On the Stability by Union of Reducibility Candidates

Colin Riba

INPL & LORIA[*], Nancy, France
riba@loria.fr

Abstract. We investigate some aspects of proof methods for the termination of (extensions of) the second-order λ-calculus in presence of union and existential types.
We prove that Girard's reducibility candidates are stable by union iff they are exactly the non-empty sets of terminating terms which are downward-closed w.r.t. a weak observational preorder.
We show that this is the case for the Curry-style second-order λ-calculus. As a corollary, we obtain that reducibility candidates are exactly the Tait's saturated sets that are stable by reduction. We then extend the proof to a system with product, co-product and positive iso-recursive types.

1 Introduction

Since their introduction in [17], union and existential types with type assignment rules are present in many type systems. From a foundational perspective, they are interesting as dual of respectively intersection and second-order types. The paper [3] provides detailed investigations on syntactic as well as semantics issues of union types. As a theoretical tool, they have been used in [8, 9] to prove that a kind of Böhm trees, called Lévy-Longo trees, distinguishes pure λ-terms exactly as does their observation in the lazy concurrent λ-calculus.

Interesting applications of union types are the XML processing languages XDuce [14] and ℂDuce [11]. They describe types of XML documents by means of regular expressions whose internal representation relies on union types.

Existentials and unions are also interesting tools for representing abstractions of programs. In the context of strictness analysis, unions are used in [15] to represent disjunctive properties of programs.

Frédéric Blanqui and the author proposed in [6] a termination criterion for higher-order conditional rewriting that use constrained types. Existential constraints arise naturally, for example when proving that some implementations of QuickSort preserves the size of its argument. This work relies on proof methods for the termination of typed λ-calculus plus rewriting in presence of existential types.

[*] UMR 7503 CNRS-INPL-INRIA-Nancy2-UHP, Campus Scientifique, BP 239, 54506 Vandoeuvre-lès-Nancy Cedex, France

Usual proofs of strong normalization (*i.e.* termination) for typed λ-calculi assign to each type T a set of strongly normalizing terms $[\![T]\!]\rho$ (the *interpretation* of T, with an assignment ρ of its free variables). Then, they use *soundness* of this interpretation w.r.t. the type system: typable terms belong to the interpretation of their types. But soundness requires that types are not interpreted by arbitrary sets of terms. They must satisfy some *closure* conditions. The two most popular ones are Girard's reducibility candidates and Tait's saturated sets. See [12] for a detailed discussion and historical references. A comparison of Girard's and Tait's closure conditions can also be found in [23].

In order to handle elimination rules of union and existential types, it is convenient to interpret these types by using unions of interpretations: $[\![T_1 \cup T_2]\!]\rho = [\![T_1]\!]\rho \cup [\![T_2]\!]\rho$ and $[\![\exists X.T]\!]\rho = \bigcup_{C \in \mathcal{C}l} [\![T]\!]\rho[C/X]$ ($\mathcal{C}l$ is the collection of closed sets under consideration). This making requires *stability by union* of closed sets: if $\mathcal{C}$ is a family of closed sets, then $\bigcup \mathcal{C} =_{\mathrm{def}} \bigcup_{C \in \mathcal{C}} C$ is closed. Approaches not relying on stability by union are briefly discussed in Sec. 8.

It is well known (see e.g. [23]) that Tait's saturated sets for β-reduction are stable by union. However, their extension with additional computational rules can by cumbersome. On the other hand, Girard's reducibility candidates are more adjustable, in particular for dealing with rewriting [5]. However, their stability by union is known to be problematic [23].

In this paper, we prove the stability by union of reducibility candidates for the polymorphic λ-calculus $\boldsymbol{\lambda 2}$. To our knowledge, this property was hitherto unknown, and even often believed to be false. We extend the proof to $\boldsymbol{\lambda 2 U^+}$, the extension of $\boldsymbol{\lambda 2}$ with product, co-product and positive iso-recursive types (it is shown in [21] that it is a proper extension of $\boldsymbol{\lambda 2}$).

The key observation is that reducibility candidates are stable by union iff they are exactly the non-empty sets of strongly-normalizing terms which are downward-closed w.r.t. a weak observational preorder (see [16] for a presentation and references on related topics). This is a very simple structure compared to the one appearing in the definition of reducibility candidates, which is not trivial and somehow mysterious. Hence, studying stability by union of reducibility candidates reveals important facts on their fundamental nature.

We show that the above condition is equivalent to say that some terms, called neutral, have a maximal reduct w.r.t. to that preorder. For the case of $\boldsymbol{\lambda 2}$ and $\boldsymbol{\lambda 2 U^+}$, we prove it by using a simple syntactic property called weak-standardization. It relies on the *orthogonality* of $\boldsymbol{\lambda 2}$ and $\boldsymbol{\lambda 2 U^+}$: computational rules are non-ambiguous and left-linear (no equality tests between open terms). As a by-product, we obtain that Girard's sets correspond exactly to the Tait's sets that are stable by reduction.

We present the syntax of $\boldsymbol{\lambda 2}$ in Sec. 2, and reducibility in Sec. 3. Our analysis of stability by union of reducibility candidates is presented in Sec. 4. Finally, the system $\boldsymbol{\lambda 2 U^+}$ is presented in Sec. 6, and stability by union of its reducibility candidates in Sec. 7.

We assume familiarity with λ-calculus and types, and refer to [13, 4] for detailed introductions.

2 The Polymorphic λ-Calculus $\boldsymbol{\lambda 2}$

The core language of the paper is the Curry-style second-order λ-calculus $\boldsymbol{\lambda 2}$, as presented in [4]. We recall the main notations below, and then discuss union and existential types.

Let $\mathcal{X}$ be a countable set of variables and Λ be the set of untyped λ-terms:

$$t, u \in \Lambda \quad ::= \quad x \in \mathcal{X} \quad | \quad \lambda x.t \quad | \quad t\,u\ .$$

They are considered equals modulo α-conversion. Terms come with the usual notion of β-reduction, namely $(\lambda x.t)u \mapsto_\beta t[u/x]$, where $t[u/x]$ is the capture-avoiding substitution of x by u in t. We let $\to$ be the smallest rewrite relation on Λ containing $\mapsto_\beta$. In the following, we refer to $\mapsto_\beta$ as the *top reduction* and denote by $\mathcal{TNF}$ the set of terms in $\mapsto_\beta$-normal form. We let $(t)_\to =_{\mathrm{def}} \{u \mid t \to u\}$ and $(t)^*_\to =_{\mathrm{def}} \{u \mid t \to^* u\}$, where $\to^*$ is the reflexive-transitive closure of $\to$. We write $(t_1, \dots, t_n) \to (t'_1, \dots, t'_n)$ iff there is i such that $t_i \to t'_i$ and $t_j = t'_j$ for all $j \neq i$. A term t is *strongly normalizing* iff every reduction sequence issued from t is finite. Let $\mathcal{SN}$ be the set of strongly-normalizing terms. Note that $t \in \mathcal{SN}$ iff either t is not reducible or all its reducts are in $\mathcal{SN}$. It follows that $\mathcal{SN}$ is the *smallest* set such that for all t,

$$(\forall u\ (t \to u \ \Rightarrow\ u \in \mathcal{SN}))\ \Rightarrow\ t \in \mathcal{SN}\ .$$

Types are the formulas of second-order minimal logic, with variables in $\mathcal{V}$:

$$T, U \in \mathcal{T} \quad ::= \quad X \in \mathcal{V} \quad | \quad T \Rightarrow U \quad | \quad \forall X.T\ .$$

We denote by $\mathcal{X}(t)$ (resp. $\mathcal{V}(T)$) the set of free variables of t (resp. T). An *environment* Γ is a finite set of declarations $x : A$ such that $x \neq y$ whenever $(x : A), (y : B) \in \Gamma$. Typing judgments are sequents of the form $\Gamma \vdash t : A$, derived with the following rules:

$$(\mathrm{Ax})\ \frac{}{\Gamma, x : T \vdash x : T}$$

$$(\Rightarrow \mathrm{I})\ \frac{\Gamma, x : U \vdash t : T}{\Gamma \vdash \lambda x.t : U \Rightarrow T} \qquad (\Rightarrow \mathrm{E})\ \frac{\Gamma \vdash t : U \Rightarrow T \qquad \Gamma \vdash u : U}{\Gamma \vdash tu : T}$$

$$(\forall\,\mathrm{I})\ \frac{\Gamma \vdash t : T}{\Gamma \vdash t : \forall X.T}\ (X \notin \mathcal{V}(\Gamma)) \qquad (\forall\,\mathrm{E})\ \frac{\Gamma \vdash t : \forall X.T}{\Gamma \vdash t : T[U/X]}$$

