{U}(z))]$$

□

Since $\mathbf{HA} + \mathbf{IP} + \mathbf{CT}_0 + \mathbf{MP}_{\mathrm{pr}}$ is inconsistent (see [Tro73]), we infer that $\mathbf{MP}_{\mathrm{pr}}$ is invalid in $\mathbb{TOP}_{\mathrm{m}}(\mathbb{N})$. Here, it is appropriate to mention an unpublished manuscript of Grayson [Gra81] which provides sketchy details of a modified realizability topos (based on the tripos construction) and the more recent work [vO91, Str92].

PERS-Extension Pairs The collection $\mathbb{PER}(U)$ (as defined in the Introduction) of PERs over a *proper* C-PCA U (*i.e.* one in which ($\mathbf{S}_2$) fails) does not form a category since the axiom ($\mathbf{S}_2$) is needed to establish closure of composition. What then is the right notion of "PERs" (and "modest sets") in the modified realizability setting?

A PER-*extension pair* over a right-absorptive C-PCA U is a pair $\langle R, \overline{R} \rangle$ where R is a PER over U and $\mathrm{dom}(R) \subseteq \overline{R} \supseteq \Theta$. We define $\mathbb{P}_{\mathrm{ext}}(U)$, the category of PER-extension pairs over U as follows:

- *objects*: PER-extension pairs $\langle R, \overline{R} \rangle$,
- *morphisms*: $F : \langle R, \overline{R} \rangle \rightarrow \langle S, \overline{S} \rangle$ where F is a function from $[R]$ (R-equivalence classes) to $[S]$ such that F is *realised* by some $f \in U$ *i.e.* for any $r, r' \in U$, whenever $r\, R\, r'$ then $(fr)\, S\, (fr')$ and $F[r]_R = [fr]_S$, *and* $f \in (\overline{R} \rightarrow \overline{S})$. Two such realisers f and g are equivalent, written $f \sim g$ iff for any $r \in \mathrm{dom}(R)$, $(fr)\, S\, (gr)$, so F is characterised by $[f]_\sim$.

Lemma 4.7 *The above data defines a category* $\mathbb{P}_{\mathrm{ext}}(U)$ *which is Cartesian closed.* □

For instance, for any PER-extension pairs $\langle R, \overline{R} \rangle$ and $\langle S, \overline{S} \rangle$, the exponential $\langle S, \overline{S} \rangle^{\langle R, \overline{R} \rangle}$ has as the first component a PER T whose domain is $\{ e \in U : e$ realises a morphism $R \rightarrow S \}$ and $e\, T\, e'$ iff $e \sim e'$; the second component is just $\overline{R} \rightarrow \overline{S}$.

Fibration of $\mathbb{P}_{\mathrm{ext}}(U)$ over $\mathbb{SET}$ For each set I, define the following category $(\mathbb{P}_{\mathrm{ext}}(U))_I$:

- *objects*: I-indexed families of PER-extension pairs $\{ \langle R_i, \overline{R_i} \rangle \}_{i \in I}$,
- *morphisms*: $[e]_\sim : \{ \langle R_i, \overline{R_i} \rangle \}_{i \in I} \rightarrow \{ \langle S_i, \overline{S_i} \rangle \}_{i \in I}$ where for each $i \in I$, e realises a morphism $\langle R_i, \overline{R_i} \rangle \rightarrow \langle S_i, \overline{S_i} \rangle$; and $e \sim e'$ iff for each $i \in I$, $e \sim e'$ as realisers of morphisms from $\langle R_i, \overline{R_i} \rangle$ to $\langle S_i, \overline{S_i} \rangle$.

