Automating the Diagram Method to Prove Correctness of Program Transformations

David Sabel
Automating the Diagram Method to Prove Correctness of Program Transformations

David Sabel
Goethe-University
Frankfurt am Main, Germany
sabel@ki.cs.uni-frankfurt.de *

Our recently developed LRSX Tool implements a technique to automatically prove the correctness of program transformations in higher-order program calculi which may permit recursive let-bindings as they occur in functional programming languages. A program transformation is correct if it preserves the observational semantics of programs- In our tool the so-called diagram method is automated by combining unification, matching, and reasoning on alpha-renamings on the higher-order meta-language, and automating induction proofs via an encoding into termination problems of term rewrite systems. We explain the techniques, we illustrate the usage of the tool, and we report on experiments.

1 Introduction

Program transformations replace program fragments by program fragments. They are applied as optimizations in compilers, in code refactoring to increase maintainability of the source code, and in verification for equational reasoning on programs. In all cases correctness of the transformations is an indispensable requirement. We focus on program calculi with a small-step operational semantics (in form of a reduction semantics with evaluation contexts, see e.g. [21]) and a notion of successfully evaluated programs. Convergence of programs holds, if the program can be evaluated to a successful program. As program equivalence we use contextual equivalence [9, 10], which holds for program fragments P_1 and P_2 if interchanging P_1 by P_2 in any program (i.e. context) is not observable w.r.t. convergence. We are particularly interested in extended lambda-calculi with call-by-need evaluation modeling the (untyped) core languages of lazy functional programming languages like Haskell (see [3, 2, 18]).

The LRSX Tool supports correctness proofs of program transformations in those calculi by automating the so-called diagram method (see e.g. [18, 14] and also [8, 20]) which was used in earlier work in non-automated pen-and-paper proofs. The diagram method is a syntactic approach that can roughly be outlined as follows: First all overlaps between standard reduction steps and transformation steps are computed, then the overlaps have to be joined resulting in a complete set of diagrams. This step is related to computing and joining critical pairs in term rewrite systems (see e.g. [4]), however, with two rewrite relations and where for one rewrite relation a strategy (defined by the standard reduction) has to be respected. Finally, the diagrams are used in an inductive proof to show correctness of the transformation.

The automation of the method is schematically depicted in Fig. 1. The input consists of a calculus description and a set of program transformations. First the diagram calculator computes the overlaps and then tries to join them. If a complete set of diagrams is obtained, it is translated into a term rewrite system (where the diagrams are represented in an abstract manner, i.e. only the names and directions of

*This research is supported by the Deutsche Forschungsgemeinschaft (DFG) under grant SA2908/3-1

available from [http://goethe.link/LRSXTOOL61](http://goethe.link/LRSXTOOL61)
the reduction and transformation steps are kept, but all information on the meta-expressions is removed) such that termination of the system implies correctness of the program transformations. The automated termination prover AProVE \cite{1,7} and the certifier CeTA \cite{5,19} are used to automate these steps. We will explain core components of the automated method and illustrate the use of the LRSX Tool.

As a running example, we use the call-by-need lambda calculus with letrec \( L_{\text{need}} \) \cite{17}. Its syntax, small-step operational semantics (called standard reduction), and the program transformations (gc1) and (gc2) to perform garbage collection, and transformations (cp-in) and (cp-e) to copy abstractions, are shown in Fig. 2. Standard reduction implements the lazy evaluation strategy with sharing by applying small-step reduction rules at needed positions, which are determined by application contexts, reduction contexts, and chains of letrec-bindings that occur as variable-to-variable bindings and also as chains \( \{w_i = A[w_{i+1}]\}_{i=1}^m \). Reduction is meant modulo (extended) \( \alpha \)-renaming, i.e. \( \alpha \)-equivalent expressions where letrec-bindings are treated like a set are not distinguished.

Outline. In Sect. 2 we explain the meta language and the input for the diagram method. In Sect. 3 we describe the automated correctness proof for the standard cases, and in Sect. 4 we discuss extensions which are also built in the tool. In Sect. 5 we report on some experiments and we conclude in Sect. 6.