Existential and Union Types. Our main point is to prove the soundness (w.r.t. some closure operator) of elimination rules of union and implicit existential types. Such types are manipulated with type-assignment rules, in the spirit of [17, 3]. Typical rules for these systems are:

$$(\exists\,\mathrm{I})\ \frac{\Gamma \vdash t : T[U/X]}{\Gamma \vdash t : \exists X.T} \qquad (\exists\,\mathrm{E})\ \frac{\Gamma \vdash t : \exists X.T \quad \Gamma, x : T \vdash u : U}{\Gamma \vdash u[t/x] : U}\ (X \notin \mathcal{V}(\Gamma, U))$$

$$(\cup\mathrm{I})\frac{\Gamma \vdash t : T_i}{\Gamma \vdash t : T_1 \cup T_2}(i \in \{1,2\}) \qquad (\cup\mathrm{E})\ \frac{\Gamma \vdash t : T_1 \cup T_2 \quad \forall i \in \{1,2\},\ \Gamma, x : T_i \vdash u : U}{\Gamma \vdash u[t/x] : U}$$

It is worth noting that such types are not subject to the Curry-Howard *propositions-as-types* isomorphism, in the sense that proofs trees do not corresponds to terms. It would require to reflect all types constructions at the term level, and this leads to use explicit constructs for disjunction and existential quantification, as discussed for e.g. in [13].

This is precisely what we want to avoid in [6], where existential quantifications are used in a constrained type system. We want terms typed in this system to be used in a constrained-free type system. Hence, constraints should not appear at the term level, and we are thus interested in implicit existential types.

On the other-hand, it is clear that the impredicative codings of unions and existential quantification given in [13] do not define union and implicit existential types. This motivates us to handle the soundness of rules ($\cup$E) and ($\exists$ E) by tools lying inside the reducibility framework. A first step is to study the behavior of Girard's reducibility candidates w.r.t. union. Since type quantifications of [6] are not the usual ones, presented above, that operate on the type structure, we study stability by union in a generic way, without committing to specific typing rules.

3 Reducibility

Strong normalization proofs of $\boldsymbol{\lambda 2}$ usually interpret types $T \in \mathcal{T}$ as sets of strongly normalizing terms $[\![T]\!]\rho \subseteq \mathcal{SN}$. Then strong normalization of typable terms follows from the soundness of the interpretation:

$$\textit{If } \Gamma \vdash t : T \textit{ and } \sigma(x) \in [\![A]\!]\rho \textit{ for all } (x : A) \in \Gamma, \textit{ then } \sigma(t) \in [\![T]\!]\rho. \qquad (\star)$$

As said in the introduction, ($\star$) does not hold when types are interpreted by arbitrary subsets of $\mathcal{SN}$. In this section, we focus on a well-known collection of suitable subsets of $\mathcal{SN}$ called Girard's reducibility candidates.

Definition 3.1 (Neutral Terms). *Terms not headed by an abstraction are called* neutral. *Let $\mathcal{N}$ be the set of neutral terms.*

Let $\mathcal{HN}$, the set of hereditary neutral terms*, be the smallest set such that for all $t \in \mathcal{N}$, $(\forall u\ (t \to u \Rightarrow u \in \mathcal{HN})) \Rightarrow t \in \mathcal{HN}$.*

Note that $\mathcal{HN} \subseteq \mathcal{SN}$. Let *elimination contexts* be $E[\ ] ::= [\ ] \mid E[\ ]t$. They correspond to call-by-name evaluation contexts, dual to call-by-value evaluation contexts of [10]. We borrowed from [1] their use in reducibility.

Remark 3.2. The general intuition behind neutral terms is linked to the duality between introductions and eliminations in natural deduction. Since neutral terms are not headed by introductions, they do not interact with elimination contexts: if $t \in \mathcal{N}$ and $E[t] \to v$ then $v = E'[t']$ with $(E[\ ], t) \to (E'[\ ], t')$. It follows that for $t \in \mathcal{N}$, we have $E[t] \in \mathcal{N}$ and $E[t] \in \mathcal{SN}$ as soon as $\{E[u] \mid t \to u\} \subseteq \mathcal{SN}$.

Definition 3.3 (Reducibility Candidates). *The set of* reducibility candidates*, denoted by $\mathcal{CR}$, is the set of all $C \subseteq \mathcal{SN}$ such that*

($\mathcal{CR}0$) *if* $t \in C$ *and* $t \to u$ *then* $u \in C$,
($\mathcal{CR}1$) *if* $t \in \mathcal{N}$ *and* $(\forall u\ (t \to u \ \Rightarrow\ u \in C))$ *then* $t \in C$.

The definition of $\mathcal{SN}$ directly implies that $\mathcal{SN} \in \mathcal{CR}$. Now, let us see why $\mathcal{CR}$ is stable by intersection ($\mathcal{C} \subseteq \mathcal{CR} \Rightarrow \bigcap \mathcal{C} \in \mathcal{CR}$). Recall that a *closure operator* on a partial order $(D, \leq)$ is a function $\overline{\cdot} : D \to D$ which is idempotent: $\overline{\overline{X}} = \overline{X}$; extensive: $X \leq \overline{X}$; and monotone: $X \leq Y \Rightarrow \overline{X} \leq \overline{Y}$. It is well-known that the greatest lower bound of a family of closed elements is closed.

The *shape* of the clauses of $\mathcal{CR}$ is sufficient for the existence of a closure operator $\overline{\cdot} : \mathcal{P}(\mathcal{SN}) \to \mathcal{P}(\mathcal{SN})$ such that $\overline{X}$ is the least reducibility candidate containing X. Indeed, clauses ($\mathcal{CR}0$) and ($\mathcal{CR}1$) are *closure rules* in the sense of [19], p.17, and the existence of $\overline{\cdot}$ is insured by Thm. 2.6, see pages 16–18 of [19]. We thus have $X \in \mathcal{CR}$ iff $X = \overline{X}$.

It follows that $(\mathcal{CR}, \subseteq)$ has all greatest lower bounds, and they are given by $\bigcap$. As a consequence, it has $\bigcap \mathcal{CR}$ as least element. It is thus an inf-semi lattice with greatest element $\mathcal{SN}$, hence a complete lattice.

Proposition 3.4. *$\mathcal{HN}$ is the least element of $\mathcal{CR}$.*

Proof. We obviously have $\mathcal{HN} \subseteq C$ for all $C \in \mathcal{CR}$, hence $\mathcal{HN} \subseteq \bigcap \mathcal{CR}$. For the converse, it suffices to remark that $\mathcal{HN} \in \mathcal{CR}$. □

We now define the interpretation of arrow types.

Proposition 3.5 (Arrow Type Constructor). *The* arrow type constructor $\Rightarrow : \mathcal{P}(\Lambda) \times \mathcal{P}(\Lambda) \to \mathcal{P}(\Lambda)$, *defined as* $\mathcal{A} \Rightarrow \mathcal{B} =_{def} \{t \mid \forall u (u \in \mathcal{A} \ \Rightarrow\ tu \in \mathcal{B})\}$, *maps reducibility candidates* $\mathcal{A}$ *and* $\mathcal{B}$ *to a reducibility candidate.*

Proof. Strong normalization and stability by reduction follows directly from that of $\mathcal{B}$. For ($\mathcal{CR}1$), we have to show that if $t \in \mathcal{N}$, then $(t)_{\to} \subseteq \mathcal{A} \Rightarrow \mathcal{B}$ implies $t \in \mathcal{A} \Rightarrow \mathcal{B}$, *i.e.* $u \in \mathcal{A} \ \Rightarrow\ tu \in \mathcal{B}$. The crucial point is given by Rem. 3.2: since $tu \in \mathcal{N}$ and t does not interact with the context $[\ ]u$, we are done with ($\mathcal{CR}1$) applied to $\mathcal{B}$, using an induction on $(t, u) \in \mathcal{SN} \times \mathcal{SN}$. □

Now, given $\rho : \mathcal{V} \to \mathcal{CR}$, we can interpret types $T \in \mathcal{T}$ as reducibility candidates $[\![T]\!]\rho \in \mathcal{CR}$, with $[\![X]\!]\rho =_{\text{def}} \rho(X)$, $[\![U \Rightarrow T]\!]\rho =_{\text{def}} [\![U]\!]\rho \Rightarrow [\![T]\!]\rho$ and $[\![\forall X.T]\!]\rho =_{\text{def}} \bigcap\{[\![T]\!]\rho[C/X] \mid C \in \mathcal{CR}\}$. We can then prove soundness ($\star$), and strong normalization is a consequence of $\mathcal{X} \subseteq \mathcal{HN}$ and Prop. 3.4. See [13, 12].

