A nominal exploration of intuitionism
Rahli, Vincent; Bickford, Mark

DOI:
10.1145/2854065.2854077

License:
Other (please specify with Rights Statement)

Document Version
Peer reviewed version

Citation for published version (Harvard):

Link to publication on Research at Birmingham portal

Publisher Rights Statement:
Checked for eligibility: 23/07/2019

© ACM 2016. This is the author's version of the work. It is posted here for your personal use. Not for redistribution. The definitive Version of Record was published in CPP 2016 Proceedings of the 5th ACM SIGPLAN Conference on Certified Programs and Proofs, http://dx.doi.org/10.1145/2854065.2854077.

General rights
Unless a licence is specified above, all rights (including copyright and moral rights) in this document are retained by the authors and/or the copyright holders. The express permission of the copyright holder must be obtained for any use of this material other than for purposes permitted by law.

• Users may freely distribute the URL that is used to identify this publication.
• Users may download and/or print one copy of the publication from the University of Birmingham research portal for the purpose of private study or non-commercial research.
• Users may use extracts from the document in line with the concept of ‘fair dealing’ under the Copyright, Designs and Patents Act 1988 (?)
• Users may not further distribute the material nor use it for the purposes of commercial gain.

Where a licence is displayed above, please note the terms and conditions of the licence govern your use of this document.

When citing, please reference the published version.

Take down policy
While the University of Birmingham exercises care and attention in making items available there are rare occasions when an item has been uploaded in error or has been deemed to be commercially or otherwise sensitive.

If you believe that this is the case for this document, please contact UBIRA@lists.bham.ac.uk providing details and we will remove access to the work immediately and investigate.

Download date: 01. Nov. 2021
Abstract
This paper extends the Nuprl proof assistant (a system representative of the class of extensional type theories à la Martin-Löf) with named exceptions and handlers, as well as a nominal fresh operator. Using these new features, we prove a version of Brouwer’s Continuity Principle for numbers. We also provide a simpler proof of a weaker version of this principle that only uses diverging terms. We prove these two principles in Nuprl’s meta-theory using our formalization of Nuprl in Coq and show how we can reflect these meta-theoretical results in the Nuprl theory as derivation rules. We also show that these additions preserve Nuprl’s key meta-theoretical results in the Nuprl theory as derivation rules. We also provide a simpler proof of a continuity Principle for numbers. We also provide a simpler proof of a continuum principle of the class of extensional type theories à la Martin-Löf) with nominality Principle for numbers. We also provide a simpler proof of a continuity Principle for numbers.

Keywords: Intuitionistic Type Theory, Nuprl, Coq, Continuity, Nominal Type Theory, Exceptions, Squashing, Truncation

1. Introduction
Continuity. There are two principles that distinguish Brouwer’s mathematics from other constructive mathematics, namely bar induction and a continuity principle. In this document we consider the following weak and strong continuity principles on the Baire space $B = N^N = N 	o N$ (II, $\Sigma$ are the logical $\forall, \exists$; as explained below, $\Sigma$ is a truncated/squashed existential quantifier; $+$ in the context of types is the disjoint union type; $\inl$ is the left injection constructor; $\inl$ checks whether a term is a left injection; $N_*$ is the type of natural numbers strictly less than $n$; and $t =_T u$ expresses that $t$ and $u$ are equal in type $T$):

$$WCP = \Pi F : B \to N, \Pi f : B, \Sigma n : N, \Pi g : B. f =_{\Sigma n} g \to F(f) =_{\Sigma n} F(g)$$

This work was partially supported by the SnT and the National Research Fund Luxembourg (FNR), through PEARL grant FNR/P14/8149128.

SCP = $\Pi : F : B \to N, \Sigma M : (\Pi n : N. N^N_n \to (N + Unit))$. \[ \Sigma f : B. \]

$M n f =_{N + Unit} inl(F(f)) \land \Sigma m : N. inl(M m f) \to m =_N n$

WCP is the usual pointwise continuity principle on natural numbers, sometimes called weak continuity principle. It says that given a function $F$ of type $B \to N$ and a function $f$ of type $B$, $F(f)$ can only depend on an initial segment of $f$. The length of the smallest such segment is called the modulus of continuity of $F$ at $f$. Kleene used some version of the strong continuity principle SCP to prove bar induction on monotone bars from bar induction on decidable bars. SCP says that there is a uniform way (called $M$ in the formula) to decide whether $n$ is the modulus of continuity of $F$ at $f$, and if so returns the value $F(f)$.

Truncation/Squashing. Escardó and Xu proved in Agda that SCP is false when $\Sigma$ is the sum type $\Sigma$ of Martin-Löf’s type theory. They also mention that this principle is consistent when $\Sigma$ is truncated at the propositional level. In Nuprl, propositional truncation corresponds to squashing a type down to a single equivalence class (i.e., all inhabitants are equal) using quotient types. SCP: $|T| = T/\text{True}$, $T$ is a proof-irrelevant type. Its members are the members of $T$, and they are all equal to each other because if $x, y \in T$ then $(x =_T y \iff \text{True})$. In Nuprl we often squash types in a much stronger sense by throwing away the evidence that a type is inhabited and squashing it down to a single inhabitant using, e.g., set types: $\downarrow T = \{ \text{Unit} | T \}$ (this is the same definition as in [28, pp.60]). The only member of this type is $\text{Unit}$ which is the single inhabitant of $\text{Unit}$, and $\ast$ inhabits $T$ if $T$ is true/inhabited, but we do not keep the proof that it is true. Note that $T \to \downarrow T$ is true because it is inhabited by $\lambda x. \ast$, but we cannot prove the converse because to prove $T$ we have to exhibit an inhabitant of $T$, which $\downarrow T$ does not give us because we have thrown away the evidence that $T$ is inhabited (only $\ast$ inhabits $T$).

In this paper we prove that versions of WCP and SCP are true facts about Nuprl’s functions. We carry out these proofs in Nuprl’s meta-theory using our formalization of Nuprl in Coq, which contains among other things: (1) an implementation

1. Rathjen calls it “Strong Continuity for Numbers” and names it C-N (as in [62]). Dunnett refers to it as “a stronger version of the Continuity Principle”, names it $CP_{\text{SN}}$, and later calls it “the Continuity Principle” [57, pp.59–60]. Troelstra [63, pp.100.06] calls it $\text{CONT}_0$. This is Kleene’s “27.2 principle” [53, pp.73], which he calls “Brouwer’s principle (for numbers)”. Bridges and Richman [19, pp.119] mention that SCP is equivalent to a “principle of continuous choice”, which they divide into a continuous part, namely WCP, and a choice part, namely the axiom of choice $\text{AC}_{1,0}$ (see Sec $\text{L}$). Note that $\text{AC}_{1,0}$ is also sometimes used to refer to SCP [45, 60].

2. The term $\ast$ can be thought of as $\perp$ in, e.g., OCaml, Haskell or SML.
of Nuprl’s computation system; (2) an implementation of Howe’s computational equivalence relation \([5, 8]\) and a proof that it is a congruence; (3) a definition of Nuprl’s Constructive Type Theory (CTT), where types are defined as Partial Equivalence Relations (PERs) on closed terms following Allen’s PER semantics \([4, 5]\); (4) definitions of Nuprl’s derivation rules and proofs that these rules are valid w.r.t. Allen’s PER semantics; (5) a proof of Nuprl’s consistency \([3, 9]\).

In Sec. 3 we prove \(\Pi SCP\) where \(\Pi SCP\) is defined as \(\downarrow T.P\), and refer to this principle as \(\Pi SCP\). We call \(SCP\), the version of \(SCP\) where \(\Sigma j\) is \(\Sigma k\). In Sec. 4 we prove \(SCP\) where the first (outer) \(\Sigma j\) is \(\downarrow \Sigma j\) and the second (inner) is \(\Sigma k\), and refer to this principle as \(SCP\). There proofs are carried out using our Coq formalization of Nuprl. We make these results available in Nuprl as inference rules, and show how we can derive directly in Nuprl a proof of \(\Pi SCP\) without the second (inner) squashing operator. Sec 5 shows that \(SCP\) and \(SCP\) are equivalent. Even though the implication \(SCP\) is trivial, we believe our proof of \(SCP\) in Sec. 3 is still valuable because of its simplicity and because \(\Pi SCP\) is often enough.

An important point is that we add operations sufficient to prove these principles to the Nuprl proof assistant without breaking any property of its type theory such as Nuprl’s consistency or the congruence of Howe’s computational equivalence relation.

Effectful computations. Following Longley’s method \([59]\), we use computational effects \([11]\), namely named exceptions, to derive \(SCP\). The basic method to find the \(n\) such that \(F(f)\) depends only on the first \(n\) elements of \(f\) is a program \(P(F, f)\) that works as follows: \(P\) tests whether \(F\) applies its argument \(f\) to a number \(n\) by running the sub-routine (written in an ML-like language):

\[
\text{let exception e in } (F (\text{fun } x \Rightarrow \text{if } x < n \text{ then } f \times \text{else raise e } ) ; true \text{ handle e } \Rightarrow \text{false})
\]

Then by testing \(F\) on increasingly larger \(n\)’s, if the continuity principle is true, \(P\) eventually finds an \(n\) such that the test returns true\(^4\). However, for extensionally equal \(F\) and \(G\), \(P(F, f)\) and \(P(G, f)\) could return different numbers. For example, if \((F(f), m)\) and \((G(f), n)\) is constructed from \(F\) by replacing an expression \(t\) occurring in \(F\) with \((\text{let } x := f(m + 1) \text{ in } t)\), that first evaluates \(f(m + 1)\) and then evaluates \(t\), then \(P(G, f)\) is not guaranteed to be \(m\). This is why we only realize squashed versions of the above mentioned continuity principles.