2 Program Calculi and Transformations

The input of the diagram technique is a program calculus – consisting of definitions of contexts, standard reduction rules, answers representing successfully evaluated programs – and a set of program transformations. Rules and answers are expressed in the meta-language LRSX (see also \cite{16}). This meta-language is parametrized over a set \( \mathcal{F} \) of function symbols and a finite set \( \mathcal{K} \) of context classes \( 2 \). The syntax of LRSX-expressions \( \text{Exp} = \text{HExp}^0 \), a countably-infinite set of variables \( \text{Var} \), higher-order expressions of order \( n \) \( \text{HExp}^n \), environments \( \text{Env} \), and bindings \( \text{Bind} \) is defined by the grammar

\[
x, y, z \in \text{Var} ::= X | x
\]
\[
s, t \in \text{HExp}^0 ::= S | D[s] | \text{letrec env in s} \mid f r_1 \ldots r_{\text{ar}(f)} \quad \text{such that } r_i \in \tau_i \text{ if } f : \tau_1 \rightarrow \ldots \rightarrow \tau_n \rightarrow \text{Exp}
\]
\[
s \in \text{HExp}^n ::= x.s_1 \quad \text{if } s_1 \in \text{HExp}^{n-1} \text{ and } n \geq 1
\]
\[
b \in \text{Bind} ::= x = s \quad \text{where } s \in \text{HExp}^0
\]
\[
env \in \text{Env} ::= \emptyset | E ; \text{env} | Ch[x,s] ; \text{env} | b ; \text{env}
\]

Every \( f \in \mathcal{F} \) has a syntactic type of the form \( \tau_1 \rightarrow \ldots \rightarrow \tau_{\text{ar}(f)} \rightarrow \text{Exp} \), where \( \tau_i \) may be \( \text{Var} \), or \( \text{HExp}^k \). We assume \( \{\text{var}, \lambda \} \subseteq \mathcal{F} \) where \( \text{var} \) of type \( \text{Var} \rightarrow \text{Exp} \) lifts variables to expressions, and \( \lambda \) has type \( \text{HExp}^1 \rightarrow \text{Exp} \). To distinguish term variables, meta-variables, and meta-symbols, we use different fonts and lower- or upper-case letters: concrete term-variables of type \( \text{Var} \) are denoted by \( x \),

\[\text{In the LRSX-Tool the set } \mathcal{K} \text{ has to be defined explicitly while the set } \mathcal{F} \text{ is extracted from the used symbols in the input.}\]
Expressions e and environments Env where v,v₁,w,w₁ are variables,\n\[ e ::= w | \lambda w.e | (e₁ e₂) | \text{letrec}\ e\text{ in } e \text{ where Env } \neq \emptyset \quad \text{Env} ::= \emptyset | w₁=e₁,\ldots,wₙ=eₙ \]

Application contexts A and reduction contexts R\n\[ A ::= [] | (A e) \quad R ::= A | \text{letrec}\ \text{Env}\ \text{in}\ A | \text{letrec}\ \{wᵢ=Aᵢ[wᵢ₊₁]\}^{m-1}_{i=1},w_m=A_m,\text{Env}\ \text{in}\ A₀[w₁] \]

Standard reduction \(\Rightarrow_S\), \(\Rightarrow_L\)\n\[ (sr,\text{beta})\ R[\lambda w.e]\ e₁) \rightarrow R[\text{letrec}\ w \rightarrow e₂ \text{ in } e₁] \]
\[ (sr,\text{app})\ R[\text{letrec}\ \text{Env}\ \text{in } e₁) \rightarrow R[\text{letrec}\ \text{Env}\ \text{in } (e₁ e₂)] \]
\[ (sr,\text{exp-in})\ \text{letrec}\ \{wᵢ=Aᵢ[wᵢ₊₁]\}^{m-1}_{i=1},w_m=\lambda w.e,\text{Env}\ \text{in}\ A₀[w₁] \rightarrow \text{letrec}\ \{wᵢ=Aᵢ[wᵢ₊₁]\}^{m-1}_{i=1},w_m=\lambda w.e,\text{Env}\ \text{in}\ A[w₁] \]
\[ (sr,\text{exp-e})\ \text{letrec}\ \{wᵢ=Aᵢ[wᵢ₊₁]\}^{m-1}_{i=1},w_m=\lambda w.e,\text{Env}\ \text{in}\ A[w₁] \rightarrow \text{letrec}\ \{wᵢ=Aᵢ[wᵢ₊₁]\}^{m-1}_{i=1},w_m=\lambda w.e,\text{Env}\ \text{in}\ A[w₁] \]