4 A General Study of Stability by Union of $\mathcal{CR}$

We have seen that stability by intersection of $\mathcal{CR}$ is a consequence of the *shape* of the clauses ($\mathcal{CR}0$) and ($\mathcal{CR}1$). Such shallow observations do not imply stability by union, which must therefore be proved through a deeper analysis of $\mathcal{CR}$. Indeed, given $\mathcal{C} \subseteq \mathcal{CR}$, in order to get $\bigcup \mathcal{C} \in \mathcal{CR}$ we must show that if t is a neutral term with $(t)_{\to} \subseteq \bigcup \mathcal{C}$, then every one-step reduct of t must be in the *same* $C \in \mathcal{C}$.

We begin by stability by union of closure operators. In the next Proposition, we assume given a set D and a closure operator $\overline{\cdot} : \mathcal{P}(D) \to \mathcal{P}(D)$. Write $\overline{x}$ for $\overline{\{x\}}$ and $\overline{\mathcal{P}(D)}$ for $\{\overline{X} \mid X \subseteq D\}$.

Proposition 4.1 (Topological Closure of $\overline{\cdot}$). *Given a closure operator $\overline{\cdot} : \mathcal{P}(D) \to \mathcal{P}(D)$, let $\overline{\Omega}$ be the set of non-empty $X \subseteq D$ such that $X = \bigcup\{\overline{x} \mid x \in X\}$. Then $\overline{\Omega}$ is the smallest set such that $\overline{\mathcal{P}(D)} \subseteq \overline{\Omega}$ and $\mathcal{C} \subseteq \overline{\Omega} \Rightarrow \bigcup\mathcal{C}, \bigcap\mathcal{C} \in \overline{\Omega}$.*

Proof. For all $X \in \overline{\mathcal{P}(D)}$ we have $X = \bigcup\{\overline{x} \mid x \in X\}$ since for all $x \in X$, $\overline{x} \subseteq X$ and $x \in \overline{x}$. It follows that $\overline{\mathcal{P}(D)} \subseteq \overline{\Omega}$. If $\mathcal{C} \subseteq \overline{\Omega}$, then $C = \bigcup\{\overline{x} \mid x \in C\}$ for all $C \in \mathcal{C}$. Hence $\bigcup\mathcal{C} = \bigcup\{\overline{x} \mid x \in \bigcup\mathcal{C}\}$, and $\bigcup\mathcal{C} \in \overline{\Omega}$. Moreover, if $t \in \bigcap\mathcal{C}$, then for all $C \in \mathcal{C}$, $t \in C$ hence $\overline{t} \subseteq C$. Therefore $\overline{t} \subseteq \bigcap\mathcal{C}$, and it follows that $\bigcap\mathcal{C} = \bigcup\{\overline{t} \mid t \in \bigcap\mathcal{C}\}$, *i.e.* $\bigcap\mathcal{C} \in \overline{\Omega}$.

Now, let $\Omega \supseteq \overline{\mathcal{P}(D)}$ be stable by union and intersection. If $X \in \overline{\Omega}$ then $X = \bigcup\{\overline{x} \mid x \in X\}$. But $\{\overline{x} \mid x \in X\} \subseteq \Omega$, hence $\bigcup\{\overline{x} \mid x \in X\} \in \Omega$. □

In other words, $(D, \overline{\Omega} \cup \{\emptyset\})$ is a topological space where the set of *opens* $\overline{\Omega} \cup \{\emptyset\}$ contains all $\overline{\cdot}$-closed sets. Proposition 4.1 implies that it is moreover the *coarser* topology with this property: if Ω is a collection of opens that contains $\overline{\cdot}$-closed sets, then $\overline{\Omega} \subseteq \Omega$. We now use these facts to study the stability by union of reducibility candidates.

Since we are concerned with properties independent from the calculus, we work with an extension $\boldsymbol{\lambda}$**ext** of $\boldsymbol{\lambda}$**2**. We assume that every term typable in $\boldsymbol{\lambda}$**2** is typable in $\boldsymbol{\lambda}$**ext** and that $\boldsymbol{\lambda}$**ext** is equipped with a rewrite relation, denoted by $\to$, that is finitely branching and contains $\mapsto_\beta$. Notations of Sec. 2 are imported in $\boldsymbol{\lambda}$**ext**. Finally, we assume given a set of neutral terms of $\boldsymbol{\lambda}$**ext**, still denoted by $\mathcal{N}$, that contains the neutral terms of $\boldsymbol{\lambda}$**2**.

Definition 4.2 ($\boldsymbol{\lambda}$ext-Reducibility Candidates). *The set of* $\boldsymbol{\lambda}$**ext**-reducibility candidates*, denoted by $\mathcal{CR}$, is the set of all $C \subseteq \mathcal{SN}$ such that*

($\mathcal{CR}0$) *if $t \in C$ and $t \to u$ then $u \in C$,*

($\mathcal{CR}1$) *if $t \in \mathcal{N}$ and $(\forall u\ (t \to u \;\Rightarrow\; u \in C))$ then $t \in C$.*

As with $\boldsymbol{\lambda}$**2**, $\mathcal{CR}$ is the set of closed sets for a closure operator $\overline{\cdot} : \mathcal{P}(\mathcal{SN}) \to \mathcal{P}(\mathcal{SN})$. An explicit inductive definition of $\overline{\cdot}$ is useful:

Lemma 4.3 (The Closure Operator $\overline{\cdot}$ of $\mathcal{CR}$). *Given $X \subseteq \mathcal{SN}$, let $\overline{X}_0 =_{def} (X)^*_{\to}$, and for all $i \geq 0$, $\overline{X}_{i+1} =_{def} \overline{X}_i \cup \{t \in \mathcal{N} \mid (t)_{\to} \subseteq \overline{X}_i\}$. Then, for all $X \subseteq \mathcal{SN}$, $\overline{X} =_{def} \bigcup_{i\geq 0} \overline{X}_i$ is the smallest reducibility candidate containing X.*

Proof. First, we show that $\overline{X} \in \mathcal{CR}$.

($\mathcal{CR}0$) Let $t \to v$ and $t \in \overline{X}_i$ with i as small as possible. If $i = 0$, then $t \in (X)^*_{\to}$, hence $v \in (X)^*_{\to} = \overline{X}_0$. Otherwise, $i = j + 1$, and $v \in \overline{X}_j$.

($\mathcal{CR}1$) Let $t \in \mathcal{N}$ such that for all $v \in (t)_{\to}$, there is i_v with $v \in \overline{X}_{i_v}$. Since $\to$ is finitely branching, there is a j greater than every i_v, thus $t \in \overline{X}_{j+1}$.

Second, by induction on i, we prove that if $C \in \mathcal{CR}$ and $X \subseteq C$, then $\overline{X}_i \subseteq C$. We have $\overline{X}_0 = (X)^*_{\to} \subseteq C$ by ($\mathcal{CR}0$). For $i \geq 0$, if $t \in \overline{X}_{i+1} \setminus \overline{X}_i$, then $t \in \mathcal{N}$ and by induction hypothesis, $(t)_{\to} \subseteq \overline{X}_i \subseteq C$. Hence $t \in C$ by ($\mathcal{CR}1$). □

Thanks to Lem. 4.3, we have an explicit definition of the closure operator of $\mathcal{CR}$, denoted by $\overline{\cdot}$. Now, Prop. 4.1 gives us $\overline{\Omega}$, which is the *topological closure* of $\overline{\cdot}$. We let $\overline{\mathcal{CR}} =_{\text{def}} \overline{\Omega}$. Proposition. 4.1 implies that $\mathcal{CR} \subseteq \overline{\mathcal{CR}}$ and that $\mathcal{CR}$ is stable by union iff $\mathcal{CR} = \overline{\mathcal{CR}}$.

