A COQ FORMALIZATION OF DE BRUIJN'S WEAK DIAMOND PROPERTY

Roy Overbeek (1983768)

BSc thesis, Computer Science

Supervisors:
dr. Jörg Endrullis
dr. Dimitri Hendriks

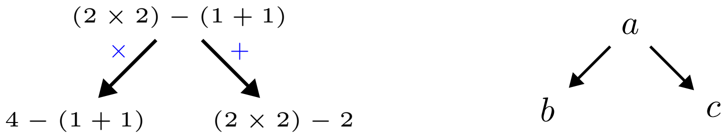
July 2015

Abstract

De Bruijn's weak diamond property is a criterion for proving confluence of abstract reduction systems. We have formalized a correctness proof for this criterion [5] using the interactive theorem prover Coq. The proof itself is inspired by Endrullis and Klop's [3] proof for the theorem that Vincent van Oostrom's decreasing diagrams imply confluence. The formalization is described and compared with the proof in [3].

1 Introduction

An *abstract reduction system (ARS)* consists of a set of objects A and a relation $\rightarrow \subseteq A \times A$ [6]. The ARS formalism unifies theory on transitional[1] properties, since it abstracts from the internal structure of transitional models of computation, as shown in Figure 1. Well-known examples of such models include term rewriting systems, graph rewriting systems and string rewriting systems.

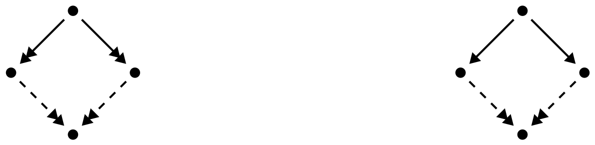


(a) Rewriting system peak.

(b) ARS peak.

Figure 1: A rewriting system peak and its corresponding ARS peak. (Note that a peak *is a single reduction step divergence.)*

One important transitional property is *confluence*. We define a *reduction sequence* to consist of zero or more consecutive reduction steps. A relation is confluent when all divergent reduction sequences can converge again in some way (see Figure 2a). Confluence is predominately of interest because it implies that every reducible term can be reduced to at most one irreducible term (or *normal form*). This means that every computation in a system generates at most one result: a desired property for most models of computation.



(a) Confluence.

(b) Local confluence.

Figure 2: Pictorial representations of confluence and local confluence. Solid lines denote universal quantification, while dashed lines denote existential quantification. Two-head arrows denote a reduction sequence, and single-head arrows denote a single reduction step.

There exists a great variety of methods for proving confluence. Some of these can be regarded as stronger variants of *local confluence*. A relation is locally confluent when all *single* reduction step divergences can converge again in some way (see Figure 2b). The methods under consideration are stronger for good reason, since local confluence does not imply confluence by itself (a "frustrating" fact in practice, according to De Bruijn [2] himself). Figure 3 proves this claim by means of a simple counterexample.

[1] *Transition*, *reduction* and *rewrite step* are synonymous notions.

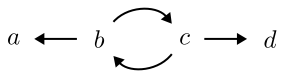


Figure 3: Local confluence does not imply confluence. Peaks $a \leftarrow b \rightarrow c$ and $b \leftarrow c \rightarrow d$ can be joined again in a and d, respectively. Thus the system is locally confluent. Should we diverge to the extremities a and d, however, then convergence is seen to be impossible. Thus the system is not confluent.

De Bruijn's weak diamond property[2] is one such method for proving confluence. It is a complete method for countable ARSs, but whether it is complete for uncountable ARSs is still open [3]. The weak diamond property is stronger than local confluence since it puts restrictions on how divergences may converge again. The property was first defined in one of De Bruijn's personal notes dating from 1978 [2]. He also included a proof of confluence in the same note. Curiously, he did not share it with the outside world until 1990, in a private correspondence with Klop [3].

Disregarding some minor adjustments, Endrullis and Klop [3] have for the first time published De Bruijn's original proof. They also show how to derive Van Oostrom's decreasing diagrams from De Bruijn's weak diamond property (the converse was already shown by Van Oostrom [7]). In addition, they provide a new and relatively short proof for the theorem that decreasing diagrams imply confluence.

For the present paper, the new decreasing diagrams proof of [3] was adapted to a proof for De Bruijn's weak diamond property.[3] The proof was then formalized using the interactive theorem prover Coq [4]. The formalization is publicly available at `http://www.few.vu.nl/~rok220/`. Whenever we refer to identifiers in the formalization, we typeset them in the `typewriter` font.

This appears to be the first formalization of the weak diamond property. Most closely related are formalizations of decreasing diagrams, of which only a few exist. Of these, Zankl's complete formalization in [8] is most notable, but it is implemented in Isabelle/HOL, not Coq. Bognar has written a decreasing diagrams formalization in Coq [1], but it concerns a non-standard variant of decreasing diagrams, in which the objects are labelled instead of the reductions. By contrast, our formalization should be adaptable to a formalization of the standard version of decreasing diagrams.

The structure of this paper is as follows. In Section 2 we present all of the preliminary notions. We then discuss a number of non-trivial lemmas in Section 3. The main theorem and its proof are presented in Section 4.

[2] Henceforth abbreviated as either *weak diamond property* or *WDP*.

[3] That such an adaptation is easy was already remarked by Endrullis and Klop in the same paper. They were not mistaken: the proof in this thesis closely follows theirs.

2 Preliminary notions

For the sake of completeness and to fix notations, we present the preliminary notions in this section.