Garbage Collection \(\text{gc}\)\n\[ \text{letrec}\ w₁=e₁,\ldots,wₙ=eₙ,\text{Env}\ \text{in } e \rightarrow \text{letrec}\ \text{Env}\ \text{in } e, \text{ if for all } i : wᵢ \text{ does not occur in Env, } e \]
\[ \text{letrec}\ w₁=e₁,\ldots,wₙ=eₙ \in e \rightarrow e, \text{ if for all } i : wᵢ \text{ does not occur in } e \]

Copy Transformation \(\text{cp}\)\n\[ \text{letrec}\ w=\lambda v.e,\text{Env}\ \text{in } C[w] \rightarrow \text{letrec}\ w=\lambda v.e,\text{Env}\ \text{in } C[\lambda v.e] \]
\[ \text{letrec}\ w₁=\lambda v.e,w₂=C[w₁],\text{Env}\ \text{in } e' \rightarrow \text{letrec}\ w₁=\lambda v.e,w₂=C[\lambda v.e],\text{Env}\ \text{in } e' \]

Figure 2: The calculus \(L_{need}\): Weak head normal forms (WHNFs) are \(\lambda w.e\) or \(\text{letrec}\ \text{Env}\ \text{in } \lambda w.e\)

y, and x,y are used as meta-symbols to denote a concrete term variable or a meta-variable. Similarly, s,t denote expressions, env denotes environments, and b denotes bindings. Meta-variables are written in upper-case letters, where \(X, Y\) are of type Var, \(S\) is of type Exp, \(E\) is of type Env, \(D\) is a context variable, and Ch is a two-hole environment-context variable (chain variable, for short) that occurs with a Var-argument x, and an Exp-argument s. Each context variable D has a class \(cl(D)\) and each Ch-variable has a class \(cl(Ch)\). An LRSX-expression s is ground (written as s) iff it does not contain any meta-variable.

Example 2.1. The syntax of the \(\lambda\)-calculus (and also of our running example \(L_{need}\)) can be expressed in LRSX, by the function symbols var, \(\lambda\), and app where app is a binary function symbol of type Exp \(\rightarrow\) Exp \(\rightarrow\) Exp. The application of the identity function to itself can be written as the LRSX-expression \(\text{app}\ (\lambda (x.\text{var}\ x)) (\lambda (x.\text{var}\ x))\). Lists can be represented by function symbols \(\text{nil}\ ::\ \text{Exp}\) and \(\text{cons}\ ::\ \text{Exp}\ \rightarrow\ \text{Exp}\ \rightarrow\ \text{Exp}\). A case-expression – usually written as case \(C\ of\ \{Nil \rightarrow e₁\} (\text{Cons}\ x\ xs \rightarrow e₂)\ – to deconstruct lists can be represented as case list \(l\ e₁ \times xs\) \(e₂\) where case list is a function symbol of type Exp \(\rightarrow\) Exp \(\rightarrow\ \text{HExp}^2\ \rightarrow\ \text{Exp}\).

Contexts are expressions, where the hole \([\cdot]\) occurs instead of one subexpression. With d we denote a ground context and \(d\) denotes LRSX-contexts, i.e. contexts, that may contain meta-variables. Filling the hole of \(d\) with \(s\) is written as \(d[s]\). Multi-contexts with \(k\) holes are written with several hole symbols \([\cdot]_1,\ldots,[\cdot]_k\). A context class \(\mathcal{K} \in \mathcal{K}\) is a set of contexts which is defined by a context free grammar describing the syntax of contexts and by a prefix and a forking table, which are used in the matching and unification algorithms to proceed with equations of the form \(D₁[s₁] \doteq D₂[s₂]\): The prefix table is a partial function that maps pairs of classes \((\mathcal{K}_1, \mathcal{K}_2)\) to a pair of classes \((\mathcal{K}_3, \mathcal{K}_4)\) such that for context variables
define A ::= [.] | (app A S)
define T ::= [.] | (app T S) | (app S T) | letrec X=T;E in S | letrec E in T where E /= {}
declare prefix A A = (A,A)
declare prefix A T = (A,T)
declare prefix T A = (A,A)
declare prefix T T = (T,T)
declare fork A T = (A,A,T,(app [.1] [.2]))
declare fork T T = (T,T,T,(app [.1] [.2]))
declare fork T T = (T,T,T,(app [.2] [.1]))
declare fork T T = (T,T,T,(app [.2] [.1]))
declare fork T T = (T,T,T,(letrec X=[.1];Y=[.2];E in S))
declare fork T T = (T,T,T,(letrec X=[.2];Y=[.2];E in S))
declare fork T A = (A,T,A,(app [.2] [.1]))