Before studying what insures the equality of $\mathcal{CR}$ and $\overline{\mathcal{CR}}$, let us have a look on the structure of the latter. We begin by a characterization of the membership $t \in \overline{u}$ that uses the *weak observational preorder* $\sqsubseteq$.

Definition 4.4. *Let $t \sqsubseteq u$ iff for all $v \notin \mathcal{N}$, $t \rightarrow^* v \;\Rightarrow\; u \rightarrow^* v$. We denote by $\sqsubseteq_{\mathcal{SN}}$ the restriction of $\sqsubseteq$ to $\mathcal{SN}$.*

Observational preorders where introduced to characterize behavioral equivalence: two pieces of programs are observationally equivalent iff when plugged in a program context, the obtained programs both diverges or evaluates to the same value. Contexts are arbitrary terms with a hole, including those of the form $t[\;]$ and $\lambda x.[\;]$. With closed terms, thanks to Milner's Context Lemma, this is equivalent to observation in applicative contexts (our elimination contexts). Of course, this fails for open terms. See [18, 16] for a presentation and references on the subject.

In $\boldsymbol{\lambda 2}$, non-neutral terms are abstractions, hence closed non-neutral terms correspond to the usual notion of value. Moreover, we have $t \sqsubseteq u$ iff for all $E[\;]$, for all $v \notin \mathcal{N}$, $(E[t] \rightarrow^* v \Rightarrow E[u] \rightarrow^* v)$. Thus, with $\sqsubseteq$ we observe the reduction to values of open terms plugged in elimination contexts. Hence the name *weak* observational preorder. We generalize these ideas to the system $\boldsymbol{\lambda 2 U^+}$ in Sec. 7.

In order to characterize $t \in \overline{u}$ with $\sqsubseteq$, we need a few properties. First, note that $t \rightarrow u$ implies $u \sqsubseteq t$.

Proposition 4.5. *Let $X \subseteq \mathcal{SN}$. Then $t \in \overline{X}$ iff either $t \in (X)^*_{\rightarrow}$ or ($t \in \mathcal{N}$ and $(t)_{\rightarrow} \subseteq \overline{X}$).*

Proof. The "if" direction directly follows from ($\mathcal{CR}0$) and ($\mathcal{CR}1$). Conversely, let i be as small as possible such that $t \in \overline{X}_i$. Thus, either $i = 0$ and $t \in (X)^*_{\rightarrow}$ or $i = j+1$, $t \in \overline{X}_{j+1} \setminus \overline{X}_j$ and by definition $t \in \mathcal{N}$ and $(t)_{\rightarrow} \subseteq \overline{X}_j$. □

As a consequence, all non-neutral terms of $\overline{X}$ are in $(X)^*_{\rightarrow}$. In other words, the values of $\overline{X}$ are entirely determined by X.

Proposition 4.6. *Let $t \in \mathcal{N} \cap \mathcal{SN}$ and $X \subseteq \mathcal{SN}$. Then $(t)_{\rightarrow} \subseteq \overline{X}$ iff for all $v \notin \mathcal{N}$, $t \rightarrow^* v \;\Rightarrow\; v \in (X)^*_{\rightarrow}$.*

Proof. For the "only-if" direction, we reason by induction on $t \in \mathcal{SN}$. Assume that $(t)_{\rightarrow} \subseteq \overline{X}$ and let $t \rightarrow^* v' \notin \mathcal{N}$. Since $t \in \mathcal{N}$, we have $t \rightarrow v \rightarrow^* v'$ with $v \in \overline{X}$. If $v \notin \mathcal{N}$, then by Prop. 4.5 we have $v \in (X)^*_{\rightarrow}$, hence $v' \in (X)^*_{\rightarrow}$. Otherwise, since $(v)_{\rightarrow} \subseteq \overline{X}$ we can apply the induction hypothesis and get $v' \in (X)^*_{\rightarrow}$.

For the converse, we also reason by induction on $t \in \mathcal{SN}$. If $t \in (X)^*_{\rightarrow}$ then we are done since $(t)_{\rightarrow} \subseteq (X)^*_{\rightarrow} \subseteq \overline{X}$. Assume that $t \notin (X)^*_{\rightarrow}$. Let $v \in (t)_{\rightarrow}$. If $v \notin \mathcal{N}$, then by assumption $v \in (X)^*_{\rightarrow}$, hence $v \in \overline{X}$. Otherwise, using ($\mathcal{CR}1$) it suffices to show that $(v)_{\rightarrow} \subseteq \overline{X}$. But by assumption, every $v' \in (v)^*_{\rightarrow} \setminus \mathcal{N}$ belongs to $(X)^*_{\rightarrow}$. Hence by induction hypothesis $(v)_{\rightarrow} \subseteq \overline{X}$. □

Thanks to Proposition 4.6, each $\overline{t}$ is in fact an *initial segment* w.r.t. $\sqsubseteq_{\mathcal{SN}}$.

Lemma 4.7. *For all $t \in \mathcal{SN}$, $\overline{t} = \{u \mid u \sqsubseteq_{\mathcal{SN}} t\}$.*

Proof. By Prop. 4.6, $u \in \overline{t}$ iff $t, u \in \mathcal{SN}$ and either $t \to^* u$ or $u \in \mathcal{N}$ and $(u)^*_{\to} \setminus \mathcal{N} \subseteq (t)^*_{\to}$. But this is exactly $u \sqsubseteq_{\mathcal{SN}} t$. □

This gives a nice straight structure to the elements of $\overline{\mathcal{CR}}$.

Theorem 4.8. *Let $\mathcal{O}$ be the set of non empty subsets of $\mathcal{SN}$ which are downward closed w.r.t. $\sqsubseteq_{\mathcal{SN}}$,* i.e. *$X \in \mathcal{O}$ iff $\emptyset \neq X \subseteq \mathcal{SN}$ and for all t, u, if $t \in X$ and $u \sqsubseteq_{\mathcal{SN}} t$ then $u \in X$. Then we have $\overline{\mathcal{CR}} = \mathcal{O}$.*

Proof. Thanks to Lem. 4.7, we have $X \in \overline{\mathcal{CR}}$ iff it is a non-empty subset of $\mathcal{SN}$ such that $X = \bigcup\{\overline{t} \mid t \in X\} = \{u \mid \exists t(u \sqsubseteq_{\mathcal{SN}} t \ \wedge \ t \in X)\}$, *i.e.* $X \in \mathcal{O}$. □

It is surprising that we can give such a simple structure to $\overline{\mathcal{CR}}$. The most important, however, is the consequence on the stability by union of $\mathcal{CR}$.

Corollary 4.9. *$\mathcal{CR}$ is stable by union iff $\mathcal{CR} = \mathcal{O}$.*

The structure of reducibility candidates is at a first sight not trivial and somehow mysterious. It is therefore extremely interesting to understand what allows $\mathcal{CR} = \mathcal{O}$, giving them a so simple structure. Hence the question of their stability by union reveals important facts on their fundamental nature.

The next step is to characterize what implies $\mathcal{CR} = \mathcal{O}$. Recall that Thm. 4.8 says that $\mathcal{CR} \subseteq \mathcal{O}$.

Proposition 4.10. *$\mathcal{O} \subseteq \mathcal{CR}$ iff for all $t \in \mathcal{N} \cap \mathcal{SN}$, there is $u \in (t)_{\to}$ such that $t \sqsubseteq_{\mathcal{SN}} u$.*

Proof. Let $C \in \mathcal{O}$. Since it is stable by reduction, it suffices to check that if $t \in \mathcal{N}$ and $(t)_{\to} \subseteq C$, then $t \in C$. But there is $u \in (t)_{\to}$ such that $t \sqsubseteq_{\mathcal{SN}} u$, and $u \in C$ implies $t \in C$. Therefore, $C \in \mathcal{CR}$. Conversely, assume that $\mathcal{O} \subseteq \mathcal{CR}$. Let $t \in \mathcal{N} \cap \mathcal{SN}$ and $X =_{\text{def}} \bigcup\{\overline{u} \mid t \to u\}$. By Lem. 4.7, we have $X \in \mathcal{O} \subseteq \mathcal{CR}$, hence $t \in X$ since $t \in \mathcal{N}$ and $(t)_{\to} \subseteq X$. It follows that there is some $u \in (t)_{\to}$ such that $t \sqsubseteq_{\mathcal{SN}} u$. □

The property of $\mathcal{SN}$ neutral terms expressed in Prop. 4.10 is that a reduct u of a neutral term t such that $t \sqsubseteq_{\mathcal{SN}} u$ is in some sense a *principal reduct of* t: the values of t are exactly those of u. Moreover, $u \in \max_{\sqsubseteq_{\mathcal{SN}}} (t)_{\to}$, *i.e.* a principal reduct is maximal among all possible reducts.