As Longley mentions, if \(F\) can catch the exception \(e\) then \(P(F, f)\) will not necessarily compute \(F\)’s modulus of continuity at \(f\). Therefore, we have extended Nuprl with exception handlers that can only catch exceptions with a specific name, and we have added the ability to generate fresh names (Sec. 7 discusses related nominal systems).

Related proofs of continuity. This is not the first (formal) proof that a type theory satisfies Brouwer’s continuity principle. Coquand and Jaber \([30, 31]\) proved the uniform continuity of a Martin-Löf-like intensional type theory using forcing \([8, 11, 24, 25, 63]\). Their method consists in adding a generic element \(g\) as a constant to the language that stands for a Cohen real of type \(2\rightarrow\) and defining the forcing conditions as approximations of \(g\), i.e., finite sub-graphs of \(g\). They then define a suitable computability predicate that expresses when a term is a computable term of some type up to approximations given by the forcing conditions. The key steps are to (1) first prove that \(g\) is computable and then (2) prove that well-typed terms are computable, from which they derive uniform continuity (the uniform modulus of continuity is given by the approximations). The uniform continuity principle is, where \(F\) is now a function on the Cantor space \(C = 2\rightarrow\) instead of the Baire space: \(\forall SCP\) \(\forall f, g \in C \Rightarrow \Pi SCP\). Escardó and Xu \([39]\) showed that in the case of uniform continuity \(\Sigma j\) can equivalently be \(\Sigma k\) or \(\downarrow \Sigma j\). In \([33]\), Coquand and Jaber provide a Haskell realizator that computes the uniform modulus of continuity of a functional on the Cantor space \([\Sigma j\].

Similarly, Escardó and Xu \([39]\) proved that the definable functions of Gödel’s system \(T\) are uniformly continuous on the Cantor space (without assuming classical logic or the Fan Theorem). For that, they developed a constructive continuous model, the \(C\)-Space category, of Gödel’s system \(T\), and proved that \(C\)-Space has a Fan functional that gives a function \(F\) in \(C \rightarrow \mathbb{N}\) can compute the modulus of uniform continuity of \(F\). Relating \(C\)-Space and the standard set-theoretical model of system \(T\), they show that all \(T\)-definable functions on the Cantor space are uniformly continuous. Finally, using this model, they show how to extract computational content from proofs in \(HA^\omega\) extended with a uniform continuity axiom \(\Pi SCP\), which is realized by the Fan functional.

In \([42]\) Escardó provides a simple and elegant proof that all \(T\)-definable functions are continuous on the Baire space and uniformly continuous on the Cantor space using a \textit{generic element} as in \([39]\) but without using forcing. His method consists in providing an alternative interpretation of system \(T\), where a number is interpreted by a dialogue tree that “describes the computation of a natural number relative to an unspecified oracle \(\alpha : \text{Eq}\rightarrow\)”. Such a computation is called a dialogue, which is a function that given a dialogue tree, returns a function of type \(\mathbb{B} \rightarrow \mathbb{N}\). Escardó first proves that dialogues are continuous. This means that a function is continuous if it is extensionally equal to a dialogue. The key steps are to (1) define a suitable logical relation between the standard interpretation and the alternative one that relates numbers and dialogues w.r.t. a given oracle; and (2) prove that all system \(T\) terms are related under the two interpretations. It then follows that for all system \(T\) term \(t\) of type \((\alpha \Rightarrow \alpha) \Rightarrow \alpha\) (where \(\alpha\) is the type of numbers), there is a dialogue tree \(d\) such that the standard interpretation of \(t\) and the dialogue on \(d\) are extensionally equal functions, from which he derives uniform continuity. The dialogue \(d\) is built using a \textit{generic} sequence that allows dialogue trees to call the oracle.

Results. Our proof method differs from the ones discussed above in the sense that it is “mostly” computational. In Sec. 3 we use diverging terms to prove \(\Pi SCP\), and in Sec. 4 we use computational effects (named exceptions) to probe terms and derive \(SCP\) using (non-strict) lock-step simulations of these effectful computations. Sec. 5 shows that \(SCP\) and \(SCP\) are equivalent. To prove \(SCP\), we added named exceptions as well as a \textit{fresh} operator to Nuprl’s computation system, and showed that these additions preserve Nuprl’s key meta-theoretical properties, such as consistency (see Sec. 8) and 4.3 and the congruence of Howe’s computational equivalence relation (see Sec. 2.2 and 4.2). As mentioned in Sec. 4.9 \(SCP\) justifies a corresponding inference rule that we added to Nuprl. Sec. 6 discusses the relation between \(SCP\) and \(SCP\) and the connection with the axiom of choice, as well as the status of the (squashed) axiom of choice in Nuprl. Using those continuity rules, as explained in Sec. 6 we have proved in Nuprl (1) a fully unsquashed version of \(UCP\) using Escardó and Xu’s method \([39]\); (2) that all real functions defined on the unit interval are uniformly continuous \([37, \text{pp}.87]\); and (3) that bar induction on monotone bars follows from bar induction on decidable bars following Kleene’s proof \([53, \text{pp}.69–73]\).

\(^4\) See also Escardó’s tutorial \(\text{http://www.cs.bham.ac.uk/~mhe/talks/popl2012/}\) for examples on how to search the Cantor space, as well as \([10]\), which point to citations and constructions by, among others, Gandy and Berger.
The results presented in this paper have either been formalized in Coq and are available both at https://github.com/vrahli/NuprlInCoq and http://www.nuprl.org/html/Nuprl2Coq/ or they have been formalized in Nuprl and are available at http://www.nuprl.org/LibrarySnapshots/Published/Version1/Standard/continuity/index.html for results related to continuity, at http://www.nuprl.org/LibrarySnapshots/Published/Version1/Standard/int-2/index.html for results related to the fan theorem, and at http://www.nuprl.org/LibrarySnapshots/Published/Version1/Standard2/reals/index.html for results related to real analysis.

2. Nuprl

Nuprl is an interactive theorem prover that implements a type theory called Constructive Type Theory (CTT) [8, 50]. Nuprl’s CTT “mostly” differs from other similar constructive type theories such as the ones implemented by Agda [4, 17], Coq [13, 33], or Idri [8, 51], in the sense that CTT is an extensional type theory (i.e., propositional and definitional equality are identified [49]) with types of partial functions [29, 34, 80]. This section presents some key aspects of Nuprl that will be used in the rest of this paper.

2.1 Nuprl’s Computation System

Fig. 1 presents a subset of Nuprl’s syntax and small-step operational semantics [4, 8]. Nuprl’s programming language is an untyped (à la Curry), lazy and applied (with pairs, injections, a fix-point operator, . . . ) λ-calculus. For efficiency, integers are primitive and Nuprl provides operations on integers such as addition, subtraction, . . . , a test for equality and a “less than” operator. Nuprl also has what we call canonical form tests [73] such as ifint, which are used to distinguish between our different kinds of values. These canonical form tests are especially useful when working with (non-disjoint) union types, which are sometimes easier to work with than disjoint unions because one does not need injections.

A term is either a variable, a value (or canonical term), or a non-canonical term. Non-canonical terms have one or two principal arguments (marked using boxes in Fig. 1). A principal argument of a term t is a term that has to be evaluated to a canonical form before checking whether t can be reduced further. For example, the application f(a) diverges if f diverges, and the canonical form test ifaxiom(t, a, b) diverges if t diverges.

Nuprl uses a uniform syntax for terms [7, 8], and the terms in Fig. 1 are “display forms” for some specific Nuprl terms. An advantage of having a uniform syntax is that operations that work uniformly on terms are easier to define—they do not have repetitive cases as when using one constructor per operator. In Nuprl a term is of the form θ(5), where θ is its operator, and 5 is a list of bound terms. A bound term b is of the form T .t, where T is a variable list. For example, the underlying representation of a λ-abstraction is [lambda](x .t). For convenience, we use the uniform syntax to, e.g., define Howe’s computational equivalence relation below.

Fig. 1 also shows part of Nuprl’s small-step operational semantics. We omit the rules that reduce principal arguments such as: if t1 → t2 then t1 u → t2 u. As usual, → is the reflexive and transitive closure of →, and t1 →k t2 is defined inductively on k: t → 0 t and t1 →k+1 t2 if there exists a t such that t1 → t and t →k t2.