declare fork T T = (T,T,(letrec X=[.1];E in S))
declare fork T T = (T,T,(letrec X=[.2];Y=[.2];E in S))
declare fork T T = (T,T,(letrec X=[.1];Y=[.2];E in S))
declare fork T T = (T,T,(letrec X=[.1];E in [.2]))
declare fork T T = (T,T,(letrec X=[.2];E in [.1]))
declare fork T T = (T,T,(letrec X=[.1];E in S))
declare fork T T = (T,T,(letrec X=[.2];E in S))
declare fork T T = (T,T,(app [.2] [.1]))
declare fork T T = (T,T,(app [.1] [.2]))
declare fork T T = (T,T,(app [.2] [.1]))
declare fork T T = (T,T,(app [.1] [.2]))
declare fork T T = (T,T,(app [.1] [.2]))
declare fork T T = (T,T,(app [.2] [.1]))
declare fork T T = (T,T,(app [.1] [.2]))

define T ::= [.] | (app T S) | (app S T) | letrec X=T;E in S | letrec E in T where E /= {}
define A ::= [.] | (app A S)

Figure 3: Definition of application and top-contexts as input for the LRSX Tool

$D_i$ with $cl(D_i) = \mathcal{K}_i$ an equation $D_1[s] \doteq D_2[r]$ where $D_1$ is a prefix of context $D_2$, can be replaced by the equation $s \doteq D_4[r]$ and the substitution $\{D_1 \mapsto D_3, D_2 \mapsto D_3[D_4]\}$. Undefined cases express that the prefix situation is impossible. The forking table is a partial function that maps pairs of classes $(\mathcal{K}_1, \mathcal{K}_2)$ to a set of tuples of the form $(\mathcal{K}_3, \mathcal{K}_4, \mathcal{K}_5, d[.1][.2])$ such that for context variables $D_i$ of class $\mathcal{K}_i$ an equation $D_1[s] \doteq D_2[r]$ where the paths to the holes of $D_1$ and $D_2$ fork, the equation can be removed by guessing one tuple in the set and substituting $D_1 \mapsto D_3[d[D_4[.1], D_5[.2]]], D_2 \mapsto D_3[d[D_4[.1], D_5[.2]]]$.

For calculus $L_{\text{need}}$, it suffices to define classes for application contexts $A$, top contexts $T$ and arbitrary contexts $C$. The definition of the former two classes as input for the LRSX Tool is shown in Fig. 3. We illustrate some exemplary entries of the prefix and forking table: The prefix table maps $(A,T)$ to $(A,T)$, since for every application context $D_1$ that is a prefix of a top-context $D_2$, we can substitute $D_1 \mapsto D_3$ and $D_2 \mapsto D_3[D_4]$ where $D_3$ must be an application context (since $D_1$ is one) and $D_4$ must be a top context (since $D_2$ is one). The prefix table maps $(T,A)$ to $(A,A)$, since for every top-context $D_1$ that is a prefix of an application context $D_2$, we can substitute $D_1 \mapsto D_3$ and $D_2 \mapsto D_3[D_4]$ where $D_3$ and $D_4$ must be application contexts to ensure that $D_2$ is an application context. The forking table for $(A,T)$ has only one entry $(A,A,T, \text{app } [.1][.2])$, since an application context $D_1$ and a top context $D_2$ can only have different hole paths, if there is an application where the hole path of $D_1$ goes through the first argument, while the hole path of $D_2$ goes through the second argument, the expression above this application must belong to application contexts (to ensure that $D_1$ is an application context) the context inside the first argument of the application must be an application context (again to ensure that $D_1$ is an application context), and the context inside the second argument must be a top context (to ensure that $D_2$ is a top context). For $(T,T)$ there are more entries, since the forking of two top-contexts may happen in an application or in a letrec-expression: There are two cases for the application depending on whether the hole path of the first context goes through the first or the second argument, and there are three cases for letrec: the hole path of the first context may go through the in-expression while the other goes through the letrec-environment, or vice versa, or both hole paths go through the environment, but through different bindings. In any case the context above the two parallel holes is a top-context and the contexts below must both be top-contexts.