For $\boldsymbol{\lambda 2}$, this has to be linked with call-by-name languages, in which terms to be evaluated are neutral, and the evaluation preserves possible values.

Definition 4.11. *A term $u \in (t)_{\to}$ is a* principal reduct *(written p.r.) of t iff $t \sqsubseteq u$ and t is said to have the* principal reduct property *(written p.r.p.) when either such a u exists or t is a normal form.*

We reduce the stability by union of $\mathcal{CR}$ to the principal reduct property for neutral terms.

Corollary 4.12. *We have $\mathcal{C} \subseteq \mathcal{CR} \Rightarrow \bigcup \mathcal{C} \in \mathcal{CR}$ iff every $t \in \mathcal{N} \cap \mathcal{SN}$ has the principal reduct property.*

As pointed out by Prop. 3.5, in order for $t \in \mathcal{N}$ to belong to $C \in \mathcal{CR}$, C uses information on the behavior of t in elimination contexts. This information is given by the values of t, and clause ($\mathcal{CR}1$) relies on the fact since $t \in \mathcal{N}$, its values are that of $(t)_{\rightarrow}$. But if $t \sqsubseteq_{\mathcal{SN}} u$, the values of t are also values of u. That is, if $u \in C$ and $t \sqsubseteq_{\mathcal{SN}} u$ then $t \in C$, and it follows that $t \sqsubseteq_{\mathcal{SN}} u$ implies $t \in \overline{u}$. Moreover, Lem. 4.7 says that this exactly characterizes $\overline{u}$: if it contains t, then the values of t are values of u.

Now, recall that given $\mathcal{C} \subseteq \mathcal{CR}$, in order to get $\bigcup \mathcal{C} \in \mathcal{CR}$ we must show that if $t \in \mathcal{N}$ has $(t)_{\rightarrow} \subseteq \bigcup \mathcal{C}$, then every $v \in (t)_{\rightarrow}$ must be in fact the *same* $C \in \mathcal{C}$. This amounts to say that $(t)_{\rightarrow}$ contains an u such that $t \sqsubseteq_{\mathcal{SN}} u$, hence that t has a principal reduct.

5 Stability by Union of $\mathcal{CR}$ in $\boldsymbol{\lambda}$2

In this section, we show the p.r.p. for $\boldsymbol{\lambda}\mathbf{2}$. This leads to observe that reducibility candidates are exactly the Tait's saturated sets which are stable by reduction. We do not give the proofs that are subsumed by those for $\boldsymbol{\lambda}\mathbf{2U}^{+}$, presented in Sec. 7.

The p.r.p. is a consequence of the standardization theorem of $\boldsymbol{\lambda}\mathbf{2}$. However, since we only need this property on $\mathcal{SN}$ terms, it can be proved using a weaker property, called weak standardization.

This property was coined in [2] as a consequence of standardization. However, it admits a much direct proof, which rely on the orthogonality of the calculus. By the way, it is less a *weak standardization* property than a standardization for the *weak head reduction*, which corresponds to reduction in elimination contexts.

Definition 5.1 (Weak Head Reduction). *The relation $\rightarrow_{\mathcal{H}}$ of* weak head reduction *is defined as $t \rightarrow_{\mathcal{H}} u$ iff $t = E[t']$, $t' \mapsto_{\beta} u'$ and $E[u'] = u$. We denote by $\mathcal{HNF}$ the set of terms in $\rightarrow_{\mathcal{H}}$-normal form.*

Lemma 5.2 (Weak Standardization). *Let $t \mapsto_{\beta} u$ and assume that $E[t] \rightarrow v$ with $v \neq E[u]$. Then $v = E'[t']$ with $(E[\ ], t) \rightarrow (E'[\ ], t')$ and there exists u' such that $t' \mapsto_{\beta} u'$ and $E[u] \rightarrow^{*} E'[u']$.*

In order to show that strongly normalizing neutral terms have the p.r.p., we use in addition the fact that $\mathcal{HNF} \cap \mathcal{N}$ (*i.e.* the set of terms of the from $E[x]$), is stable by reduction. We then obtain stability by union of $\mathcal{CR}$, thanks to Cor. 4.12.

Lemma 5.3 (Principal Reduct Property). *Let $t \in \mathcal{N} \cap \mathcal{SN}$. If there is u such that $t \rightarrow_{\mathcal{H}} u$ then it is a p.r. of t, otherwise every $u \in (t)_{\rightarrow}$ is a p.r. of t.*

Theorem 5.4. *If $\mathcal{C} \subseteq \mathcal{CR}$ then $\bigcup \mathcal{C} \in \mathcal{CR}$.*

The principal reduct property of neutral terms corresponds to the fact that reducibility candidates are stable by strongly normalizing weak head expansions.

Lemma 5.5 (Weak Head Expansion and Reducibility Candidates). *Let $C \in \mathcal{CR}$. If $E[s] \in C$, $t \mapsto_\beta s$ and $t \in \mathcal{SN}$ then $E[t] \in C$.*

Weak head reduction is the main notion of the Krivine Abstract Machine, and stability by weak head expansion is the main property required by truth values of Krivine and Danos [7].

Thanks to Cor. 4.9, we have shown that $\mathcal{CR} = \mathcal{O}$, thus giving a nice straight structure to $\mathcal{CR}$. Moreover, Lem. 5.3, 4.7 and 5.5 imply that for all $C \in \mathcal{CR}$,
($\mathcal{SAT}1$) if $E[x] \in \mathcal{SN}$ then $E[x] \in C$; and
($\mathcal{SAT}2$) if $E[s] \in C$, $t \mapsto_\beta s$ and $t \in \mathcal{SN}$, then $E[t] \in C$.

Subsets of $\mathcal{SN}$ satisfying ($\mathcal{SAT}1$) and ($\mathcal{SAT}2$) are Tait's *saturated sets*.

Definition 5.6. *Let $\mathcal{SAT}$ be the set of all subsets $S \subseteq \mathcal{SN}$ satisfying ($\mathcal{SAT}1$) and ($\mathcal{SAT}2$). We denote by $\mathcal{SAT}_\rightarrow$ the collection of $S \in \mathcal{SAT}$ that are stable by reduction: If $t \in S$ and $t \to u$ then $u \in S$ ($\mathcal{SAT}0$).*

The definition makes sense since in ($\mathcal{SAT}1$) we have $E[x] \in \mathcal{SN}$, and, in ($\mathcal{SAT}2$) we have $E[t] \in \mathcal{SN}$ by Lem. 5.5.

The stability by union of $\mathcal{CR}$ is therefore linked with the fact that every $C \in \mathcal{CR}$ is saturated. This inclusion has been coined in [12]. The converse is false, as shown by a counter-example given in [23] (Lem. 3.16 pp. 87–88). It relies on the fact that saturated sets are not stable by reduction. However, we can show that saturated sets that are stable by reduction are exactly the reducibility candidates. This seems to have not been remarked before.

Theorem 5.7. *$\mathcal{SAT}_\rightarrow = \mathcal{CR}$.*

Proof. The inclusion $\mathcal{CR} \subseteq \mathcal{SAT}$ has been coined in [12]. It is a direct consequence of Lem. 5.5 and the stability by reduction of head-normal forms.