We now define a few useful abstractions:

- \( \perp = \text{fix}(\lambda x.x) \)
- \( \text{N}_1 = \text{N} \cup \text{Unit} \)
- \( \text{tt} = \text{inl}(x) \)
- \( \text{isint}(t) = \text{ifint}(t, \text{tt}, \text{ff}) \)
- \( \text{ff} = \text{inr}(x) \)
- \( \text{isl}(t) = \text{if l then tt else ff} \)
- \( \text{if } t \text{ then } t_1 \text{ else } t_3 = \text{case } t_1 \text{ of } \text{inl}(x) \Rightarrow t_1 \mid \text{inr}(x) \Rightarrow t_3 \)

We sometimes write \( a \equiv b \) for the type \( a = b \in T \). Also, we sometimes write \( b \) for \( (b \text{ then Unit else Void}) \), where Unit and Void can, e.g., be defined as \( \equiv 0 \equiv 0 \) and \( 0 \equiv 1 \) respectively. We define True as Unit and False as Void.

2.2 Howe’s Computational Equivalence

It turns out that Nuprl’s type system is not only closed under computation but more generally under Howe’s computational equivalence \( \sim \), which he proved to be a congruence [50]. In Nuprl, in any context \( C \), when \( t \sim t’ \) we can rewrite \( t \) into \( t’ \) without having to prove anything about types. We rely on this relation to prove equalities between programs (bisimulations) without concern for typing [73]. Howe’s computational equivalence is defined on closed terms as follows: \( t \sim t’ \) if \( t \equiv t’ \). Howe conductively defines the approximation (or simulation) relation \( \leq \) as the largest relation \( R \) on closed terms such that \( R \subseteq \sim \), where \( \sim \) is the following closure operator (also defined on closed terms): \( (R) u \) if whenever \( t \) computes to a value \( \theta(u) \), then \( u \) also computes to a value \( \theta(v) \) such that \( \theta(R) \theta(u) \theta(v) \). To make that precise we have to extend \( R \) to open and bound terms: see [8, 51] for details. By definition, one can derive, e.g., that \( \perp \equiv t \) for all closed term \( t \).

2.3 Nuprl’s Type System

Following Allen’s PER semantics, Nuprl’s types are defined as partial equivalence relations (PERs) on closed terms [4, 5]. Allen’s PER semantics can be seen as an inductive-recursive definition of:

1. an inductive relation \( T_1 \equiv T_2 \) that expresses type equality; and
2. a recursive function \( a \equiv b \in T \) that expresses equality in a type.

We write type \( t \) for \( T \in T \), and \( t \in T \) for \( t \in T \). In other words, it follows that the (theoretical) proposition \( a \equiv b \in T \) is true (inhabited by *) if \( a \equiv b \in T \) holds in the meta-theory. See [4, 8] for more details.

Nuprl’s type system includes Martin-Löf dependent types, identity (or equality) types, a hierarchy of universes, \( W \) types, union and intersection types, quotient types [28], set types, and partial and base types [39]. The top part of Fig. 1 lists some of Nuprl’s types. Among these, Base is the type of all closed terms of the computation system with \( \sim \) as its equality. The type \( t_1 \equiv t_2 \) is true if the meta-theoretical statement \( t_1 \equiv t_2 \) is true, and \( t_1 \equiv t_2 \) and \( t_2 \equiv t_3 \) are equal types if \( t_1 \equiv t_2 \leftrightarrow t_3 \equiv t_4 \). Similarly the type \( t_1 \equiv t_2 \) is true if \( t_1 \equiv t_2 \) is true, and \( t_1 \equiv t_2 \) and \( t_1 \equiv t_2 \) are equal types if \( t_1 \equiv t_2 \leftrightarrow t_3 \equiv t_4 \) (see [73] and [74]). Appendix A&B for more details). For example, it is enough to prove that \( t_1 \) and \( t_2 \) are members of Base to prove that \( t_1 \equiv t_2 \) is a type. Also, it turns out that \( t \equiv t \) is a true type in any context. These types allow us, to some extent, to reason about Nuprl’s computation system directly in the theory. Nuprl has a rich type theory that makes type checking undecidable. In practice this is mitigated by type inference and type checking heuristics implemented as tactics.

We have implemented Nuprl’s type language, its computation system, Howe’s \( \sim \) relation, and Allen’s PER semantics in Coq [4, 8]. We have also showed that Nuprl is consistent by (1) proving that Nuprl’s inference rules are valid w.r.t. Allen’s PER semantics, and (2) proving that False is not inhabited. Using these two facts, we derive that there cannot be a proof derivation of False, i.e., Nuprl is consistent. (In addition to [4, 8], see also [73] Appendix A) for more details regarding Nuprl’s consistency.)

We are using our Coq formalization to prove all the inference rules of Nuprl, and have already verified a large number of them. This paper presents extensions we made to Nuprl in order to prove SCP. It includes adding some nominal features such as a fresh operator, named exceptions, and exception handlers. Using our Coq formalization, we provide in Sec. 3 a simple proof that \( WCP \) is true w.r.t. Nuprl’s PER semantics using the fact that \( \perp \) diverges, and in Sec. 4 we prove SCP using the nominal features mentioned above.

3. Weak Continuity Principle

Our proof of \( WCP \) uses \( \perp \) and the fact that it diverges. For further details regarding this proof conducted in our implementation of
Nuprl in Coq, the interested reader is invited to look at https://github.com/zhahNuprlInCoq/blob/master/continuity/continuity_roadmap.v. The same proof would not work for |, because using ↓ we can compute the modulus of continuity of a function in the meta-theory (this computation does not have to be expressible in the theory because only \* inherits ↓-squashed types), while using ↓ we would have to come up with a Nuprl term that does the computation (Sec.4 shows how to do that), i.e., such that f:wcp.

Let $F : Z^r \rightarrow Z$ and $f : Z^2$ (we use $Z$ here instead of $N$, but we proved a slightly more general result for functions of type $T^n \rightarrow Z$ where $T$ is a non-empty subtype of $Z$, such as $N$ or $\mathbb{N}$).

**Step 1.** By typing, this means that $F(f) \in Z$, i.e., $F(f)$ computes to an integer $i$.

**Step 2.** It might seem that in that computation $f$ only gets applied to integers, however, this is not necessarily true in an untyped language such as Nuprl. To remedy this issue, let $force(f) = \lambda x.let x := x + 0 in f x$. Because $f = force(f) \in Z^2$, by typing again we get $F(force(f)) \mapsto i$. Let us call that computation $C_1$. We use force to ensure that $f$’s arguments are integers. If $force(f)$ was to be applied to a term that is not an integer then the computation would either get stuck or diverge. We know that this cannot happen because $F(force(f)) \mapsto i$.

**Step 3.** Let bound$(t, b) = \lambda x.let x := t in if |x| < b then x else 1$. By computation we prove that there exists a number $b$ such that $F(\lambda x.let x := bound(x, b) in f x) \mapsto i$. We can get such a $b$ in the meta-theory by computing the largest number occurring in the computation $C_1$, i.e., if $t_1 = F(force(f)) \mapsto t_2 \mapsto \cdots \mapsto t = t_0$, then let $b$ be the largest number occurring in one of the $t_i$. We have to squash WCP’s existential quantifier using ↓ because this meta-theoretical computation of $b$ is not a Nuprl term. We prove this step using a simulation technique that we will reuse over and over again in this paper. We prove that given a context $G$, if $G[x+0] \mapsto v$ then $G[bound(x, b)]$ also computes to $v$, assuming that $b$ is greater than any other number occurring in the computation $G[x+0] \mapsto v$. Note that we have not yet used the fact that ↓ diverges. This will be used in step 5. Let us call $C_2$ the computation $F(\lambda x.let x := bound(x, b) in f x) \mapsto i$.

**Step 4.** We can now instantiate our conclusion using $b$. It remains to prove that $\Pi g : Z^2. f \equiv g \rightarrow F(f) =_Z F(g)$. Because $f$ and $g$ agree up to $b$, and because the computation $C_2$ converges, by computation we know that $F(\lambda x.let x := bound(x, b) in g x) \mapsto i$. We prove this by showing that given a context $G$, if $G[let x := bound(x, b) in f x]$ computes to a value, then $G[let x := bound(x, b) in g x]$ computes to the same value. We still have not used the fact that ↓ diverges, because we could use any number in bound’s definition instead of ↓, such as 0, and make sure that $0 < b$.

**Step 5.** Again by computation: $F(force(g)) \mapsto i$. We prove this by showing that given a context $G$, if $G[bound(x, b)]$ computes to a value then $G[x+0] \mapsto v$ computes to the same value because the “less than” operator in bound’s definition ensures that $x$ is an integer, and because we know that $G[bound(x, b)]$ does not diverge.