The semantics of meta-variables is straightforward except for chain-variables: $Ch[x,s]$ with $cl(Ch) = \mathcal{K}$ stands for $x.d[s]$ or chains $x.d_1[(\text{var } x_1)]; x_1.d_2[(\text{var } x_2)]; \ldots; x_n.d_n[e]$ with fresh $x_i$ and contexts $d, d_i$ of class $\mathcal{K}$. For expression $e$, $MV(e)$ denotes the meta-variables of $e$, $FV(e)$ denotes the free variables, $BV(e)$ denotes the bound variables, and $\text{Var}(e) := FV(e) \cup BV(e)$. For a ground context $d$, $CV(d)$ (the captured variables) is the set of variables $x$ which become bound if plugged into the hole of $d$. For
environment \textit{env}, \textit{LV(env)} are the let-bound variables in \textit{env}. Let \(\sim_{let}\) be the reflexive-transitive closure of permuting bindings in a \texttt{letrec}\textendash environment, and \(\sim_{\alpha}\) be the reflexive-transitive closure of combining \(\sim_{let}\) and \(\alpha\)-equivalence. An LRSX-expression \(s\) satisfies the \textit{let variable convention (LVC)} iff a let-bound variable does not occur twice as a binder in the same \texttt{letrec}\textendash environment; and \(s\) satisfies the \textit{distinct variable convention (DVC)} iff \(BV(s)\) and \(FV(s)\) are disjoint and all binders bind different variables.

A \textit{constrained expression} \((s, \Delta)\) consists of an LRSX-expression \(s\) and a \textit{constraint tuple} \(\Delta = (\Delta_1, \Delta_2, \Delta_3)\) such that \(\Delta_1\) is a finite set of context variables, called \textit{non-empty context constraints}; \(\Delta_2\) is a finite set of environment variables, called \textit{non-empty environment constraints}; and \(\Delta_3\) is a finite set of pairs \((t, d)\) where \(t\) is an LRSX-expression and \(d\) is an LRSX-context, called \textit{non-capture constraints (NCCs)}. A ground substitution \(\rho\) satisfies \(\Delta\) iff \(\rho(D) \neq [\cdot]\) for all \(D \in \Delta_1\); \(\rho(E) \neq \emptyset\) for all \(E \in \Delta_2\); and \(\text{Var}(\rho(t)) \cap \text{CV}(\rho(d)) = \emptyset\) for all \((t, d) \in \Delta_3\). The \textit{concretizations} of \((s, \Delta)\) are \(\gamma(s, \Delta) := \{\rho(s) \mid \rho\) is a ground substitution, \(\rho(s)\) fulfills the LVC, \(\rho\) satisfies \(\Delta\}\).

\textbf{Definition 2.2.} For \(\ell, r \in \text{Exp}\), a constraint tuple \(\Delta, \kappa \in \{\text{SR}, \text{T}\}\), a name \(n\), \(\ell \xrightarrow{\kappa n} \Delta r\) is called a \textit{letrec rewrite rule}, provided that \(MV(\Delta) \subseteq MV(\ell) \cup MV(r)\) and in each of the expressions \(\ell\) and \(r\), every variable of type \(S\) occurs at most twice; every variable of kind \(E, Ch, D\) occurs at most once; if \(\kappa = \text{SR}\), then \(Ch\)-variables occurring in \(\ell\) must occur in one \texttt{letrec}\textendash environment only; for any ground substitution \(\rho\) that satisfies \(\Delta\), \(\rho(\ell)\) fulfills the LVC iff \(\rho(r)\) fulfills the LVC. A letrec rewrite rule represents the set of ground rewrite rules \(\gamma(\ell \xrightarrow{\kappa n} \Delta r) := \left\{ \rho(\ell) \rightarrow \rho(r) \mid \rho\) is a ground substitution for \(\ell, r,\right.\) the LVC holds for \(\rho(\ell), \rho(r)\), \(\rho\) satisfies \(\Delta\} \) . For a set \(\{\ell \xrightarrow{\kappa n_i} \Delta r \mid i = 1, \ldots, m\}\) of letrec rewrite rules, we write \(s \xrightarrow{\kappa n_i} t\) if \((s \rightarrow t) \in \gamma(\ell \xrightarrow{\kappa n_i} \Delta r)\) and \(s \xrightarrow{\kappa} t\) if \(s \xrightarrow{\kappa n_i} t\) for some \(1 \leq i \leq m\). We write \(s \xrightarrow{\kappa n_i} s'\) if there exists \(s''\) such that \(s \sim_{\alpha} s'' \xrightarrow{\kappa n_i} s'\).