Theorem 4.8 *The above data defines a cloven fibration* $\begin{smallmatrix}\mathbb{P}_{\mathrm{ext}}(U)\\ \downarrow \\ \mathbb{SET}\end{smallmatrix}$ *which is complete i.e.*

(i) *each fibre* $(\mathbb{P}_{\mathrm{ext}}(U))_I$ *has finite limits and reindexing functors preserve limits,*

(ii) *for each morphism* $\phi : I \rightarrow J$ *in* $\mathbb{SET}$, ϕ^* *has a right adjoint* Π_ϕ *satisfying the Beck-Chevalley condition,*

and it has a generic object. □

5 "Generic" S.N. Argument: an application

As an application of the machinery which we have set up, consider the s.n. argument of System F. First, note that the fibration $\begin{smallmatrix}\mathbb{P}_{\mathrm{ext}}(U)\\ \downarrow\\ \mathbb{SET}\end{smallmatrix}$ satisfies all the structural requirements of a category-theoretic model for System F (as spelt out in the Introduction). For any derivable type-assignment sequent of the form $x_1 : \sigma, \cdots, x_n : \sigma_n \vdash_{\vec{X}} s : \tau$ where the free type variables of $\sigma_1, \cdots, \sigma_n, \tau$ are a subset of $\{\vec{X}\}$, we can establish the *realiser argument* (the first of the "stripping arguments") by a straightforward induction:

Lemma 5.1 (Realiser) *For any derivable sequent $x_1 : \sigma_1, \cdots, x_n : \sigma_n \vdash_{\vec{X}} s : \tau$, the untyped term $\lambda\xi.\lambda x_1 \cdots x_n.\lceil s \rceil$ (where $\lceil s \rceil$ is obtained from s by stripping off all embedded type expression) realises the following morphism*

$$[\![\, \vec{x} : \vec{\sigma} \vdash_{\vec{X}} s : \tau \,]\!] \quad : \quad [\![\, \vec{X}; \mathbf{1} \,]\!] \times [\![\, \vec{X}; \sigma_1 \,]\!] \times \cdots \times [\![\, \vec{X}; \sigma_n \,]\!] \quad \rightarrow \quad [\![\, \vec{X}; \tau \,]\!]$$

in the fibre over $(\mathbb{P}_{\mathrm{ext}}(U))^m$ where m is the length of $\vec{X}$. □

To see the validity of the *reflection argument*, note that the term-β reduction in System F corresponds precisely to β-reduction of the stripped terms. Moreover, the type-β reduction leaves the corresponding stripped terms unchanged. The argument for the s.n. of System F is now complete.

Further Directions Does the above argument establish s.n. of the Calculus of Constructions? We can show that the category of PER-extension pairs is strongly complete (see *e.g.* [HRR90]) as a fibration over an appropriate category of *assemblies* (*not* equivalent to the category of $\neg\neg$-separated objects) thus giving rise to a model of the calculus and much more. The stripping arguments therein are valid and the details will be presented elsewhere. The challenge that remains is to show that this approach is systematically applicable to the family of Generalized Type Systems *i.e.* Barendregt's "cube" [Bar91].

Until and unless we can establish the general applicability of the two "stripping arguments", or demonstrate that they are easily verifiable for a significant class of type theories, we cannot properly claim to have a generic s.n. proof.

References

[B8́5] J. Bénabou. Fibred categories and the foundations of naïve category theory. *J. Symb. Logic*, pages 10–37, 1985.

[Bar84] H. Barendregt. *The Lambda Calculus.* North-Holland, revised edition, 1984.

[Bar91] H. Barendregt. Introduction to generalized type systems. *J. Functional Prog.*, 1:125–154, 1991.

[Bee85] M. J. Beeson. *Foundations of Constructive Mathematics.* Springer-Verlag, 1985.

[Bet87] I. Bethke. On the existence of extensional partial combinatory algebras. *J. Symb. Logic*, pages 819–833, 1987.

[CH88] T. Coquand and G. Huet. The Calculus of Constructions. *Info. and Comp.*, 76:95–120, 1988.

[Gal90] J. Gallier. On Girard's "Candidats de Réductibilité". In P. Odifreddi, editor, *Logic and Computer Science*. Academic Press, 1990.