The converse, $\mathcal{SAT}_\rightarrow \subseteq \mathcal{CR}$, does not seem to have been published before. Let $S \in \mathcal{SAT}_\rightarrow$. It satisfies ($\mathcal{CR}0$) thanks to ($\mathcal{SAT}0$). As for ($\mathcal{CR}1$), let $v \in \mathcal{N}$ such that $(v)_\rightarrow \subseteq S$. Thus $v \in \mathcal{SN}$. If $v \in \mathcal{HNF}$, then $v = E[x] \in S$ by ($\mathcal{SAT}0$). Otherwise, $v = E[t]$ with $t \mapsto_\beta u$ and $E[u] \in S$ by assumption. Hence $v \in S$ by ($\mathcal{SAT}2$). □

6 The System $\boldsymbol{\lambda}$2U$^+$ of Product, Co-Product and Positive Iso-Recursive Types

We now extend results of the previous section by applying Cor. 4.12 to a system with more elaborated types. The system considered, called $\boldsymbol{\lambda}\mathbf{2U}^+$, features product, co-product, positive iso-recursive types and the final type 1. It is a proper extension of $\boldsymbol{\lambda}\mathbf{2}$ [21]. Our presentation is inspired by that of [1]. Types are extended with:

$$T, U \in \mathcal{T} \quad ::= \quad \dots \quad | \quad T \times U \quad | \quad T + U \quad | \quad \mu X.T \quad | \quad 1$$

where, in $\mu X.T$, X occurs only positively in T: any path from the root of T to an occurrence of X chooses the left argument of $\Rightarrow$ an even number of times. The syntax of terms is enriched with corresponding introductions and eliminations:

$$\begin{array}{lllll} s, t \in \Lambda ::= & \dots & \mid & () & \\ & \mid\ \langle t, u \rangle & \mid & \pi_i t & i \in \{1,2\} \\ & \mid\ \mathsf{inj}_i\, t & \mid & \mathsf{case}\,(u, x_1.t_1, x_2.t_2) & i \in \{1,2\} \\ & \mid\ \mathsf{in}\, t & \mid & \mathsf{out}\, t & \end{array}$$

We consider the following extension of β-reduction:

$$\pi_i \langle t_1, t_2 \rangle \mapsto_\beta t_i \qquad \mathsf{case}\,(\mathsf{inj}_i\, u, x_1.t_1, x_2.t_2) \mapsto_\beta t_i[u/x_i] \qquad \mathsf{out}\,(\mathsf{in}\, t) \mapsto_\beta t\ .$$

We let $\rightarrow$ be the smallest rewrite relation on Λ containing $\mapsto_\beta$. The type system is enriched with the following additional rules:

$$(1\,\mathrm{I})\ \frac{}{\Gamma \vdash () : 1}$$

$$(\times\mathrm{I})\ \frac{\Gamma \vdash t_1 : T_1 \qquad \Gamma \vdash t_2 : T_2}{\Gamma \vdash \langle t_1, t_2 \rangle : T_1 \times T_2} \qquad (\times\mathrm{E})\ \frac{\Gamma \vdash t : T_1 \times T_2}{\Gamma \vdash \pi_i t : T_i}\ (i \in \{1,2\})$$

$$(+\mathrm{I})\ \frac{\Gamma \vdash t : T_i}{\Gamma \vdash \mathsf{inj}_i\, t : T_1 + T_2}\ (i \in \{1,2\}) \qquad (+\mathrm{E})\ \frac{\Gamma \vdash t : T_1 + T_2 \quad \Gamma, x : T_i \vdash t_i : U}{\Gamma \vdash \mathsf{case}\,(t, x_1.t_1, x_2.t_2) : U}$$

$$(\mu\mathrm{I})\ \frac{\Gamma \vdash t : T[\mu X.T/X]}{\Gamma \vdash \mathsf{in}\, t : \mu X.T} \qquad (\mu\mathrm{E})\ \frac{\Gamma \vdash t : \mu X.T}{\Gamma \vdash \mathsf{out}\, t : T[\mu X.T/X]}$$

Example 6.1. Our motivation to consider $\boldsymbol{\lambda}\mathbf{2U}^{+}$ is that it is a very atomic calculus for inductives types. For example, polymorphic lists can be encoded as follows:

$$\begin{array}{rcl} \mathsf{List} & =_{\mathrm{def}} & \forall Y.\mu X.1 + Y \times X \\ \mathsf{nil} & =_{\mathrm{def}} & \mathsf{in}\,(\mathsf{inj}_1\, ()) \\ \mathsf{cons}\,(x, xs) & =_{\mathrm{def}} & \mathsf{in}\,(\mathsf{inj}_2\, \langle x, xs \rangle) \end{array}$$

In [21], it is shown that higher-order primitive recursion can be defined using iso-recursives types and the rule $\mathsf{out}\,(\mathsf{in}\, t) \mapsto_\beta t$, and moreover that this rule can not be simulated in $\boldsymbol{\lambda}\mathbf{2}$ by means of β-reductions.

7 Reducibility and Stability by Union for $\boldsymbol{\lambda}\mathbf{2U}^{+}$

We now introduce tools for reducibility in $\boldsymbol{\lambda}\mathbf{2U}^{+}$. We then prove the p.r.p. and equivalence of $\mathcal{CR}$ and a suitable version of $\mathcal{SAT}_{\rightarrow}$.

We define the *top reduction* as $\mapsto_\beta$, and still denote by $\mathcal{TNF}$ the set of terms in top-normal form. It is convenient to factorize the introduction-elimination duality of natural deduction with the following atomic contexts: *atomic eliminations contexts* (aec) denoted by $\epsilon[\ ]$ and *atomic introduction contexts* (aic) denoted by $\iota[\ ]$ are defined as follows:

$$\epsilon[\ ] ::= \ [\ ]t \ \mid\ \pi_1[\ ] \ \mid\ \pi_2[\ ] \ \mid \mathsf{case}\,([\ ], x_1.t_1, x_2.t_2) \mid \mathsf{out}\,[\ ]\ ;$$

$$\iota[\ ] ::= \lambda x.[\ ] \mid \langle [\ ], t \rangle \mid \langle t, [\ ] \rangle \mid\ \ \mathsf{inj}_1\,[\ ] \ \ \mid\ \ \mathsf{inj}_2\,[\ ] \ \ \mid\ \ \mathsf{in}\,[\ ] \ \ \mid () \ .$$

Note that the introduction context for the terminal type constructor is not linear. The columns of the above array define a relation written $\epsilon[\ ] \perp \iota[\ ]$. We have $\epsilon[\ ] \perp \iota[\ ]$ when $\epsilon[\iota[\ ]]$ is a β-redex, except for the product, where we let

$$\begin{array}{rccc} & \pi_1[\ ] \perp \langle [\ ], t\rangle & \text{and} & \pi_2[\ ] \perp \langle t, [\ ]\rangle \\ \text{but} & \pi_2[\ ] \not\perp \langle [\ ], t\rangle & \text{and} & \pi_1[\ ] \not\perp \langle t, [\ ]\rangle\ . \end{array}$$

Then, to each aec $\epsilon[\ ]$ corresponds the set $\epsilon[\ ]^{\perp}$ of aic $\iota[\ ]$ such that $\epsilon[\ ] \perp \iota[\ ]$, and conversely, $\iota[\ ]^{\perp}$ is the set of aec $\epsilon[\ ]$ such that $\epsilon[\ ] \perp \iota[\ ]$. In the following, we will sometime write unambiguously $\iota[\ ] \perp \epsilon[\ ]$ instead of $\epsilon[\ ] \perp \iota[\ ]$. The extension of elimination contexts $E[\ ]$ is obvious: $E[\ ] ::= [\ ] \mid \epsilon[E[\ ]]$.

Proposition 7.1. *If $E[\epsilon[t]] \to v$, then $v = E'[t']$ with $(E[\ ], \epsilon[t]) \to (E'[\ ], t')$.*

Proof. By structural induction on $E[\ ]$. The case $E[\ ] = [\ ]$ is obvious. In the other cases, we have $E[\ ] = \epsilon'[F[\ ]]$. First, the reduction $\epsilon'[F[\epsilon[t]]] \to v$ can not be a top reduction. Hence we have $v = \epsilon''[v']$ with $(\epsilon'[\ ], v) \to (\epsilon''[\ ], v')$, and by induction hypothesis $v' = F'[t']$ with $(F[\ ], t) \to (F'[\ ], t')$. Take $E'[\ ] = \epsilon''[F'[\ ]]$. □

Definition 7.2. *We say that terms not of the form $\iota[t]$ are neutral and denote by $\mathcal{N}$ the set of neutral terms.*

Hence, the terms nil and $\mathsf{cons}(x, l)$ of Ex. 6.1 are not neutral. This strengthen our intuition that non-neutral terms corresponds to values. Note that elimination contexts are a generalization of applicative contexts to product, coproduct and iso-recursive types. We can now substantiate our claim that $\sqsubseteq$ is a weak observational preorder.