2.1 Relations

Basic relations

Definition 1 (Reflexive closure)**.** The *reflexive closure* $R^=$ of a relation $R \subseteq A \times A$ is defined by the following inference rules:

$$\frac{xRy}{xR^=y}\ \text{(Step)} \qquad \frac{x \in A}{xR^=x}\ \text{(Reflexivity)}$$

Definition 2 (Reflexive transitive closure)**.** The *reflexive transitive closure* R^* of a relation $R \subseteq A \times A$ is inductively defined by the following inference rules:

$$\frac{xRy}{xR^*y}\ \text{(Step)} \qquad \frac{x \in A}{xR^*x}\ \text{(Reflexivity)} \qquad \frac{xR^*y \quad yR^*z}{xR^*z}\ \text{(Transitivity)}$$

Definition 3 (Converse)**.** The *converse* R^{-1} of a binary relation R is defined as $\{(y,x) \mid xRy\}$.

If $\rightarrow$ is used to denote a relation, then we write $\twoheadrightarrow$ instead of $\rightarrow^*$, and $\leftarrow$ instead of $\rightarrow^{-1}$. Furthermore, any induction on R^* will always be *structural induction* according to the inference rules in Definition 2.

Definition 4 (Relational composition)**.** Let $R \subseteq X \times Y$ and $S \subseteq Y \times Z$ be two relations. The *composition of R and S*, denoted $R \cdot S$, is defined as $\{(x,z) \mid (\exists y \in Y)(xRy \ \wedge \ ySz)\}$.

Definition 5 (Identity relation)**.** Let $id_A \subseteq A \times A$ denote the identity relation on A, i.e. $id_A := \{(a,a) \mid a \in A\}$.

Definition 6 (n-fold composition)**.** The *n-fold composition of* $R \subseteq A \times A$ (with $n \in \mathbb{N}$), denoted R^n, is defined inductively as:

- $R^0 := id_A$
- $R^{n+1} := R \cdot R^n$

Definition 7 (Labelled relations)**.** Let I be a set of *labels*, and $< \subseteq I \times I$ an order on I. For *labelled relations* $\rightarrow_i$ with $i \in I$ we define the following relations:

1. $\rightarrow := \bigcup \rightarrow_i$,
2. $\rightarrow_{<i} := \bigcup_{j<i} \rightarrow_j$,

3. $\rightarrow_{\leq i} := \bigcup_{j \leq i} \rightarrow_j$, and
4. $\rightsquigarrow_i := \twoheadrightarrow_{<i} \cdot \rightarrow_i^{=} \cdot \twoheadrightarrow_{<i}$.

The labelled relations described in Definition 7 are used to dictate how divergent reduction sequences must converge again.

Finally, we denote the union $\rightarrow_{<\alpha} \cup \rightarrow_{\leq\beta}$ by $\rightarrow_{<\alpha\cup\leq\beta}$.

Confluence

Definition 8 (Confluence)**.** A relation $\rightarrow \subseteq A \times A$ is *confluent* when $\twoheadleftarrow \cdot \twoheadrightarrow \subseteq \twoheadrightarrow \cdot \twoheadleftarrow$. Or stated in predicate logic, when:

$$(\forall a, b, c \in A)((c \twoheadleftarrow a \wedge a \twoheadrightarrow b) \Rightarrow (\exists d \in A)(c \twoheadrightarrow d \wedge d \twoheadleftarrow b))$$

Definition 9 (Local confluence)**.** A relation $\rightarrow \subseteq A \times A$ is *locally confluent* when $\leftarrow \cdot \rightarrow \subseteq \twoheadrightarrow \cdot \twoheadleftarrow$. Or stated in predicate logic, when:

$$(\forall a, b, c \in A)((c \leftarrow a \wedge a \rightarrow b) \Rightarrow (\exists d \in A)(c \twoheadrightarrow d \wedge d \twoheadleftarrow b))$$

A word on notation. Whenever we do not care to refer to variable names, we generally formulate sentences using the more concise set notation above instead of predicate logic. In addition, we sometimes employ the pictorial representation shown in Figure 2.

Relational properties such as (local) confluence are said to hold for an ARS $(A, \rightarrow)$ when those properties hold for $\rightarrow$. For readability, we sometimes abbreviate $(\twoheadleftarrow \cdot \twoheadrightarrow \subseteq \twoheadrightarrow \cdot \twoheadleftarrow)$ as $CR(\rightarrow)$ in formal sentences.

Well-foundedness

Definition 10 (Well-foundedness)**.** A relation $R \subseteq A \times A$ is well-founded if there exists an R-minimal element in every non-empty subset A' of A, or formally, when:

$$(\forall A' \subseteq A)[A' \neq \varnothing \Rightarrow (\exists a \in A')((\forall b \in A')(b, a) \notin R)]$$

Well-foundedness is generally of interest because it implies the *principle of well-founded induction* (Lemma 1).

Lemma 1 (Principle of well-founded induction)**.** *Let $P(x)$ denote that some property P holds for some $x \in S$. If $R \subseteq S \times S$ is well-founded, then*

$$[(\forall z \in S)[(\forall y \in S)(yRz \Rightarrow P(y))] \Rightarrow P(z)] \Rightarrow (\forall x \in S)P(x)$$

The proof for the main theorem in this paper makes appeal to this principle through repeated application of well-founded induction.

2.2 Abstract reduction systems

For completeness, we restate the definition of an ARS. In addition, we define the notion of a labelled ARS, which is a rather straightforward extension of an ARS: instead of one relation, there are multiple relations which are distinguished by the labels from some associated index set I.