Standard reductions are letrec rewrite rules that are always applicable to expressions which fulfill the DVC, and answers represent successful programs:

\textbf{Definition 2.3.} A letrec rewrite rule \(\ell \xrightarrow{\kappa n} \Delta r\) is a \textit{standard reduction} if \(\kappa = \text{SR}\) and: If for ground expressions \(s_1, s_2\) with \(s_1 \xrightarrow{\text{SR}, n} s_2 \in \gamma(\ell \xrightarrow{\kappa n} \Delta r)\), then for all ground expressions \(t_1\), such that \(s_1 \sim_{\alpha} t_1\) and \(t_1\) fulfills the DVC, there exists \(t_2 \sim_{\alpha} s_2\), such that \(t_1 \xrightarrow{\text{SR}, n} t_2 \in \gamma(\ell \xrightarrow{\kappa n} \Delta r)\). An \textit{answer set} \(\text{Ans}\) is a finite set of constrained expressions \((t, \Delta)\) such that if \(s \in \gamma(t, \Delta)\), then for all \(s' \sim_{\alpha} s\) such that \(s'\) fulfills the DVC we have \(s' \in \gamma(t, \Delta)\). If \(s \in \gamma(t, \Delta)\) for some \((t, \Delta) \in \text{Ans}\) and \(s' \sim_{\alpha} s\), then \(s'\) is called an \textit{answer}. A \textit{program calculus} is a pair \((\text{SR}, \text{Ans})\), a finite set of standard reductions \(\text{SR}\) and an answer set \(\text{Ans}\), such that whenever \(s \xrightarrow{\text{SR}, n} s'\) and \(s\) is an answer, then also \(s'\) is answer.

In the LRSX Tool, standard reduction \(\ell \xrightarrow{\text{SR}, n} \Delta r\) is written \(\{\text{SR}, n, k\} \ell => r\) where Constraints such that \(k\) is a number (the variant of the rule\footnote{In the LRSX Tool constrained expressions are written as “\textit{e where Constraints}” such that Constraints is a list of constraints, where non-empty context constraints are written as \(D \neq \{\cdot\}\), non-empty environment constraints are written as \(E \neq \{\cdot\}\), and non-capture constraints can occur as \((s, d)\), but also as \([\text{env}, d]\) representing the NCC \(\text{letrec env in c, d}\) for some constant \(c\).} \) and Constraints are the constraints in \(\Delta\) written as in constrained expressions. Answers are defined in the LRSX Tool by “\textit{Answer e where Constraints}.”

For the calculus \(L_{need}\), standard reductions on usual reductions hold. An excerpt of the description of \(L_{need}\) as input of the LRSX Tool is in Fig.\footnote{In short representation of rule names, the LRSX Tool unions all variants of a rule of the same name. 4} where several rule variants are used for the different cases of a reduction context and side conditions of the rules (see Fig.\footnote{4} 2) are expressed by constraints. For instance, rule \((\text{SR}, \text{1beta})\) is “implemented” by three rules \((\text{SR}, \text{1beta}, 1)\), \((\text{SR}, \text{1beta}, 2)\), and \((\text{SR}, \text{1beta}, 3)\) : one variant for each variant of the reduction contexts \(R\), and the rule \((\text{SR}, \text{1let-in}, 1)\) requires a NCC to ensure that let-bound variables in \(E2\) are disjoint from the variables in \(E1\). Answers in \(L_{need}\) are the weak head normal forms, i.e. abstractions perhaps with an outer \texttt{letrec}. 