Proposition 7.3. *$t \sqsubseteq u$ iff $\forall E[\ ]\ (E[t] \to^* \iota[h] \ \Rightarrow\ E[u] \to^* \iota[h])$.*

Proof. Obviously, $\forall E[\ ]\ (E[t] \sqsubseteq E[u])$ implies $t \sqsubseteq u$ (take the empty context). Conversely, assume that $t \sqsubseteq u$. If $E[t] \to^* \iota[h]$, we are in the case that $E[t] \to^* E'[\iota'[h']] \to^* \iota[h]$ with $(E[\ ], t) \to^* (E'[\ ], \iota'[t'])$. Since $t \sqsubseteq u$, we have $u \to^* \iota'[h']$, hence $E[u] \to^* E'[\iota'[h']] \to^* \iota[h]$. □

We obtain $\mathcal{CR}$ by instantiating Def. 4.2 with $\boldsymbol{\lambda 2}\mathbf{U}^{+}$ and $\mathcal{N}$. Notions of weak head reduction and weak head normal forms are directly adapted from Sec. 5, with the obvious update of elimination contexts. Recall that $u \in \mathcal{HNF}$ iff for all $E[\ ]$, t such that $u = E[t]$, we have $t \in \mathcal{TNF}$. It follows that untyped terms in $\mathcal{HNF} \cap \mathcal{N}$ need not to be of the form $E[x]$. However, stability by reduction of $\mathcal{HNF} \cap \mathcal{N}$ still holds.

Proposition 7.4. *If $t \in \mathcal{HNF} \cap \mathcal{N}$ and $t \to u$, then $u \in \mathcal{HNF} \cap \mathcal{N}$.*

Proof. We reason by structural induction on t. The case $t \in \mathcal{X}$ is trivial. Assume $t = \epsilon[t_1]$ and let $t \to t'$. Since $t \in \mathcal{HNF}$, we have $t' = \epsilon'[t_1']$ with $(t_1, \epsilon[\ ]) \to (t_1', \epsilon'[\ ])$, hence $t' \in \mathcal{N}$. If $t_1 \in \mathcal{N}$, then $t_1 \in \mathcal{N} \cap \mathcal{HNF}$ and by induction hypothesis $t_1' \in \mathcal{N} \cap \mathcal{HNF}$. It follows that $t' = \epsilon'[t_1'] \in \mathcal{HNF}$. Otherwise, $t_1 = \iota[t_2]$ with $\epsilon[\ ] \not\perp \iota[\ ]$. Hence, $t_1' = \iota'[t_2']$ with $(t_2, \iota[\ ]) \to (t_2', \iota'[\ ])$, and $\epsilon'[\ ] \not\perp \iota'[\ ]$. Hence $t' = \epsilon'[\iota'[t_2']] \in \mathcal{HNF}$. □

We now turn to weak standardization. It is stated and used for $\boldsymbol{\lambda 2\mathbf{U}^+}$ in [1].

Proposition 7.5. *If $t \mapsto_\beta u$ and $t \to v$, then either $v = u$ or there exists u' such that $v \mapsto_\beta u' \leftarrow^* u$.*

Proof. By cases on $t \mapsto_\beta u$.

$t = (\lambda x.t_1)t_2$. In this case, $u = t_1[t_2/x]$ and if $v \neq u$, then $v = (\lambda x.t'_1)t'_2$ with $(t_1, t_2) \to (t'_1, t'_2)$, and $v \mapsto_\beta t'_1[t'_2/x] \leftarrow^* u$.

$t = \pi_i\langle t_1, t_2\rangle$. In this case, $u = t_i$, and if $v \neq u$, then $v = \pi_i\langle t'_1, t'_2\rangle$ with $(t_1, t_2) \to (t'_1, t'_2)$, and $v \mapsto_\beta t'_i \leftarrow^* u$.

$t = \mathsf{case}\,(\mathsf{inj}_i\, r, x_1.t_1, x_2.t_2)$. In this case, $u = t_i[r/x_i]$ and if $v \neq u$, then $v = \mathsf{case}\,(\mathsf{inj}_i\, r', x_1.t'_1, x_2.t'_2)$ with $(r, t_1, t_2) \to (r', t'_1, t'_2)$ and $v \mapsto_\beta t'_i[r'/x_i] \leftarrow^* u$.

$t = \mathsf{out}\,(\mathsf{in}\, r)$. In this case, $u = r$ and if $v \neq u$, then $v = \mathsf{out}\,(\mathsf{in}\, r')$ with $r \to r'$ and $v \mapsto_\beta r' \leftarrow u$.

□

Lemma 7.6 (Weak Standardization). *If $t \mapsto_\beta u$ and $E[t] \to v$, then either $v = E[u]$ or $v = E'[t']$ for some $E'[\ ]$, t' such that $(E[\ ], t) \to (E'[\ ], t')$ and there exists u' such that $t' \mapsto_\beta u'$ and $E[u] \to^* E'[u']$.*

Proof. Let $E[t] \to v$ with $v \neq E[u]$. Since $t \mapsto_\beta u$, t is an elimination and by Prop. 7.1, $v = E'[t']$ where $(E[\ ], t) \to (E'[\ ], t')$. The case $E[\ ] \to E'[\ ]$ with $t = t'$ is trivial. Otherwise, we have $t \to t'$ with $E'[\ ] = E[\ ]$ and we conclude by Prop. 7.5. □

It follows that strongly normalizing neutral terms have the p.r.p..

Lemma 7.7 (Principal Reduct Property). *Let $t \in \mathcal{N} \cap \mathcal{SN}$. If there is u such that $t \to_\mathcal{H} u$, then it is a p.r. of t, otherwise every $u \in (t)_\to$ is a p.r. of t.*

Proof. Let $t \in \mathcal{N} \cap \mathcal{SN}$. If $t \in \mathcal{HNF}$, since $\mathcal{HNF} \cap \mathcal{N}$ is stable by reduction by Prop. 7.4, t never reduces to a non-neutral term. It follows that $t \sqsubseteq_{\mathcal{SN}} u$ for all $u \in (t)_\to$. Otherwise, $t \to_\mathcal{H} u$ and by induction on $t \in \mathcal{SN}$, we show that u is the p.r. of t. If $t \to^* v \notin \mathcal{N}$, since $t \in \mathcal{N}$, there is t' such that $t \to t' \to^* v$. By Lem. 7.6, if $t' \neq u$, there is u' such that $t' \to_\mathcal{H} u' \leftarrow^* u$. Therefore, $t' \in \mathcal{N} \cap \mathcal{SN}$ and by induction hypothesis $t' \sqsubseteq_{\mathcal{SN}} u'$, hence $u \to^* u' \to^* v$. □

Using Cor. 4.12, we have thus proved:

Theorem 7.8. *If $\mathcal{C} \subseteq \mathcal{CR}$ then $\bigcup \mathcal{C} \in \mathcal{CR}$.*

As in Sec. 5, we get stability of reducibility candidates by weak head expansion.

Lemma 7.9 (Weak Head Expansion and Reducibility Candidates). *Let $C \in \mathcal{CR}$. If $E[s] \in C$, $t \mapsto_\beta s$ and $t \in \mathcal{SN}$, then $E[t] \in C$.*

Proof. We obtain easily that $E[t] \in \mathcal{SN}$, using Lem. 7.6 and an induction on $(E[\ ], t) \in \mathcal{SN} \times \mathcal{SN}$. It suffices to show that $(E[t])_\to \subseteq \mathcal{SN}$. Given $v \in (t)_\to$, if $v \neq E[s]$, then by Prop. 7.6, $v = E'[t']$ with $(E[\ ], t) \to (E'[\ ], t')$ and there is s' such that $t' \mapsto_\beta s'$ and $E[s] \to^* E'[s']$. Since $E'[s'] \in \mathcal{SN}$, by induction hypothesis $E'[t'] \in \mathcal{SN}$.