Definition 11 (ARS)**.** An *ARS* is a tuple $(A, \to)$, with A a set of objects and $\to\ \subseteq A \times A$.

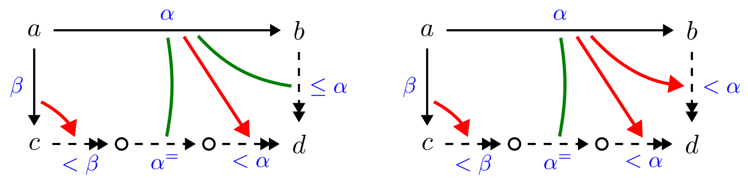
Definition 12 (Labelled ARS)**.** A *labelled ARS* is a tuple $(A, (\to_\alpha)_{\alpha \in I})$, with A a set of objects and $(\to_\alpha)_{\alpha \in I}$ a family of relations $\to_\alpha\ \subseteq A \times A$ labelled by $\alpha \in I$.

2.3 The weak diamond property

The expression 'weak diamond property' can refer to either the property itself or the theorem which states that the property implies confluence. We define the property below. The associated theorem and its proof are provided in Section 4.

Definition 13 (Weak diamond property)**.** Let $\mathcal{A} = (A, (\to_\alpha)_{\alpha \in I})$ be a labelled ARS with reduction relations indexed by a well-founded total order $(I, <)$.

We say that $\mathcal{A}$ satisfies the *weak diamond property* if every peak $c \leftarrow_\beta a \to_\alpha b$ with $\beta \leq \alpha$ can be joined according to one of the elementary diagrams in Figure 4.



$\alpha = \beta$ $\beta < \alpha$

Figure 4: De Bruijn's elementary diagrams. Note that the diagrams correspond to a case distinction on the total order $(I, <)$. The green and red lines indicate weak and strict decrease, respectively, and are only there to facilitate understanding.

3 Preliminary lemmas

In this section we prove a number of lemmas used in the main proof. Coq identifiers will be typeset in `typewriter` font. Some lemma statements are simpler than their Coq implementations (for example, when auxiliary conjuncts are included in Coq for reasons of convenience), but the essentials are captured. Relatively minor Coq lemmas are left unmentioned, unless we wish to make explicit reference to them. In that case we state them without proof.

In what follows, assume that we have some ARS $\mathcal{A} = (A, (\rightarrow_\alpha)_{\alpha \in I})$ indexed by a well-founded total order $(I, <)$. This assumption will also be granted by the main theorem.

Furthermore, assume without loss of generality that there exist bottom and top elements $\bot$ and $\top$ in I (respectively `bot_bot` and `top_top` in Coq), and that $\rightarrow_\bot = id_A$ (`bot_id`). These assumptions are also used in the main proof, but they are not granted by the theorem. We use these hypotheses to reduce the number of case distinctions in the main proof. The intuition behind their admissibility is that they do not influence the confluence property.

For completeness, we remark that there is one additional hypothesis in Coq, called `REcongr`. It is required because we use custom two-place predicates `E` and `L` to express respectively the equality and less-than relations over labels $i \in I$. `E` is an equivalence relation like $=$, but it does not imply congruence of labelled relations under label equality. Since we sometimes require such congruence, hypothesis `REcongr` states that $(\forall i, j \in I)(\texttt{E}ij \Rightarrow R_i = R_j)$.

We note that, for our purposes, we could have used $=$ instead of `E`. `E` was used, however, since the supervisors of this thesis already have a formalization of the theorem that the weak diamond property implies the decreasing diagrams property. This formalization switches from partial to total orders and introduces `E` as an equality predicate, and the predicate `L` as a well-founded order. Thus, using `L` and `E` here facilitates their own formalization task.

For readability, we will continue to write respectively $=$ and $<$ instead of `E` and `L` when comparing labels.

Finally, note that [3] also assumes that $\rightarrow_\top = id_A$, but this is redundant. In addition, they assume $id_A \subseteq \rightarrow_\alpha$ for all $\alpha \in I$, but we have eliminated the need for this assumption by incorporating reflexivity within all relevant diagram definitions.

3.1 Relations

The strip lemma (Lemma 2) can be used to relax the requirements for proving confluence of any binary relation $\rightarrow$.

Lemma 2 (`strip_lemma`)**.** *For any binary relation* $\rightarrow$*:*

$$(\twoheadleftarrow \cdot \rightarrow \;\subseteq\; \twoheadrightarrow \cdot \twoheadleftarrow) \;\Rightarrow\; CR(\rightarrow)$$

Proof. $\rightarrow$ is confluent when $\forall a, b, c[(a \twoheadrightarrow b \wedge a \twoheadrightarrow c) \Rightarrow \exists d(b \twoheadrightarrow d \wedge c \twoheadrightarrow d)]$. Thus we need to prove for arbitrary a, b that $\forall c[(a \twoheadrightarrow c) \Rightarrow \exists d(b \twoheadrightarrow d \wedge c \twoheadrightarrow d)]$ under assumption of:

(i) $(\twoheadleftarrow \cdot \rightarrow \;\subseteq\; \twoheadrightarrow \cdot \twoheadleftarrow)$, and

(ii) $a \twoheadrightarrow b$.

We proceed by induction on $a \twoheadrightarrow b$:

1. $a = b$: assume $a \twoheadrightarrow c$ for arbitrary c. Then $b \twoheadrightarrow c$ by both $a \twoheadrightarrow c$ and $a = b$, and $c \twoheadrightarrow c$ by reflexivity of $\twoheadrightarrow$.