**Step 6.** Finally, by typing, $F(g) \mapsto i$, i.e., $F(f) =_Z F(g)$.

## 4. Strong Continuity Principle

We now prove SCP\_1 [53, pp.69–73] (Sec.5 shows that SCP\_1 and SCP\_2 are equivalent). We need to come up with a Nuprl term of type $\Pi n : N. N^{n^n} \rightarrow N + \mathbb{N}$ that checks whether we have reached the modulus of continuity of a function. For that, we now use exceptions as a probing mechanism to compute the modulus of continuity of a function. Instead of SCP\_1, we prove the following equivalent but slightly simpler statement [53, pp.71–72] (where the $T$ in SCP\_3 is for Test—see below):

$$SCP(F) = \Sigma :\langle \Pi n : N. N^{n^n} \rightarrow N + N \rangle$$

$$\Pi f : N \\downarrow \Pi n : N.$$ \hspace{1pt}

$$\text{isint}(M n f) \rightarrow M n f =_N F(f)$$

$$\text{SCPT} = \Pi F : B \rightarrow N. \text{SCP(F)}$$

Using our Coq formalization and making use of computations on terms that are only possible in the meta-theory, we proved that SCPT is true w.r.t. the PER semantics of Nuprl extended with the nominal features mentioned above. We then proved directly in Nuprl that SCPT and SCP\_3 are equivalent. We prove SCPT rather than SCP\_3 mainly because its realizer is simpler. Intuitively, the $M$ part of SCPT’s realizer is a simple test function (top), while the one for SCP\_3 is a recursive search function of the form (bottom)\footnote{In both functions, None means that $n$ is less than the modulus of continuity of $F$ at $f$. In the test function, Some means that $v = F(f)$ and $n$ is greater than or equal to the modulus of continuity of $F$ at $f$, while the search function returns $F(f)$ only when $n$ is the modulus of continuity of $F$ at $f$ (and not when $n$ is past the modulus as in the test function).}.

```coq
fun test n f =
  let exception e in
  (let v = F (fun x => if x < n then f x else raise e)
in some v) handle e => None
```
let fun search n m f =
    if m <= 0 then test n f
    else case test m f of
        | Some k => None
        | None => search (n - 1) f
end

in search n (n - 1) f

4.1 Extension of Nuprl’s Computable System

4.1.1 Syntax

We extend Nuprl with names (or unguessable atoms [14]), named exceptions, exception handlers, and a fresh operator as follows:

\[
v ::= \cdots | a \quad \text{(name value)} \\
v \vdash ::= \cdots \\
| \text{Name} \quad \text{(name type)} \\
| \text{Exc}(t_1, t_2) \quad \text{(exception type)} \\
e ::= \text{exc}(t_1, t_2) \quad \text{(exception)} \\
t ::= \cdots \\
| e \quad \text{(exception)} \\
| \text{if} \{t_1\} = \{t_2\} \text{ then } t_3 \text{ else } t_4 \quad \text{(name equality)} \\
| \nu t \quad \text{(fresh)} \quad \text{(try/catch)} \\
| \text{try}_n t \text{ with } x.c \quad \text{(try/catch)}
\]

Name is a type of names (constants) and a stands for a name. Names were introduced in Nuprl to reason about logical foundations for security [14]. To account for names, Allen generalized his PER semantics [8] to a so-called supervaluation semantics that quantifies over all possible implementations of the name type [3]. Names come with two meta-theoretical operations: a fresh operator to generate a fresh name w.r.t. a list of names, and a test for equality. As in Pitts and Stark’s \(\nu\)-calculus [68] or Odersky’s \(\lambda\nu\)-calculus [63], we add two corresponding operators to Nuprl.

Our exceptions and handlers are similar to Lebresne’s [57]. In Nuprl, an exception \(e\) has two subterms: the first one is \(e\)’s name and the second one is some piece of data that can be used if \(e\) is caught. The type \(\text{Exc}(t_1, t_2)\) is the type of exceptions with names of type \(t_1\) and data of type \(t_2\). In general exceptions can be named with terms other than names. For example, if \(a\) and \(b\) are names, both \(\text{exc}(a, 0)\) and \(\text{exc}(b, 0)\) have type \(\text{Exc}(\text{Name}, \mathbb{Z})\) (among others); and \(\text{exc}(1, 0)\) has type \(\text{Exc}(\mathbb{Z}, \mathbb{Z})\). We also add exception handlers of the form \(\text{try}_n t\) with \(x.c\), where \(t\) is the term we try to evaluate, and \(c[x\downarrow d]\) is the code we run if we catch an exception with name \(n\) and data \(d\). Therefore, a handler cannot catch all exceptions. A canonical operator is now either a value or an exception.

Let us define a few useful abstractions/abbreviations:

\[
\begin{align*}
\text{Name}_n &= \{ x : \text{Name} \mid x \simeq n \} \\
\text{Exc}_n(T) &= \text{Exc}(\text{Name}_n, T) \\
\text{Exc}_n &= \text{Exc}_n(\text{Unit}) \\
T_{\nu} &= T \cup \text{Exc}_n \\
\text{try}_n t &= \text{try}_n t \text{ with } x.x \\
\end{align*}
\]

If \(T\) is not an exception type, \(T_{\nu}\) is the type of terms that either compute to elements of type \(T\) or that compute to exceptions with name \(n\) and data \(d\).

The type \(T_{\nu}\) is similar to Lebresne’s type \(A_{\nu}\{\epsilon\}\), where \(A\) is a type and \(\epsilon\) is an exception [56,57]. In addition Lebresne also introduces corruption types of the form \(A^{(*)}\). A term in \(A^{(*)}\) is a term in \(A\) where some part has been replaced by the exception \(\epsilon\). As he mentions, an expression of that type does not necessarily evaluate to an exception. For example, if Nuprl had such a type, \(\text{inl}(\text{exc}_{\alpha})\) could be of type \((\mathbb{N}+\text{Unit})^{(*)}\). We leave adding corruption types to Nuprl for future work (Sacchini [78] shows that corruption in the presence of dependent types has interesting consequences).

Exceptions are a standard programming language feature. In the interactive theorem proving realm they are “well-adapted to programming strategies which may be (in fact usually are) inapplicable to certain goals” [43, pp.11]. However, exceptions are often not accounted for in types. As mentioned above, Lebresne’s Fx system [55] provides type constructors to express two different levels of corruption. Lebresne [56] mentions that to get exceptions one could either directly encode them in the language (e.g., using monads) or add them as primitive. We decided to add them as primitives for the same reasons (e.g., compositionality) stated in his paper. David and Mounier [60] introduced E2x as an extension of Krivine’s FA2 system [55] with exceptions. As in Nuprl, both Fx and in E2x implement call-by-name exceptions. Also, in all three systems exceptions and handlers are named, and handlers can only catch exceptions with the correct name.

4.1.2 Operational Semantics of \(\nu\)

Let us now precisely define how fresh and handlers compute. A fresh expression of the form \(\nu x.t\) computes differently depending on whether \(t\) is a variable, a canonical term, or a non-canonical term. Let us consider each of these cases.

Variable. If \(t\) is the variable \(x\) then \(\nu x.t\) reduces to itself and therefore diverges. Therefore, one can prove that \(\nu x.x \sim \bot\). This differs both from Odersky’s [63] approach where \(\nu x.x\) is stuck and from Pitts’ approach [66] where \(\nu x.x\) is a normal form. If \(t\) reduces to another variable than \(x\) then the computation gets stuck because the term is open.

Non-canonical. If \(t\) is non-canonical then

\[
\nu x.t \rightarrow \nu x.u[a\downarrow x] \quad \text{if } t[x\downarrow a] \rightarrow u
\]

where \(a\) is a fresh name w.r.t. \(t\) (written \(a\#t\)), and \(t[x\downarrow u]\) is a capture avoiding substitution function on names (similar to the usual substitution operation on variables). This ensures that fresh names do not escape the scope of \(\nu\) expressions. As expected (if \(x \neq y\)):

\[
\nu x.\nu y.\text{if } x=y \text{ then } tt \text{ else } ff \rightarrow^* ff
\]

We cannot simply reduce \(\nu\) as follows: \(\nu x.t \rightarrow t[x\downarrow a]\), because Howe’s computational equivalence would not be a congruence. For example, \(\nu x.\text{inl}(x) \rightarrow \text{inl}(a)\) and \(\text{let } y := a \text{ in } x\) \(\sim x\) but \(\nu x.\text{inl}(\text{let } y := a \text{ in } x) \neq \nu x.\text{inl}(a)\).

Canonical. If \(t\) is a canonical form (a value or an exception), then we “push” \(\nu\) “down” the expression as in Odersky’s \(\nu\)-calculus [60,63] (as opposed to using, e.g., stateful dynamic allocation [60] or the notion of prevalues [52], which are values prefixed with a list of “fresh name” binders):

\[
\nu x.t \rightarrow \nu x.t
\]

where \(\nu\) computes as follows on terms:

\[
\nu x.a_1 \cdots \nu x.a_n \theta(b_1 ; \cdots ; b_n) = \theta(\nu x.b_1 ; \cdots ; \nu x.b_1)
\]

and as follows on bound terms:

\[
\nu x.\text{let } t = \ell.t \quad \rightarrow \nu x.\ell.t
\]

where, in order to avoid variable capture, \(x’\) is \(x\) if \(x \notin \ell\), and a fresh variable w.r.t. \(t\) otherwise. For example \(\nu x.\{x\} \rightarrow (\nu x.1, \nu x.x)\) and \(\nu x.\lambda y.t \rightarrow \lambda y.\nu x.t\) if \(x \neq y\). Note that when \(x \in \ell\), we could have defined \(\nu x.\text{let } t = \ell.t\) to be \(\ell.t\). However, this would make the definition less uniform and therefore harder to reason about. To this effect, we proved \(\nu x.t \sim t\) if \(t\) is closed.