Now, by Lem. 4.7, $E[t] \in \overline{E[s]}$ iff $E[t] \sqsubseteq_{\mathcal{SN}} E[s]$. But this follows from Lem. 7.7, and we get $E[t] \in \overline{E[s]} \subseteq C$. □

Unlike reducibility candidates, saturated sets are modified. They use elimination contexts in an essential way. The new clauses for $\mathcal{SAT}$ are the following:
($\mathcal{SAT}1$) $\mathcal{HNF} \cap \mathcal{SN} \cap \mathcal{N} \subseteq S$.
($\mathcal{SAT}2$) If $s \in S$, $t \to_{\mathcal{H}} s$ and $t \in \mathcal{SN}$ then $t \in S$.
As in Def. 5.6, we denote by $\mathcal{SAT}_{\to}$ the collection of saturated sets that are stable by reduction (axiom ($\mathcal{SAT}0$)).

Non-emptiness of $\mathcal{SAT}$ follows from Lem. 7.9. The clauses given for $\mathcal{SAT}$ are not common. They are usually replaced by:
($\mathcal{SAT}1'$) If $E[x] \in \mathcal{SN}$ then $E[x] \in S$.
($\mathcal{SAT}2'$) If $E[s] \in S$, $t \mapsto_{\beta} s$ and $t \in \mathcal{SN}$ then $E[t] \in S$.
First, according to Lem. 7.9, ($\mathcal{SAT}2'$) is equivalent to ($\mathcal{SAT}2$). Second, for the strong normalization proof, ($\mathcal{SAT}1'$) is sufficient. But for the correspondence with Girard sets we use ($\mathcal{SAT}1$). The following suggests that ($\mathcal{SAT}1'$) would have been sufficient if $\mathcal{CR}$ and $\mathcal{SAT}_{\to}$ have consists of *well typed* terms only.

Proposition 7.10. *Well typed terms in $\mathcal{N}$ are the terms of the form $E[t]$ where either $t \in \mathcal{X}$ or $t \notin \mathcal{TNF}$.*

Theorem 7.11. $\mathcal{SAT}_{\to} = \mathcal{CR}$.

Proof. We begin by showing that $\mathcal{CR} \subseteq \mathcal{SAT}_{\to}$. Let $C \in \mathcal{CR}$. ($\mathcal{SAT}0$) follows from ($\mathcal{CR}0$). For ($\mathcal{SAT}1$), we can reason by induction on $\to$, since by Prop. 7.4, $\mathcal{HNF} \cap \mathcal{N} \cap \mathcal{SN}$ is stable by reduction. Finally, the satisfaction ($\mathcal{SAT}2$) directly follows from Lem. 7.9.

Conversely, we show that $\mathcal{SAT}_{\to} \subseteq \mathcal{CR}$. Let $S \in \mathcal{SAT}_{\to}$. As above, ($\mathcal{CR}0$) follows from ($\mathcal{SAT}0$). For ($\mathcal{CR}1$), we have to show that for every neutral term v such that $(v)_{\to} \subseteq S$, then $v \in S$. First, $v \in \mathcal{SN}$ since $(v)_{\to} \subseteq S \subseteq \mathcal{SN}$. Thus, we conclude by ($\mathcal{SAT}1$) if $v \in \mathcal{HNF}$. Otherwise, $v = E[t]$ with $t \mapsto_{\beta} s$ and $E[s] \in S$. Thus $v \in S$ by ($\mathcal{SAT}2$). □

8 Conclusion and Related Works

Related Works. There are interesting alternatives approaches, which may not rely on stability by union. Using bi-orthogonality (see [7]), Melliès and Vouillon present a semantic of types that is not stable by union, and instead relies on a closer adequation between the interpretations and the typing rules [22].

Without unions and existentials, bi-orthogonals work well for strong normalization, especially for classical logic [20]. With non-ambiguous left-linear calculus, it is not unreasonable to expect that they can deal with existentials and union types, but the proof would rely on non-trivial properties of the calculus.

Concluding Remarks. We have shown that, with some well-behaved calculi, Girard's reducibility candidates are stable by union. This was commonly believed to be false. Moreover, and maybe more important, we have shown that their definition hide a very simple structure, namely that candidates are exactly the non empty subsets of $\mathcal{SN}$ that are downward-closed w.r.t. the weak observational preorder $\sqsubseteq_{\mathcal{SN}}$.

This shed new light on the semantics of strong normalization. In particular, we hope that this can lead to precise comparisons of bi-orthogonal and candidates. A related question is to know when the soundness of elimination rules of union and existentials types can be proved without stability by union of some type interpretation.

Acknowledgments. The author thanks Frédéric Blanqui and Claude Kirchner for useful advices, support and comments, and Marco Gaboardi for a plenty of interesting discussions. Antoine Reilles suggested interesting improvements in the presentation, and the anonymous referees made interesting insightful comments.

References

[1] A. Abel. Termination Checking with Types. *RAIRO – Theoretical Informatics and Applications*, 38(4):277–319, 2004. Special Issue (FICS'03). 4, 10, 13

[2] T. Altenkirch. *Constructions, Inductive Types and Strong Normalization.* PhD thesis, University of Edinburgh, 1993. 9

[3] F. Barbanera, M. Dezani-Ciancaglini, and U. de'Liguoro. Intersection and Union Types: Syntax and Semantics. *Information and Computation*, 119:202–230, 1995. 1, 3

[4] H. Barendregt. Lambda Calculi with Types. In S. Abramsky, D.M. Gabbay, and T.S.E. Maibaum, editors, *Handbook of Logic in Computer Science*, volume 2. Oxford University Press, 1992. 2, 3

[5] F. Blanqui, J.-P. Jouannaud, and M. Okada. Inductive-Data-Types Systems. *Theoretical Computer Science*, 271, 2002. 2

[6] F. Blanqui and C. Riba. Combining Typing and Size Constraints for Checking the Termination of Higher-Order Conditional Rewrite Systems. In *LPAR'06*, LNCS, 2006. 1, 4

[7] V. Danos and J.-L. Krivine. Disjunctive Tautologies as Synchronisation Schemes. In *CSL'00*, volume 1862 of *LNCS*, pages 292–301, 2000. 10, 14

[8] M. Dezani-Ciancaglini, U. de' Liguoro, and P. Piperno. A Filter Model for Concurrent Lambda-Calculus. *Siam Journal on Computing*, 27(5):1376–1419, 1998. 1

[9] M. Dezani-Ciancaglini, J. Tiuryn, and P. Urzyczyn. Discrimination by Parallel Observers. In *LICS'97*, 1997. 1

[10] M. Felleisen and R. Hieb. The Revised Report on the Syntactic Theories of Sequential Control and State. *Theoretical Computer Science*, 103(2):235–271, 1992. 4

[11] A. Frisch, G. Castagna, and V. Benzaken. Semantic Subtyping. In *LICS'02*, 2002. 1

[12] J.H. Gallier. On Girard's "Candidats de Reducibilité". In P. Odifredi, editor, *Logic and Computer Science*. Academic Press, 1989. 2, 5, 10

[13] J.-Y. Girard, Y. Lafont, and P. Taylor. *Proofs and Types.* Cambridge University Press, 1989. 2, 4, 5

[14] H. Hosoya, J. Vouillon, and B. Pierce. Regular Expression Types for XML. In *ICFP'00*, 2000. 1

[15] T. Jensen. Disjunctive Strictness Analysis. In *LICS'92*, 1992. 1

[16] T. Jim and A. R. Meyer. Full Abstraction and the Context Lemma. *Siam Journal on Computing*, 25(3):663–696, 1996. 2, 7

[17] D. MacQueen, G. Plotkin, and R. Sethi. An Ideal Model for Recursive Polymorphic Types. *Information and Control*, 71(1-2):95–130, 1986. 1, 3

[18] R. Milner. Fully Abstract Models of Typed λ-Calculi. *Theoretical Computer Science*, 4:1–22, 1977. 7

[19] J.-B. Nation. Notes on Lattice Theory. Available at `http://www.math.hawaii.edu/~jb/books.html`. 5

[20] M. Parigot. Proofs of Strong Normalization for Second Order Classical Natural Deduction. *Journal of Symbolic Logic*, 62(4):1461–1479, 1997. 14

[21] Z. Spławski and P. Urzyczyn. Type Fixpoints: Iteration vs. Recursion. In *ICFP'99*, pages 102–113. ACM, 1999. 2, 10, 11

[22] J. Vouillon and P.-A. Melliès. Semantic Types: A Fresh Look at the Ideal Model for Types. In *POPL'04*. ACM, 2004. 14

[23] B. Werner. *Une Théorie des Contructions Inductives.* PhD thesis, Université Paris 7, 1994. 2, 10