2. $a \to b$: apply (i) with $a \twoheadrightarrow c$ for arbitrary c and $a \to b$.

3. $a \twoheadrightarrow b'$ and $b' \twoheadrightarrow b$ for some b': assume $a \twoheadrightarrow c$ for arbitrary c. Then $a \twoheadrightarrow b$ and $a \twoheadrightarrow c$ can be joined again according to the diagram below:

$$\begin{tikzcd}
a \arrow[r, two heads] \arrow[d, two heads] \arrow[dr, phantom, "\text{IH1}"] & b' \arrow[r, two heads] \arrow[d, dashed, two heads] \arrow[dr, phantom, "\text{IH2}"] & b \arrow[d, dashed, two heads] \\
\mathrm{c} \arrow[r, dashed, two heads] & \bullet \arrow[r, dashed, two heads] & \bullet
\end{tikzcd}$$

□

Lemma 3 (`refl_trans_monotone`). $R \subseteq S \Rightarrow R^* \subseteq S^*$.

Lemma 4 (`le_trans_eq_curly_trans`). $\twoheadrightarrow_{\leq i} = \rightsquigarrow_i^*$.

Proof. The $\subseteq$ and $\supseteq$ directions are considered in turn for arbitrary $i \in I$.

$\subseteq$: By Lemma 3 it suffices to prove $\to_{\leq i} \subseteq \rightsquigarrow_i$. Recall that $\rightsquigarrow_i = \twoheadrightarrow_{<i} \cdot \to_i^= \cdot \twoheadrightarrow_{<i}$.

By definition of $\to_{\leq i}$, there exists a j such that $\to_j$ with either $j < i$ or $j = i$. If $j < i$, then let the first $\twoheadrightarrow_{<i}$ component of $\rightsquigarrow_i$ be the single step $\to_j$, and the remaining components be reflexive. If $j = i$, then define both of the $\twoheadrightarrow_{<i}$ components to be reflexive. The middle component $\to_i$ follows from the congruence assumption.

$\supseteq$: Trivial. The key observation is that any sequence of $\rightsquigarrow_i$ steps is a sequence of $\to_{<i}$ and $\to_{\leq i}$ steps, which is obviously in $\twoheadrightarrow_{\leq i}$. □

Lemma 5 (`refl_trans_nfold`). $R^* = \{(a, b) \mid (\exists n \in \mathbb{N})(aR^n b)\}$.

Proof. The $\subseteq$ and $\supseteq$ directions are considered in turn.

$\subseteq$: Suppose aR^*b for some a, b. We perform induction on aR^*b. If aR^*b is reflexive, then we have aR^0b. If aR^*b is a single step, then we have aR^1b. If aR^*b because aR^*b' and $b'R^*b$ for some b', then by the induction hypotheses there exist $i, j \in \mathbb{N}$ such that aR^ib' and $b'R^jb$. Thus we have $aR^{i+j}b$.[4]

$\supseteq$: By induction on n. If $n = 0$, we have $a = b$ so that aR^*b follows by reflexivity of R^*. For the inductive step, assume we have $aR^{n+1}b$ for some $n > 0$. This is equivalent to $aRb'R^nb$ for some b'. aRb' implies aR^*b' by the step clause of R^*. $b'R^nb$ implies $b'R^*b$ by the induction hypothesis. Thus we obtain aR^*b by transitivity of R^*. □

From Lemmas 4 and 5 we obtain $\twoheadrightarrow_{\leq i} = \rightsquigarrow_i^* = \{(a, b) \mid (\exists n \in \mathbb{N})(a \rightsquigarrow_i^n b)\}$ for all $i \in I$, which allows us to freely convert between these notions. In this thesis we will often do so implicitly.

[4] Implementing this proof in Coq would be much harder, since i and j cannot simply be summed. For this reason, the proof in Coq makes use of an alternative definition for the reflexive transitive closure (Coq definition `refl_trans_close'`), which is equivalent to R^* (Coq lemma `samerel_refl_trans_close_refl_trans_close'`) and which in this case admits an easier formalization.

3.2 Diagrams

The two diagrams in this section will be used in the main proof.

Diagram $X(\alpha, \beta)$

Let $X(\alpha, \beta)$ be the diagram in Figure 5. It is slightly different from the definition in [3], since the single step reductions have been replaced by their reflexive closures.

This diagram is the centerpiece of the main proof, mostly due to Lemma 6 below.

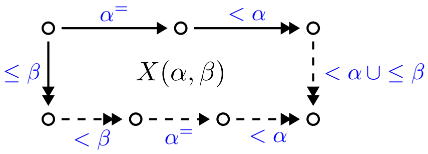


Figure 5: The diagram $X(\alpha, \beta)$, defined for $\alpha, \beta \in I$.

Lemma 6 (X_confluence)**.** $(\forall \alpha \in I)(X(\alpha, \alpha) \Rightarrow CR(\to_{\leq \alpha}))$.

Proof. Assume $X(\alpha, \alpha)$ for some α. By the strip lemma (Lemma 2), it suffices to prove $\twoheadleftarrow_{\leq \alpha} \cdot \to_{\leq \alpha} \subseteq \twoheadrightarrow_{\leq \alpha} \cdot \twoheadleftarrow_{\leq \alpha}$. Thus we may assume $c \twoheadleftarrow_{\leq \alpha} a \to_{\leq \alpha} b$ for arbitrary $a, b, c \in A$, and we need to show $\exists d(c \twoheadrightarrow_{\leq \alpha} d \twoheadleftarrow_{\leq \alpha} b)$. Since $\rightsquigarrow_\alpha \subseteq \twoheadrightarrow_{\leq \alpha}$ and $\twoheadleftarrow_{< \alpha \cup \leq \alpha} = \twoheadleftarrow_{\leq \alpha}$, it suffices to show $\exists d(c \rightsquigarrow_\alpha d \twoheadleftarrow_{< \alpha \cup \leq \alpha} b)$.