4.1.3 Operational Semantics of \text{try}

Handlers of the form \(\text{try}_n e\) with \(x.c\) catch exceptions of the form \(e\) \(\sim_n d\). For example,

\[
\text{try}_n (1 + \text{exc}(\lambda x.x + 1)) \text{ with } f.f(2) \rightarrow^* 3
\]
When its principal argument is non-canonical or a variable, a handler computes exactly like the other non-canonical operators (except $\nu$). Let us consider the exception and value cases.

**Exception.** If $t$ is an exception of the form $\text{exc}(n,d)$ then we have to check whether the handler has the right name as follows:

$$\text{try}_{m_0} \text{exc}(n,d) \text{ with } x.c \\
\implies \text{if } m = n \text{ then } c[x \mapsto d] \text{ else } \text{exc}(n,d)$$

This computational rule also has the following effect that if $m$ computes to an exception $e$, then $\text{try}_{m_0} \text{exc}(n,d) \text{ with } x.c \mapsto e$. Also, if $m$ is a name and $n$ computes to an exception $e$ then $\text{try}_{m_0} \text{exc}(n,d) \text{ with } x.c \mapsto e$.

**Value.** A naive way or reducing a handler when its principal argument is a value would be to simply return the value as follows:

$$\text{try}_{n_0} v \text{ with } x.c \mapsto v$$

However, note that in the case where the principal argument of a handler is an exception, we have to evaluate the “name” part of the handler to check whether the exception has the correct name. This means that if we were to simply return the value here and if the “name” part was $\top$ for example, raising an exception in an expression that is “well-behaved” could cause the expression to diverge. For example, using the above rule: $\text{try}_{1} 1 \mapsto 1$, and if we replace 1 by $\text{exc}_a$, then $\text{try}_{1} \text{exc}_a$ diverges. This is undesirable, especially in the context of using exceptions to probe a function, e.g., to compute its modulus of continuity. Therefore, instead of simply returning the value, we first check that $n$ is something that we can compare:

$$\text{try}_{n_0} v \text{ with } x.c \mapsto \text{if } n = n \text{ then } v \text{ else } \bot$$

### 4.2 Howe’s Computational Equivalence in the Presence of $\nu$

To prove that $\sim$ is a congruence, Howe first proves that $\equiv$ is a congruence [50]. Unfortunately, this is not easy to prove directly. Howe’s “trick” was to define another relation $\equiv^*$, which is a congruence and contains $\equiv$ by definition.

Howe’s definition of $\equiv^*$ does not use types, but to account for the fact that the binders of $\nu$ expressions are only meant to be names (as opposed to the binders of, e.g., $\lambda$-abstractions, which can be substituted by any term when applied), rather than turn Nuprl into a typed language, we added “simple” type information to the definition of $\equiv^*$. We define a function $\text{BT}$ that, for a given operator, returns the types of the binders of its bound terms. The type of a binder can either be $\text{NAME}$ or $\text{ANY}$. $\text{BT}(\nu) = [\text{NAME}]$ because $\nu$ has one subterm (the outer brackets) that has one binder (the inner brackets). The type of all the other binders is $\text{ANY}$. For example, $\text{BT}(\lambda) = [\text{ANY}]$ because a $\lambda$-abstraction has one subterm which has one binder. When extending the definition of $\equiv^*$ from terms to bound terms, BT is used to restrict what terms can be substituted for free variables. This modification of $\equiv^*$’s definition was inspired by Gordon’s [43] and Jeffrey and Rathke’s [53] adaptations of Howe’s method to typed $\lambda$-calculi. It is interesting to note that until we added the $\nu$ operator to Nuprl, there was no need to use type information in the proof that $\sim$ is a congruence.

Howe defines $t \equiv^* u$ by induction on $t$: if $t$ is a variable then $t \equiv^* u$ if $t \equiv u$; and if $t$ is of the form $\tau(b)$ then $t \equiv^* u$ if there exists $\overline{b}$ such that $\overline{b} \equiv^* b$ and $\tau(\overline{b}) \equiv u$. To prove that $\equiv^*$ and $\equiv$ are equivalent and therefore that $\equiv$ and $\sim$ are congruences, it suffices to prove that $\equiv^*$ respects computation, i.e., given that $t \equiv^* u$, if $t$ computes to a value of the form $\theta(\overline{b})$ then $u$ also computes to a value $\theta(\overline{b})$ such that $\overline{b} \equiv^* b$. Howe’s Lemma 2 in [50] shows that this is true when $t$ is a value.

Howe then defines a condition called *extensionality* that non-canonical operators of lazy computation systems have to satisfy for $\equiv^*$ to imply $\equiv$, and therefore for $\equiv$ and $\sim$ to be congruences.

First, we extended all these definitions to deal with the fact that canonical forms can either be values or exceptions. Then, using our new definition of $\equiv^*$ we were able to prove that $\nu$ is extensional (see [22] Appendix D for more details).

### 4.3 Consistency

As mentioned above, Nuprl’s consistency follows from the fact that all its inference rules are valid w.r.t. Allen’s PER semantics and from the fact that False is not inhabited. In addition to extending Nuprl’s computation system, and fixing its properties including Howe’s computational equivalence relation, we had to re-run all the proofs that Nuprl’s inference rules are valid. Most of these rules and proofs did not have to change. The only one that had to change is discussed in details in [22] Appendix C (see [22] Appendices A&B) for details regarding the validity of rules). Let us summarize this discussion here.

First, note that because exceptions are canonical forms as mentioned in Sec. 4.1 above, if $a \mapsto \text{exc}(t_1,t_2)$ then $a \equiv b$ if there exists $u_1$ and $u_2$ such that $b \mapsto \text{exc}(u_1,u_2)$, $t_1 \equiv u_1$, and $t_2 \equiv u_2$. Therefore, even though we cannot have a canonical form test (such as ifint or ifixor) for exceptions that would check whether a term computes to an exception because we cannot catch an exception without having its name (i.e., we have no way of catching all exceptions), we can define a proposition $\text{isexc}(t)$ that asserts that a term $t$ computes to an exception as follows: $\text{isexc}(t) = \text{exc}_{\bot} t$, where $\text{exc}_{\bot} = \text{exc}(\bot,\bot)$. Similarly, the following proposition $\text{halt}(t)$ asserts that $t$ computes to a value: $\text{halt}(t) = * \equiv \text{let } x := t \text{ in } x$. By definition of Howe’s approximation relation, before adding exceptions, when proving a proposition of the form $t_1 \equiv t_2$ we could assume $\text{halt}(t_1)$. This was captured by our old [convergence] inference rule described in [22] Appendix C. This is no longer true because we also have to consider the case where $t_2$ is an exception. To that effect our new [convergence] inference rule generates (among others) two subgoals: one that assumes $\text{halt}(t_1)$ and one that assumes $\text{isexc}(t_1)$. Alternatively, we could capture that a term $t$ computes to either a value or an exception using the type: $\text{exc}_{\bot} (\text{let } x := t \text{ in } x)$. We have not yet investigated the usefulness of such a type.

### 4.4 Computing the Modulus of Continuity

We now have the tools in hand to compute the modulus of continuity of a functional using exceptions as described above:

$$\text{force}(k,t) = \text{if } k < 0 \text{ then } \bot \text{ else } t$$

$$\text{bound}(n,f,e,k) = \text{force}(k, \text{if } k < n \text{ then } f[k], \text{else exc}_{e})$$

$$\text{test}(F,n,f) = \nu x.\text{try}_{F}(\text{bound}(n,f,x))$$

$$M(F) = \lambda n.\text{test}(F,n,f)$$

i.e., unfolding the definitions, $M(F)$ is

$$\lambda n.\text{try}_{F}(\nu x.\text{force}(x,f(x)))$$

Also, let $\text{force}(f) = \lambda x.\text{force}(x,f(x))$. As in our proof of WCP, we will partly use typing, partly use computation to prove that $M(F)$ is indeed our witness for SCPT. This is why bound starts off by checking whether its argument $x$ is an integer less than 0. If a computation that uses bound converges and along the way applies $f$ to some term $k$, we will be guaranteed that $k$ is a natural number.

### 4.5 Well-Typedness

To prove SCPT, we first prove that $M(F)$ has type $\Pi n: \mathbb{N}.\mathbb{N}^n \rightarrow \mathbb{N}$. As mentioned above, this term does not respect computation, it is not functional over $F \in \mathcal{B} \rightarrow \mathbb{N}$. However, given a
As we show below in Sec. 4.6, to prove that it is enough to prove

We have to prove

Let us prove that

\[ C \text{ is such that } a \# F, a \# \#. \]

Again, it is enough to prove

\[ F(\text{bound}(k, f, a)) \equiv F(\text{bound}(k, g, a)) \in \mathbb{N}_a \]

By typing again, from \( \# \equiv g \in \mathbb{N}_a \), we deduce that

\[ \# \equiv g \in \mathbb{N}_a \]

A general fact about exceptions is: if \( F : F \rightarrow N \) and \( a \# F \) then

\[ \text{Force}(F) \in (\mathbb{N}_a)^N 
\]

where \( \text{Force}(F) = \lambda x. F(\text{force}(f)) \). Is Force necessary? Can’t we simply prove \( F \in (\mathbb{N}_a)^N \)?