[Gir72] J.-Y. Girard. Interprétation fonctionelle et elimination des coupures dans l'arithmetíque d'order supérieur. Thèse de Doctorat d'Etat, Paris, 1972.

[Gir86] J.-Y. Girard. The system F of variable types, fifteen years later. *Theoretical Computer Science*, 45:159–192, 1986.

[Gra81] R. Grayson. Modified realizability toposes. unpublished manuscipt, 1981.

[HJP80] J. M. E. Hyland, P. T. Johnstone, and A. M. Pitts. Tripos theory. *Math. Proc. Camb. Phil. Soc.*, 88:205 –232, 1980.

[HP89] J. M. E. Hyland and A. M. Pitts. The theory of constructions: Categorical semantics and topos-theoretic models. *Contemporary Mathematics*, 92:137–199, 1989.

[HRR90] J. M. E. Hyland, E. P. Robinson, and G. Rosolini. The discrete objects in the effective topos. *Proc. London Math. Soc. (3)*, 60:1–36, 1990.

[Hyl82] J. M. E. Hyland. The effective topos. In *The L. E. J. Brouwer Centenary Symposium*, pages 165–216. North-Holland, 1982.

[Hyl88] J. M. E. Hyland. A small complete category. *Annals of Pure and Applied Logic*, 40:135–165, 1988.

[Joh77] P. T. Johnstone. *Topos Theory*. Academic Press, 1977. L.M.S. Monograph No. 10.

[Kre59] G. Kreisel. Interpretation of analysis by means of constructive functionals of finite type. In A Heyting, editor, *Constructivity in Mathematics*. North-Holland, 1959.

[LS86] J. Lambek and P. J. Scott. *Introduction to Higher Order Categorical Logic*. Cambridge Studies in Advanced Mathematics No. 7. Cambridge University Press, 1986.

[ML73] P. Martin-Löf. An intuitionistic theory of types: Predicative part. In Rose and Shepherdson, editors, *Logic Colloquium '73*. North-Holland, 1973.

[ML84] P. Martin-Löf. *Intuitionistic Type Theory*. Bibliopolis, 1984. Studies in Proof Theory Series.

[Pit87] A. M. Pitts. Polymorphism is set-theoretical, constructively. In D. H. Pitt *et al.*, editor, *Proc. Conf. Category Theory and Computer Science, Edinburgh*, Berlin, 1987. Springer-Verlag. LNCS. Vol. 287.

[Pra65] D. Prawitz. *Natural Deduction*. Almqvist and Wiksell, 1965. Stockholm Studies in Philosophy 3.

[Rey74] J. C. Reynolds. Towards a theory of type structure. In B. Robinet, editor, *Colloque sur la Programmation*, pages 405–425. Springer-Verlag, 1974. Lecture Notes in Computer Science Vol. 19.

[Sce89] A. Scedrov. Normalization revisited. In J. W. Gray and A. Scedrov, editors, *Categories in Computer Science and Logic*, pages 357 – 369. AMS, 1989.

[See87] R. A. G. Seely. Categorical semantics for higher order polymorphic lambda calculus. *J. Symb. Logic*, 52:969–989, 1987.

[Str92] T. Streicher. Truly intensional models of type theory arising from modified realizability. dated 25 May '92 mailing list at `CATEGORIES@mta.ca`, 1992.

[Tai67] W. W. Tait. Intensional interpretation of functionals of finite type i. *J. Symb. Logic*, 32:198–212, 1967.

[Tai75] W. W. Tait. A realizability interpretation of the theory of species. In *Logic Colloquium*. Springer-Verlag, 1975. Lecture Notes in Mathematics Vol. 453.

[Tro73] A. Troelstra. *Metamathematical Investigation of Intuitionistic Arithmetic and Analysis*. Springer, 1973. Springer Lecture Notes in Mathematics 344.

[vO91] J. van Oosten. *Exercises in Realizability*. PhD thesis, University of Amsterdam, 1991.