We proceed by case analysis on $a \to_{\leq \alpha} b$. If we have $a \to_\alpha b$, then we apply $X(\alpha, \alpha)$ with $c \twoheadleftarrow_{\leq \alpha} a$ for the left sequence and $a \to_\alpha b \twoheadrightarrow_{< \alpha} b$ for the top sequence. If we have $a \to_\beta b$ for some $\beta < \alpha$, then we apply $X(\alpha, \alpha)$ with $c \twoheadleftarrow_{\leq \alpha} a$ for the left sequence and $a \to_\alpha^= a \to_\beta b$ for the top sequence. In both cases $\exists d(c \rightsquigarrow_\alpha d \twoheadleftarrow_{< \alpha \cup \leq \alpha} b)$, as required. □

Diagram WDP$^=$

Let the *reflexive WDP* (WDP$^=$) the property denoted by the diagram in Figure 6. WDP$^=$ differs from WDP in that the diverging reduction steps have been replaced by their reflexive closures. In addition, the case distinction on $\beta \leq \alpha$ has been moved to the right converging reduction sequence. This simplifies proofs in Coq.

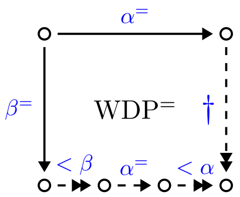


Figure 6: The reflexive weak diamond property. † *represents the annotation: "$\leq \alpha$, in addition, $< \alpha$ when $\beta < \alpha$".*

Lemma 7 (`wdp_refl`)**.** *If an ARS satisfies WDP, it also satisfies WDP$^=$.*

Proof. Assume $c \leftarrow_{\beta}^{=} a \rightarrow_{\alpha}^{=} b$ for arbitrary $a, b, c \in A$. We distinguish four cases:

1. Neither step is reflexive: we join in some d, whose existence is guaranteed by WDP. The bottom converging sequence can be straightforwardly derived from WDP in both the $\beta < \alpha$ and $\beta = \alpha$ cases. For the right converging sequence we still need to show that $(b \twoheadrightarrow_{\leq\alpha} d \wedge (\beta < \alpha \Rightarrow b \twoheadrightarrow_{<\alpha} d))$. If $\beta = \alpha$, then $b \twoheadrightarrow_{\leq\alpha} d$ follows from WDP, and the right conjunct is vacuously true. If $\beta < \alpha$, then $b \twoheadrightarrow_{<\alpha} d$ follows from WDP, and the left conjunct is obtained by virtue of the inclusion $\twoheadrightarrow_{<\alpha} \subseteq \twoheadrightarrow_{\leq\alpha}$.

2. Only $c \leftarrow_{\beta}^{=} a$ is reflexive: we join in b. Let the bottom sequence consist of only an α step towards b, and let its other two components as well as the right sequence be reflexive.

3. Only $a \rightarrow_{\alpha}^{=} b$ is reflexive: we join in c. Let every component in the bottom sequence be reflexive, and let the right sequence be a β step towards c.

4. Both steps are reflexive: we join in a. Let both converging sequences be entirely reflexive.

□

3.3 The §-lemmas

Here we formulate a number of conditional lemmas, named after their corresponding lemmas in [3]. Their conditions will be satisfied inside an inductive environment outlined in Section 4.

Lemma 8 ($\S_1$ / `SS1`)**.** *For all $\alpha \in I$, if $X(\gamma, \gamma)$ holds for all $\gamma < \alpha$, then the relation $\rightarrow_{\leq\beta}$ is confluent for all $\beta < \alpha$.*

Proof. Follows trivially from Lemma 6. □

Lemma 8 is used a total of four times in [3], and each time the goal is to derive $CR(\rightarrow_{<\beta})$ given $\beta \leq \alpha$ for some α and β. Even though it might be intuitively easy to see that these inferences are permitted, the reasoning behind it is not easily formalized. For this reason, we introduce the subtle variant $\S_1^<$ below (Lemma 11), which fits the intended applications better.

Lemma 9 (`lt_red_lt`)**.** *For all $\beta \in I$, and for all $a, b \in A$, if $a \twoheadrightarrow_{<\beta} b$, then either $\beta = \bot$ or there exists some $\gamma < \beta$ such that $a \twoheadrightarrow_{\leq\gamma} b$.*

Lemma 10 (`max_label`)**.** *For all $\beta, \delta, \gamma \in I$, and for all $a, b, c, d \in A$, if we have $\delta, \gamma < \beta$, $a \twoheadrightarrow_{\leq\delta} b$ and $c \twoheadrightarrow_{\leq\gamma} d$, then there exists some $\varepsilon < \beta$ such that $a \twoheadrightarrow_{\leq\varepsilon} b$ and $c \twoheadrightarrow_{\leq\varepsilon} d$.*

Lemma 11 ($\S_1^<$ / `SS1_lt`)**.** *For all $\alpha \in I$, if $X(\gamma, \gamma)$ holds for all $\gamma < \alpha$, then the relation $\rightarrow_{<\beta}$ is confluent for all $\beta \leq \alpha$.*

Proof. Let α be arbitrary and assume:

1. $X(\gamma, \gamma)$ holds for all $\gamma < \alpha$.
2. $c \twoheadleftarrow_{<\beta} a \twoheadrightarrow_{<\beta} b$ for arbitrary $a, b, c \in A$ and some arbitrary $\beta \leq \alpha$.