To prove that we use the same technique as in WCP’s proof. Given

it is trivial to deduce that the equality \( \equiv \) is true using equality \( \equiv \).

Let us now prove 3. We have to prove that for all \( F \in \mathcal{B} \rightarrow N \), and \( f \) such that \( \# \equiv g \in (\mathbb{N}_a)^N \),

\[ \text{Force}(f) \equiv \text{Force}(\# \equiv g) \in \mathbb{N}_a \]

First, we define a function \( \text{force} \) so that the function \( f' = \lambda x. \text{force}(f(x), f) \) computes as the function \( f_0 = \text{force}(f) \), except that on natural numbers, when \( f_0 \) returns \( \text{exc} \), \( f' \) returns 0 (this 0 could be any natural number):

\[ \text{force}(f)(x, f) = \text{case } x < 0 \text{ then } 0 \text{ else } \text{force}(f)(x) \text{ with } z = 0 \]

Let \( g_0 = \text{force}(g) \). Note that \( f_0 \equiv g_0 \in \mathbb{N}_a \). Because \( f' \) is in \( \mathcal{B} \), we get that \( \text{force}(F) \) computes to a natural number.

Let us now use again the same simulation technique as before. Let us prove that in any context \( C \) with no occurrence of \( a \), if \( C[f] \) computes to a natural number \( j \), then either both \( C[f_0] \) and \( C[g_0] \) also compute to \( j \) or both \( C[f_0] \) and \( C[g_0] \) compute to \( \text{exc} \). We prove that by induction on the length of the reduction \( C[f] \rightarrow \_ \). For that we prove that if \( C[f] \rightarrow u \) and \( u \) computes to a canonical expression, then there exists a context \( C' \) such that \( u \rightarrow C'[f] \) and either both \( C[f_0] \rightarrow C'[f_0] \) and \( C[g_0] \rightarrow C'[g_0] \) or both \( C[f_0] \rightarrow C'[g_0] \) and \( C[g_0] \rightarrow C'[f_0] \). This gives us that \( F(f_0) \equiv F(g_0) \in \mathbb{N}_a \).

4.6 Interlude: Reasoning about \( \nu \)

In Sec. 3.1.2 we saw how \( \nu \) computes. We show here how to reason about \( \nu \). One can prove that \( \nu (x, f, t) \equiv \nu (x, f, t) \in T \) by proving that \( t_1[x] \equiv t_2[x] \in T \), assuming \( a \# 1 \) and \( a \# t_2 \), and that \( T \) is flat, meaning that its inhabitants compute to terms that have no subterms and that are not names, such as integers or \( \ast \). This follows from the way \( \nu \) computes. If \( t[x] \rightarrow u \) such that \( a \# 1 \) and \( u \rightarrow v \rightarrow v \rightarrow a \), then \( t[x] \rightarrow v \rightarrow v \rightarrow a \equiv x \). By the method of proof above, we would get \( \nu (x, f, t) \equiv \nu (x, f, t) \). This proves \( \nu (x, f, t) \equiv \nu (x, f, t) \).
computes to an exception $e$ with some other name than $a$ and then $\text{try}_a F'(\text{bound}(n, f, a)) \rightarrow^* e$ and $e \neq k$. In both cases we get a contradiction.

(2) We now assume that $F'(\text{bound}(n, f, a))$ computes to a value $k$. If so, it has to compute to $k$. We now prove that $k \neq k'$. As before, because $F(f) = F(\text{force}(f)) \in \mathbb{N}$, we get that $F(\text{force}(f)) \rightarrow^* k'$. The rest of this proof closely follows the one in Sec. [4.7] We prove that in any context $C$ with no occurrence of $a$, if $C[\text{force}(f)]$ computes to the natural number $k'$ then $C[\text{bound}(n, f, a)]$ computes to either $k'$ or $\text{exc}_a$. We prove that by induction on the length of the reduction $C[\text{force}(f)] \rightarrow^* k'$. For that we prove that if $C[\text{force}(f)] \rightarrow u$ such that $u$ computes to a canonical form then there exists a context $C'$ such that $u \rightarrow C'[\text{force}(f)]$ and $C'[\text{bound}(b, f, a)] \rightarrow C'[\text{bound}(b, f, a)] \rightarrow \text{exc}_a$. We get that either: (1) $F'(\text{bound}(n, f, a)) \rightarrow k'$ and therefore $k = k'$; or (2) $F'(\text{bound}(n, f, a)) \rightarrow \text{exc}_a$ and we get a contradiction because $k \neq k'$.

### 4.9 Nuprl’s Strong Continuity Inference Rule

Using the fact that SCP (defined at the beginning of Sec. 4) is true in Nuprl’s meta-theory, we proved that the following inference rule, called [[strong-continuity]2-no-inner-squash], is true w.r.t. Allen’s PER semantics (for further details regarding this proof conducted in our implementation of Nuprl in Coq, the interested reader is invited to look at [https://github.com/vrahli/Nuprl1InCoq/blob/master cont/continuity/continuity_roadmap.v]:

$$
\begin{align*}
H \vdash F & : (\mathbb{N} \rightarrow T) \rightarrow \mathbb{N} \\
H \vdash \downarrow T & \\
H \vdash T & \subseteq \mathbb{N}
\end{align*}
$$

Using this inference rule, we prove that SCP is the following version of Nuprl in Coq, where the first (outer) existential quantifier is \text{-}squashed and the second (inner) one is not squashed (this lemma can be accessed by clicking the following hyperlink: [strong-continuity2-no-inner-squash]).

We get rid of the second squash operator using the usual unbounded search \text{μ} operator. As expected the extract of that lemma is (we use colored parentheses for visual convenience):

$$
\lambda F'. (M'(F'), \lambda f. (\mu (\lambda n. \text{inl}(\text{test'}(F, n, f)))), (\ast, \lambda m. \lambda i. *))\]$$

where

$$
\begin{align*}
\text{test'}(F, n, f) & := \text{let } x := \text{test}(F, n, f) \text{ in } \\
& \quad \text{if} \{ x = \text{inl}(x), \text{inr}(*) \}
\end{align*}
$$

$$
M'(F) = \lambda n. M. \lambda f. \text{test'}(F, n, f)
$$

$$
\mu(f) = \text{fix} \left( \lambda F'. M'. \lambda n. \mu \text{if} (f(n) \text{ then } n \\text{ else let } m := n + 1 \text{ in } F(m)) \right)
$$

We then derived a version of SCP where, as mentioned in the introduction, the first (outer) $\Sigma$ is $\downarrow$ and the second (inner) one is $\Sigma$ (see/click Nuprl lemma [strong-continuity2-no-inner-squash-unique]. Therefore, because these versions of SCP are equivalent of SCP, we also refer to them as SCP.}

### 5. Relations Between WCP and SCP

As mentioned in Sec. [19] Bridges and Richman [19] state that SCP is equivalent to WCP plus some form of the axiom of choice—some version of A\text{C}_1,0. As we saw above the existential quantifiers in these statements have to be truncated using $\downarrow$ (see Escardó and Xu [29]). Therefore, for that equivalence to be true, we probably need the $\downarrow$-truncated version of A\text{C}_1,0, which is true in

6 Alternatively, the reader can search for the lemma with that name available here: [http://www.nuprl.org/LibrarySnapshots/Published/Versions/1/index.html](http://www.nuprl.org/LibrarySnapshots/Published/Versions/1/index.html); and similarly for the other Nuprl lemmas mentioned below and highlighted in green (or gray).

Nuprl as discussed below in Sec. [5.3] Therefore, we only need to prove that SCP; and WCP are equivalent. We prove below that WCP is a trivial consequence of SCP, and that SCP is a consequence of WCP using the same “trick” as the one used by Bridges and Richman to prove that WCP follows from the Fan Theorem and WCP [19, pp.113] (see Sec. [6.1] below on uniform continuity).

### 5.1 SCP Implies WCP

Let us sketch the proof that SCP $\rightarrow$ WCP. For convenience, we will write $\mathbb{N}_0$ for $\mathbb{N} \uparrow \mathbb{N}$. Let $F : B \rightarrow \mathbb{N}$ and $f \in B$. We prove the formula $C : \mathbb{N}_0 : \mathbb{N}. \Pi g : B. f \equiv g. F(f) = F(g)$.

From SCP, we get a $M : \Pi m : \mathbb{N}_{n, n}. \mathbb{N}$. We can un squash SCP’s outer $\Sigma$ because our conclusion $C$ is squashed and a function

$$
A \in \Pi f : B. \Sigma: \mathbb{N}. M m f = \mathbb{N}_0 \text{inl}(F(f)) \land \Pi m : \mathbb{N}_0. \text{inl}(M m f) = \mathbb{N}_0 n
$$

By applying $A$ to $f$ we get a $n : \mathbb{N}$ such that:

- $M n f = \mathbb{N}_0 \text{inl}(F(f))$.
- $B \in \Pi m : \mathbb{N}_0. \text{inl}(M m f) = \mathbb{N}_0 n$.