Our goal is to show $\exists d(c \twoheadrightarrow_{<\beta} d \twoheadleftarrow_{<\beta} b)$.

We use Lemma 9 twice, both for $c \twoheadleftarrow_{<\beta} a$ and for $a \twoheadrightarrow_{<\beta} b$. We have either $\beta = \bot$ or $\beta > \bot$. If $\beta = \bot$, then $\twoheadrightarrow_{<\beta}$ can only be reflexive (since $\bot$ is the smallest element), and confluence follows trivially.

If $\beta > \bot$, then Lemma 9 guarantees the existence of $\delta, \gamma < \beta$ such that $c \twoheadleftarrow_{\leq\gamma} a \twoheadrightarrow_{\leq\delta} b$. By Lemma 10 and the preceding, there exists some $\varepsilon < \beta$ such that $c \twoheadleftarrow_{\leq\varepsilon} a \twoheadrightarrow_{\leq\varepsilon} b$. Since we have assumption (1) and $\varepsilon < \beta \leq \alpha$, we can apply $\S_1$ (Lemma 8) to conclude confluence of $\rightarrow_{\leq\varepsilon}$, and derive $\exists d(c \twoheadrightarrow_{\leq\varepsilon} d \twoheadleftarrow_{\leq\varepsilon} b)$. Since $\varepsilon < \beta$, we have $\twoheadrightarrow_{\leq\varepsilon} \subseteq \twoheadrightarrow_{<\beta}$, allowing us to complete the proof by relaxing $\exists d(c \twoheadrightarrow_{\leq\varepsilon} d \twoheadleftarrow_{\leq\varepsilon} b)$ to $\exists d(c \twoheadrightarrow_{<\beta} d \twoheadleftarrow_{<\beta} b)$.

□

Lemma 12 ($\S_2$ / `SS2`)**.** *For all $\alpha, \beta \in I$ with $\beta \leq \alpha$, if $(\forall \delta \in I)(\delta < \alpha \Rightarrow X(\delta, \delta))$ and $(\forall \gamma \in I)(\gamma < \beta \Rightarrow X(\beta, \gamma))$, then for all $n \in \mathbb{N}$, we have $\twoheadleftarrow_{<\beta} \cdot \rightsquigarrow_\beta^n \subseteq \rightsquigarrow_\beta^n \cdot \twoheadleftarrow_{<\beta}$.*

Proof. By induction on n. The proof for the base case $n = 0$ is trivial: simply converge to wherever $\twoheadrightarrow_\beta$ diverges to. The proof for the induction step from n to $n + 1$ is provided in Figure 7 below. We follow [3] in the construction of the $n = 1$ diagram, and we then paste it to the diagram granted by the induction hypothesis. □

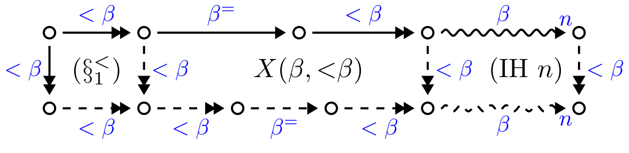


Figure 7: The diagram which proves claim $\S_2$ for the induction step.

We note that $X(\alpha, {<}\beta)$ is a notational shorthand for: “we apply $X(\alpha, \gamma)$ for some $\gamma < \beta$, after which we relax the γ labels to ${<}\beta$”. The corresponding reasoning in Coq is similar to that of the proof for Lemma 11.

4 Proof of the main theorem

We are now ready to state and prove the main theorem of this paper. For clarity, we provide a largely visual proof in Section 4.1, and we then map the proof to its formalization in Section 4.2.

4.1 The proof

Theorem 1 (Weak diamond property)**.** *Let $\mathcal{A} = (A, (\rightarrow_\alpha)_{\alpha \in I})$ be a labelled ARS with reduction relations indexed by a well-founded total order $(I, <)$.*

If $\mathcal{A}$ satisfies the weak diamond property, then $\mathcal{A}$ is confluent.

Proof. Apart from the hypotheses granted by the theorem statement, we repeat that we may assume without loss of generality that there exist bottom and top elements $\bot$ and $\top$ in I, and that $\rightarrow_\bot = id_A$. See the introduction to Section 3 for a discussion of these hypotheses.

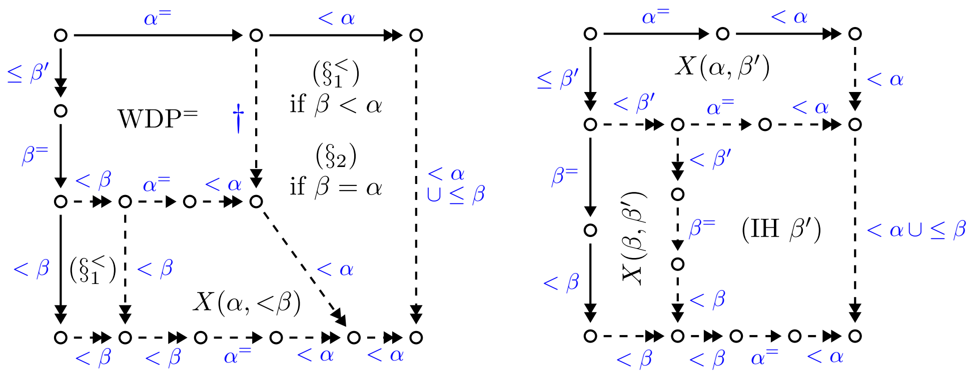
Since $\rightarrow_{\leq \top} = \rightarrow$, it suffices to prove $X(\top, \top)$ by Lemma 6. We obtain $X(\top, \top)$ by showing that $X(\alpha, \beta)$ holds for all α, β with $\beta \leq \alpha$. We use well-founded induction on α, directly followed by well-founded induction on β. We may thus assume $X(\alpha', \beta')$ for all $\beta' \leq \alpha'$ provided that either $\alpha' < \alpha$ or $(\alpha' = \alpha \wedge \beta' < \beta)$.[5]

One can verify that our induction hypotheses allow us to apply $\S_1^<$ (Lemma 11) and $\S_2$ (Lemma 12) in what follows.

Let $\sigma : \rightsquigarrow_\beta^n$ be the reduction sequence on the left of $X(\alpha, \beta)$ (this conversion is permitted by Lemma 5). We first prove $X(\alpha, \beta)$ with $\beta \leq \alpha$ for the $n = 1$ case. We then prove $X(\alpha, \beta)$ with $\beta \leq \alpha$ in general by induction on n.

For the case $n = 1$, we have that σ is of the form $\sigma : \twoheadrightarrow_{\leq \beta'} \cdot \rightarrow_\beta^= \cdot \twoheadrightarrow_{<\beta}$ with $\beta' < \beta$. We proceed by induction on β'. For the base case $\beta' = \bot$, we have that $\twoheadrightarrow_{\leq \beta'}$ is empty. Its proof is provided in the left diagram of Figure 8a. Figure 8b provides the proof for the $\beta' > \bot$ induction step.

[5] This is equivalent to well-founded induction on (α, β) in the lexicographical order with respect to $<$, so in this respect we do not diverge from the proof in [3].



(a) The $\beta' = \bot$ base case.

(b) The $\beta' > \bot$ induction step.

Figure 8: The $n = 1$ diagrams.

We now prove $X(\alpha, \beta)$ with $\beta \leq \alpha$ in general by induction on n. The base case $n = 0$ is trivial. The proof for the induction step from n to $n + 1$ is shown in Figure 9.

□

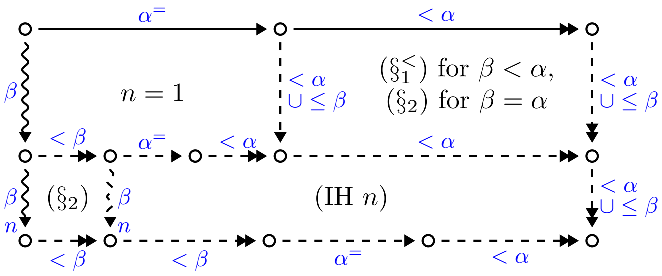


Figure 9: The n to $n + 1$ induction step diagram.

4.2 The formalization

Lemma 13 (`X_n_eq_1_beta'_eq_bottom`). *For all $\alpha, \beta \in I$, and for all $a, b, c \in A$, if:*

- $\beta \leq \alpha$,
- $(\forall \alpha' < \alpha)\ X(\alpha', \alpha')$,
- $(\forall \alpha' < \beta)\ X(\alpha, \alpha')$,
- $(\forall \gamma < \beta)\ X(\beta, \gamma)$,

- *$a(\to_{\alpha}^{=} \cdot \twoheadrightarrow_{<\alpha})b$, and*
- *$a(\to_{\beta}^{=} \cdot \twoheadrightarrow_{<\beta})c$,*

then there exists some $d \in A$ such that:

- *$b \twoheadrightarrow_{<\alpha \cup \leq\beta} d$, and*
- *$c(\twoheadrightarrow_{<\beta} \cdot \to_{\alpha}^{=} \cdot \twoheadrightarrow_{<\alpha})d$.*

Lemma 13 and its Coq proof correpond to the $\beta = \bot$ base case diagram in Figure 8a. Note that the formalization omits any mention of β': since $\beta' = \bot$, the $\twoheadrightarrow_{\beta'}$ reduction on the left of Figure 8a will be reflexive and irrelevant for inferring the conclusion.

Definition 14 (`X_n_eq_1_dia`)**.** For $\alpha, \beta, \beta' \in I$, `X_n_eq_1_dia`$(\alpha, \beta, \beta')$ is defined as the diagram in Figure 10.

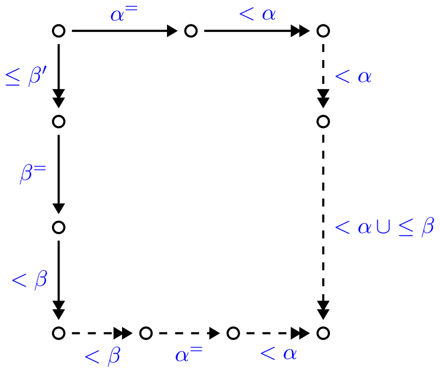


Figure 10: The `X_n_eq_1_dia` *diagram.*

Lemma 14 (`X_n_eq_1`)**.** *For all $\alpha, \beta, \beta' \in I$, and for all $a, b, c \in A$, if:*

- *$\beta \leq \alpha$,*
- *$\beta' < \beta$,*
- *$(\forall \alpha' < \alpha)\ X(\alpha', \alpha')$,*
- *$(\forall \alpha' < \beta)\ X(\alpha, \alpha')$,*
- *$(\forall \gamma < \beta)\ X(\beta, \gamma)$, and*
- *$(\forall \delta < \beta')$ `X_n_eq_1_dia`(α, β, δ),*

then `X_n_eq_1_dia`(α, β, β').