We un squash and instantiate with $n$ our conclusion $C$, and we now get to assume that there is a $g : B$ such that $f \equiv g, g$. It remains to prove that $F(f) = \mathbb{N}_0 F(g)$. By applying $A$ to $g$ we get a $n' : \mathbb{N}$ such that:

- $M n' g = \mathbb{N}_0 \text{inl}(F(g))$.
- $B' \in \Pi m : \mathbb{N}_0. \text{inl}(M m g) = \mathbb{N}_0 n'$.

Because $f \equiv g, g$, we get that $M n f = \mathbb{N}_0 M n g$. Because $M n f = \mathbb{N}_0 \text{inl}(F(f))$, we get $\text{inl}(M n f)$ and therefore also $\text{inl}(M g)$. Then, by applying $B'$ to $n$ we get $n = n'$. Therefore, $\text{inl}(F(f)) = \mathbb{N}_0 \text{inl}(F(g))$, and finally we get that $F(f) = \mathbb{N}_0 F(g)$.

### 5.2 WCP Implies SCP

In this section we prove that W\text{\&}CP implies SCP (see Nuprl [[weak-continuity-implies-strong]], where W\text{\&}CP is the following “skolemized” version of WCP:

$$
\text{SCP} = \Pi F. B \rightarrow \mathbb{N}. \\
| \Sigma M : B \rightarrow \mathbb{N}. \\
\Pi f : B. \Sigma n : M. N m n f = \mathbb{N}_0 \text{inl}(F(f)) \land \Pi n : \mathbb{N}_0. \text{inl}(M m f) = \mathbb{N}_0 \text{inl}(F(f))
$$

It is easy to prove that W\text{\&}CP and SCP are equivalent using our proof that the $\downarrow$-truncated version of choice A\text{C}_1,0 discussed below in Sec. [5.3] is true (see Nuprl lemma [axiom-choice-\text{X-quot}]). Let us assume W\text{\&}CP and let $F : B \rightarrow \mathbb{N}$. We have to prove the following formula C:

$$
| \Sigma M : \Pi n : \mathbb{N}. N m n f = \mathbb{N}_0 \text{inl}(F(f)) \land \Pi n : \mathbb{N}_0. \text{inl}(M m f) = \mathbb{N}_0 \text{inl}(F(f))
$$

Instantiating W\text{\&}CP with $F$ we get (because our conclusion $C$ is $\downarrow$-truncated, we can un squash our hypothesis):

- a $M : B \rightarrow \mathbb{N} (F \uparrow \text{modulus of continuity})$
- a $G \in \Pi f : B. f = \mathbb{N}_0 \text{inl}(F(f)) \rightarrow (F(f) = \mathbb{N}_0 F(g))$

Bridges and Richman’s trick is to also use the modulus of continuity of $M$. Therefore, instantiating W\text{\&}CP with $M$ we get:

- a $X : B \rightarrow \mathbb{N} (M \uparrow \text{modulus of continuity})$
- a $K \in \Pi f : B. f = \mathbb{N}_0 \text{inl}(F(f)) \rightarrow (M(f) = \mathbb{N}_0 M(g))$

Let us now un squash our conclusion $C$ and instantiate it with $B = \lambda n. \lambda a. \text{if } M(a, n) \leq n \text{ then } \text{inl}(F(a, n)) \text{ else } \text{inr}(*)$
where $a_{n,k} = \lambda x. \text{if } x < n \text{ then } a(x) \text{ else } k$ (this is the infinite sequence consisting of the first $n$ values of a followed by $k$’s, $a_{n,0}$ is sometimes denoted $\pi_n$; e.g., in \cite{13, 38}). If $a \in \mathbb{N}^n$ and $k \in \mathbb{N}$ then $a_{n,k} \in \mathbb{N} \rightarrow \mathbb{N}$. We now have to prove that assuming that $f \in B$ then:

$$\Sigma n : \mathbb{N}. B n \ f =_{\mathbb{N}} \text{inl}(F(f))$$

(4) \hspace{1cm} $\Pi n : \mathbb{N}. \text{inl}(B n \ f) \rightarrow (B n \ f =_{\mathbb{N}} \text{inl}(F(f)))$

(5) Equalities \(5\) follows from \(G\). We now prove \(4\) by instantiating it with $m = \max(M(f), X(f))$. We have to prove $B m \ f =_{\mathbb{N}} \text{inl}(F(f))$, i.e.,

$$\text{if } M(a_{n,0}) \leq m \text{ then } \text{inl}(F(a_{m,0})) \text{ else } \text{inr}(\star)$$

(6) \hspace{1cm} $=_{\mathbb{N}} \text{inl}(F(f))$

Because $f =_{\mathbb{N}} M(f) =_{\mathbb{N}} a_{m,0}$, then using $G$ we obtain: $F(f) =_{\mathbb{N}} F(a_{m,0})$. Therefore, to prove equality \(5\) it remains to prove that its conditional is true, i.e., $M(a_{n,0}) \leq m = \max(M(f), X(f))$. If we instantiate $K$ with $f$ and $a_{m,0}$, we have to prove $f =_{\mathbb{N}} X(f)$, which is true by definition of $m$, and get to assume $M(f) =_{\mathbb{N}} M(a_{m,0})$ which gives us that $M(a_{m,0}) \leq m$.

5.3 Axiom of Choice

The following axiom of choice is usually trivial in constructive type theories such as Nuprl when $\Sigma$ is $\Sigma$ (where $A$ and $B$ are types):$AC = \Pi n : A. \Sigma b : B. P \ a \ b \Rightarrow \Sigma f : B^A. \Pi a : A. P \ a (f(a))$

It follows from the usual rules of the universal and existential quantifiers. We can prove that these rules are true in our predicative Coq model \cite{18} without assuming any axiom. In that predicative model we can model n Nuprl universes using $n + 1$ Coq universes. However, in our impredicative model we have to assume some axiom of choice, namely FunctionalChoice on (see http://coq.inria.fr/ctocorico/CoqAndAxioms), to prove some of these rules.

However, the non-squashed version of $AC$ is not always enough because as we saw above existential quantifiers cannot always be interpreted as $\Sigma$ but sometimes as truncated $\Sigma$’s. Therefore, we sometimes need instances of $AC$ where $\Sigma$ is either $\Sigma$ or $\mathbb{1} \Sigma$. In that case it is not obvious anymore which instances of $AC$ are consistent or provable in Nuprl.

Some versions of $AC$ for particular choices of types $A$ and $B$ are of particular interest. One can often find in the literature the name $AC_{n,m}$, where $n, m \in \{0, 1\}$ \cite{22, 23}; $n = 0$ means that $A = \mathbb{N}$ and $n = 1$ means that $A = B$; similarly $m = 0$ means that $B = \mathbb{N}$ and $m = 1$ means that $B = \mathbb{1}$.

Using a technique similar to the one discussed in \cite{71}, we proved the $\Sigma$-squared version of $AC_{0,0}$, where $\Sigma$ is $\mathbb{1} \Sigma$, once again conducting the proof first in the meta-theory, and then reflecting the meta-theoretical result in the Nuprl theory as an inference rule: see lemma rule\_AC0\_true in \cite{https://github.com/vrahli/NuprlInCoq/blob/master/axiom_choice/axiom_choice.v}. We also proved directly in Nuprl the $\Sigma$-squared versions of $AC$, where $\Sigma$ is $\Sigma$ namely $AC_{0,0}$ (see Nuprl lemma \texttt{axiom-choice-0\_0-quot}) and $AC_{1,0}$ (see Nuprl lemma \texttt{axiom-choice-1\_0-quot}). $X$ here indicates that the type $B$ above could be anything. These two lemmas are instances of the more general Nuprl lemma \texttt{axiom-choice-quot}.

6. Applications

Using SCP, we proved in Nuprl a $\Sigma$-truncated version of UCP (see Sec. \ref{SCP}) from the fan theorem, and then a fully squashed version of this principle using Escardó and Xu’s method \cite{39} (see Sec. \ref{UCPF}). We write UCP, for the version of UCP where $\Sigma$ is $\Sigma$. Using SCP, we then proved that real functions defined on the unit interval are uniformly continuous (see Sec. \ref{UCP}).

We have recently proved that Bar Induction on Decidable bars (BID) is consistent with Nuprl using our Coq model of Nuprl \cite{71}, and this for free choice sequences of natural numbers. Following Kleene, given that SCP is true we can now prove Bar Induction on Monotone bars (BIM) \cite{53, pp.78} (see also Dummett’s Thm 3.8 \cite{37, pp.64}); see Nuprl lemma\texttt{monotone-bar-induction}.

We have also recently used exceptions to implement the constructive content of the completeness result of intuitionistic first-order logic proved in \cite{27}. As in the present paper, exceptions are used to probe how a computation uses its arguments. Given a uniform evidence for a proposition, we construct a proof of that proposition by using this probing mechanism to determine the next step of the proof.