Lemma 14 and its Coq proof correspond to the *entire* $n = 1$ case of Figure 8. In the proof, the $\beta' = \bot$ case is dealt with by application of Lemma 13. Next, the $\beta' > \bot$ case is proven by a formalization of Figure 8b.

Definition 15 (`X_n_eq_1_dia`)**.** For $\alpha, \beta \in I$ and $n \in \mathbb{N}$, `X_ind_step_dia`(α, β, n) is defined as the diagram in Figure 11.

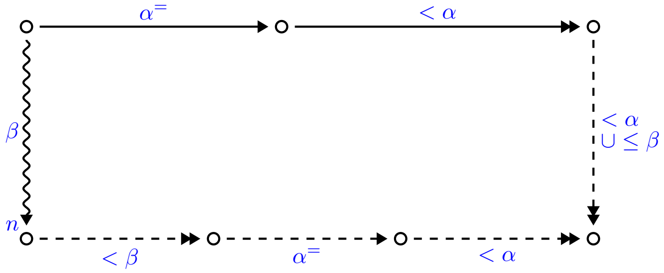


Figure 11: The `X_ind_step_dia` *diagram.*

Lemma 15 (`X_ind_step`)**.** *For all $\alpha, \beta \in I$, and for all $n \in \mathbb{N}$, if*

- $\beta \leq \alpha$,
- $(\forall \alpha' < \alpha)\ X(\alpha', \alpha')$,
- $(\forall \alpha' < \beta)\ X(\alpha, \alpha')$,
- $(\forall \gamma < \beta)\ X(\beta, \gamma)$,
- $(\forall \beta' < \beta)$ `X_n_eq_1_dia`(α, β, β'), *and*
- $n > 0 \Rightarrow$ `X_ind_step_dia`$(\alpha, \beta, n - 1)$,

then `X_ind_step_dia`(α, β, n)*.*

Lemma 15 and its Coq proof correspond to the diagram in Figure 9.

Lemma 16 (`X_inh`)**.** *For all $\alpha, \beta \in I$ with $\beta \leq \alpha$, we have that $X(\alpha, \beta)$.*

In the Coq proof for Lemma 16, well-founded induction on α is followed by well-founded induction on β. Thus, as already outlined in Section 4.1, we have $X(\alpha', \beta')$ for all $\beta' \leq \alpha'$ provided that either $\alpha' < \alpha$ or $(\alpha' = \alpha \wedge \beta' < \beta)$. From these are then derived:

- $(\forall \alpha' < \alpha)\ X(\alpha', \alpha')$,
- $(\forall \alpha' < \beta)\ X(\alpha, \alpha')$, and
- $(\forall \gamma < \beta)\ X(\beta, \gamma)$,

which are required hypotheses for any applications of Lemmas 13 and 14. After this, $(\forall \beta' < \beta)$ `X_n_eq_1_dia`(α, β, β') is proven by induction on β' and application of Lemma 14. Subsequently, the induction step diagram is proven (for all n) by induction on n, applying Lemma 15 with the preceding results.

Lemma 17 (`X_top`). *$X(\top, \top) \Rightarrow CR(\to)$.*

Lemma 18 (`weak_diamond_property_implies_confluence`). *$CR(\to)$.*

Lemma 18 follows straightforwardly from Lemmas 16 and 17, and concludes the Coq formalization.

5 Conclusion

We have completely formalized the theorem that the weak diamond property implies confluence in Coq. The formalization is based on Endrullis and Klop's [3] paper proof for the theorem that decreasing diagrams imply confluence. The formalization uses four hypotheses which could in principle still be eliminated. One of these hypotheses is used so that the formalization is more easily adapted to a formalization for the confluence of decreasing diagrams.

Acknowledgements

I thank Jörg Endrullis and Dimitri Hendriks for their helpful and enthusiastic supervision. In addition, I would like to thank Jörg Endrullis and Jan Willem Klop for granting access to the Ti*k*Z source code of their nice diagrams in [3].

References

[1] M. Bognar. A point version of decreasing diagrams. In *Proceedings Accolade 1996. Dutch Graduate School in Logic*, pages 1–14, 1997. The formalization is available at: `http://web.archive.org/web/20051226052550/http://www.cs.vu.nl/~mirna/`.

[2] N. G. de Bruijn. A note on weak diamond properties. *Memorandum 78-08*, 1978. Available at: `http://www.win.tue.nl/automath/archive/pdf/aut057.pdf`.

[3] J. Endrullis and J. W. Klop. De Bruijn's weak diamond property revisited. *Indigationes Mathematicae*, 24:1050–1072, 2013.

[4] The Coq development team. *The Coq proof assistant reference manual.* LogiCal Project, 2004. Version 8.0. `http://coq.inria.fr`.

[5] R. Overbeek. Coq script used to formalize De Bruijn's weak diamond property, 2015. Available at: `http://www.few.vu.nl/~rok220/`.

[6] Terese. *Term rewriting systems.* Cambridge University Press, 2003.

[7] V. van Oostrom. Confluence by decreasing diagrams. *Theoretical Computer Science*, 126:259–280, 1994.

[8] H. Zankl. Confluence by decreasing diagrams – formalized. In F. van Raamsdonk, editor, *Proceedings of the 24th International Conference on Rewriting Techniques and Applications*, volume 21 of *Leibniz International Proceedings in Informatics*, pages 352–367, 2013.