6.1 Uniform Continuity

6.1.1 UCP, \texttt{F}}\texttt{ollows From FT} and SCP.

Using BID we prove that the Fan Theorem (FT) is true: see Nuprl lemma \texttt{fan-theorem}. We then derive UCP, from FT and SCP: see Nuprl lemma \texttt{strong-continuity2-implies-uniform-continuity}. Let us sketch that proof. The version of FT that we have proved in Nuprl is (if $X$ is a bar and is decidable then it is uniform):

$$FT = \Pi X : (\Pi n : \mathbb{N}. 2^{\mathbb{N}_n} \rightarrow \mathbb{P}). \Pi f : C. \Sigma n : \mathbb{N}. X n f \rightarrow \Pi n : \mathbb{N}. f : 2^{\mathbb{N}_n} \rightarrow \Pi X. X n f$$

We also use the following corollary of SCP for functions on the Cantor space instead of the Baire space:

$$SCP \ = \ \Pi f : C \rightarrow \mathbb{N}. \ | \Sigma M f : (\Pi n : \mathbb{N}. 2^{\mathbb{N}_n} \rightarrow \mathbb{N}_0). \Pi n : \mathbb{N}. M n f =_{\mathbb{N}} \text{inl}(F(f)) \wedge \Pi n : \mathbb{N}. \text{inl}(M n f) \rightarrow M n f =_{\mathbb{N}} \text{inl}(F(f))$$

Let us start proving UCP. Let $F$ be in $C \rightarrow \mathbb{N}$. We have to prove:

$$| \Sigma n : \mathbb{N}. \Pi f : g, C. f =_{\mathbb{N}} g \rightarrow F(f) =_{\mathbb{N}} F(g)$$

(7) We start by instantiating SCPB with $F$ and we unsquash the resulting formula (which we can do because our conclusion is squashed), i.e., we get to assume:

- $M \in \Pi n : \mathbb{N}. 2^{\mathbb{N}_n} \rightarrow \mathbb{N}_0$
- $G \in \Pi f : C. \Sigma n : \mathbb{N}. M n f =_{\mathbb{N}} \text{inl}(F(f)) \wedge \Pi n : \mathbb{N}. \text{inl}(M n f) \rightarrow M n f =_{\mathbb{N}} \text{inl}(F(f))$

We now instantiate FT using $X = \lambda n. \lambda f. \text{inl}(M n f)$. We now have to prove (1) $\Pi f : C. \Sigma n : \mathbb{N}. M n f 
=_{\mathbb{N}} \text{inl}(F(f)) \wedge \Pi n : \mathbb{N}. f : 2^{\mathbb{N}_n} \rightarrow \Pi X. \text{inl}(M n f)$, which follows from $G$; and (2) $\Pi n : \mathbb{N}. f : 2^{\mathbb{N}_n} \rightarrow \Pi X. \text{inl}(M n f)$, which is trivial; and we get a $k \in \mathbb{N}$ and $A \in \Pi f : C. \Sigma n : \mathbb{N}. M n f$. We unsquash and instantiate our conclusion \cite{7} using $k - 1$. We have to prove that $F(f) =_{\mathbb{N}} F(g)$ assuming that $f =_{\mathbb{N}} g$ for $f$ and $g$ in $C$. From $G$ we get:

- $G(f) \in \Pi n : \mathbb{N}. \text{inl}(M n f) \rightarrow M n f =_{\mathbb{N}} \text{inl}(F(f))$
- $G(g) \in \Pi n : \mathbb{N}. \text{inl}(M n g) \rightarrow M n g =_{\mathbb{N}} \text{inl}(F(g))$

and from $A$ (applying $A$ to $f$) we get $a i \in \mathbb{N}_0$ and that $\text{inl}(M i f)$. Therefore, because $f =_{\mathbb{N}} g$, we get $M i f =_{\mathbb{N}} M i g$ and $\text{inl}(M i g)$. Which means that (from $G(f)$ and $G(g)$):

- $M i f =_{\mathbb{N}} \text{inl}(F(f))$
- $M i g =_{\mathbb{N}} \text{inl}(F(g))$

We conclude that $F(f) =_{\mathbb{N}} F(g)$.

6.1.2 UCP, \texttt{F}}\texttt{ollows From FT} and \texttt{akUCP}.

Following Bridges and Richman’s proof of their Theorem 3.2 \cite{13, pp.113}, the following Nuprl lemma proves that UCP follows...
7. Related Work on Nominal Systems

Nominal systems. There has been a tremendous amount of work on nominal approaches to logic and programming starting from Gabbay and Pitts’ work on using Fraenkel-Mostowski’s permutation model of set theory to formally reason about abstract syntax in the presence of $\alpha$-equivalence and variable binding [48]. This work then led to the design of the so-called Nominal Logic [65], which provides primitives and axioms to reason about names, name-swapping, freshness, and name-binding. These ideas were then later used and implemented in programming languages and type theories [16, 28, 29, 32, 43, 54, 60, 67, 68, 79, 88, 89, 88] (to cite only a few). We know describe some of these systems.

FreshML. For example, FreshML [57, 79] is an extension of ML with constructs for declaring and manipulating data with binding structure that provide support for object-level $\alpha$-equivalence, such as constructs for binding names, declaring new types of bindable names, and generating fresh names. Nuprl does not yet have such a name-abstraction construct. Also, our paper does not try to tackle the issue of reasoning about $\alpha$-equivalence classes of terms using names. This provides an alternative approach to, e.g., using de Bruijn indices or HOAS in order to deal with names and binders. These ideas were then also ported to OCaml [78]. Following this line of work, Pure FreshML [69] is a pure (in the sense that name generation is not an observable side effect) version of FreshML [79] that ensures fresh atoms do not escape their scopes.

Nominal type theories. Schapp and Stark [76, 77] developed a “bunched” dependent type theory for programming and reasoning with names, based on a categorical axiomatization of names, and taking freshness as the central primitive instead of swapping. Bunches are typing contexts that have a tree-like shape instead of a list-like shape, where branching is used to model the disjointness of names spaces. In their theory, $\alpha$-equivalence classes can be either modeled as “fresh functions” or as pairs, which are members of “non-standard fresh” $\Pi$ and $\Sigma$ types. It turns out that these types are isomorphic when indexed by names, giving rise to a hidden-name type constructor $\mathcal{H}$ which can either be interpreted as a sum or a product, and which corresponds to Gabbay and Pitts freshness quantifier $\mathcal{V}$ [44]. In our paper, we only focus on computational aspects of freshness.

Cheney designed SNTT [20], which is a nominal simply-typed $\lambda$-calculus with names as well as name-abstraction and name-concretion operators (but no name-generation operator such as $\nu$). SNTT contexts are expressive enough so that one can state the freshness constraint on name-concretions. It is also designed with decidable typechecking in mind. Cheney extended SNTT to a dependent type theory, called $\lambda^\Delta$ [21], with dependent products (\Pi) and dependent name-abstraction types (\Sigma). As for SNTT, one of his main focus was to provide a strongly normalizing theory with decidable type checking.

Westbrook’s CNIC calculus (the Calculus of Nominal Inductive Constructions) [87, 88] can also be seen as an extension of SNTT with inductive constructions, or similarly as an extension of CIC [83] with nominal features such as name abstraction and concretion operators, and pattern matching operators for names and name abstractions.

Pitts’ Nominal System T [69] extends System T with nominal features such as a fresh operator $\nu$ à la Odersky and a name-swapping operator. As opposed to the systems mentioned above,
this system has ordinary non-bunched contexts. FreshMLTT is a dependent type theory that has name-abstraction and name-concretion operators, as well as a name-swapping operator and a fresh operator à la Odersky, which allow them to derive expressive name-concretion rules.

8. Conclusion and Future Work

This paper provides “mostly” computational proofs of two Brouwerian continuity principles that use (1) diverging terms to prove that the modulus of continuity of a function on the Baire space exists in the meta-theory (Sec. 3), and (2) named exceptions to exhibit it in the theory (Sec. 4). We proved that all functions of type $T^\omega \rightarrow \mathbb{N}$ are continuous, where $T$ is a subtype of $\mathbb{N}$. It is not clear how to adapt our proof for other types or subtypes of $\mathbb{N}$. This is left for future work.

In Sec. 5.3 we used the fact that the exception $\text{exc}_a$ cannot be caught by $F$ if $a\#F$. This would no longer be true if our computational system was non-deterministic or if we allowed parallel computations. For example, let $t_1 || t_2$ be an operator that dovetails the computations of $t_1$ and $t_2$. If $t_1$ computes to $\text{exc}_a$, then this exception might get “caught” if $t_2$ computes to a canonical expression “before” $t_1$. Once we add non-determinism to Nuprl, we might be able to use non-deterministic computations to compute the modulus of continuity of functions in a similar fashion as done by Coquand and Jaber. This is left for future work.

Finally, many more inference rules can be derived (and verified in our Coq model) from the definitions of our new computations and types than the ones discussed in Sec. 4. Investigating these rules is left for future work.

Acknowledgements

We would like to thank our colleagues Robert L. Constable, Ross Tate, Rich Eaton, Abhishek Anand, and Evan Moran for their helpful criticism.

References