\footnote{In the LRSX Tool constrained expressions are written as “\textit{e where Constraints}” such that Constraints is a list of constraints, where non-empty context constraints are written as \(D \neq \{\cdot\}\), non-empty environment constraints are written as \(E \neq \{\cdot\}\), and non-capture constraints can occur as \((s, d)\), but also as \([\text{env}, d]\) representing the NCC \(\text{letrec env in c, d}\) for some constant \(c\).}
Definition 2.4. For a program calculus (SR, Ans), a ground expression $s_0, s_0$ converges (written $s_0 \Downarrow$) iff there exists a sequence $s_0 \xrightarrow{SR} s_1 \xrightarrow{SR} s_2 \ldots \xrightarrow{SR} s_k$ where $s_k$ is an answer and $k \geq 0$. We write $s \Downarrow_{\leq} t$ iff $s_\Downarrow \Longrightarrow t_\Downarrow$ ($\leq$ is called convergence approximation), and $s \Downarrow_{\alpha} t$ iff $s \Downarrow_{\leq} t$ and $t \Downarrow s$ ($\downarrow_{\alpha}$ is called convergence equivalence). If for all contexts $\Delta$ we have $d[s] \Downarrow_{\leq} d[t]$, then we write $s \Downarrow_{\leq} t$ and say that $t$ contextually approximates $s$. Expressions $s, t$ are contextually equivalent ($\Downarrow_{\leq} c$) if $s \Downarrow_{\leq} t$ and $t \Downarrow_{\leq} s$.

Meta transformations are letrec rewrite rules that fulfill some form of stability w.r.t. $\alpha$-renaming:

Definition 2.5. A letrec rewrite rule with $\Delta = T$ is a meta transformation, if the following conditions hold (see also Fig. 3):

(1) For all $s_1, s_2, t_1$ with $s_1 T_{\alpha} s_2, s_1 \sim_{\alpha} t_1$, such that $t_1$ fulfills the DVC: 1. If $t_1 \in \gamma(\Delta, \Delta)$ for some $(t, \Delta) \in \text{Ans}$, then there exists $s'_1 \in \gamma(t, \Delta)$ such that $s'_1 \sim_{\alpha} s_1$ and $s'_1 T_{\alpha} s'_2$ with $s'_2 \sim_{\alpha} s_2$. 2. If $t_1 \xrightarrow{SR_{\alpha}'} t_2$, then there exist $s'_1 \sim_{\alpha} s_1, s'_2 \sim_{\alpha} s_2, t'_2 \sim_{\alpha} t_2$ such that $s'_1 T_{\alpha} s'_2$ and $s'_1 \xrightarrow{T_{\alpha}'} t'_2$.

A meta transformation $\ell \xrightarrow{T_{\alpha}} r$ is correct iff $\gamma(\ell) \subseteq \gamma(r)$. A meta transformation $\ell \xrightarrow{T_{\alpha}} r$ is called overlapable if no $Ch$-variable occurs in $\ell$ and $r$ and the transformation is closed w.r.t. a sufficient context class for $\sim_{\leq}$, i.e. $s \xrightarrow{T_{\alpha}} t, s \Downarrow_{\leq} t$ imply $s \Downarrow_{\leq} t$.

The conditions on meta transformations allow us to inspect overlaps between transformations and standard reductions and answers without considering $\alpha$-renaming steps. A sufficient criterion to fulfill
Conditions (1) and (2) from Definition 2.5 is that applicability of a transformation to an expression \( s \) implies applicability of the transformation to all \( \alpha \)-renamed expressions \( s' \sim_\alpha s \) that fulfill the DVC (see Proposition A.1 in the appendix). In the calculus \( L_{\text{need}} \), this conditions holds for most of the transformations under consideration. An exception is the reversed copy transformation, (e.g. the reversal of \( \text{cp-in} \) in Fig. 2). The rule does not fulfill the mentioned condition, since all ground instances of the left hand side violate the DVC. However, the conditions (1) and (2) from Definition 2.5 hold, since two occurrences of \( \lambda \) do not forbid the application of a standard reduction.

Meta transformations \( \ell \to_T n \to_A r \) are written in the LRSX Tool as \( \{n,k\} \ell \implies r \) where Constraints" where \( k \) is a non-negative integer representing the variant of the rule. For the calculus \( L_{\text{need}} \) a context lemma [15] holds, which shows that top contexts are a sufficient class for \( \sim_c \), thus it suffices to consider the closure of garbage collection w.r.t. top contexts. We can represent the rules for garbage collection as:

\[
\begin{align*}
\{\text{gcT},1\} & : T[\text{letrec } E_1; E_2 \text{ in } S] \implies T[\text{letrec } E_1 \text{ in } S] \\
& \quad \text{where } E_1 /\neg= \{\}, E_2 /\neg= \{\}, [E_1, \text{letrec } E_2 \text{ in } [.]], (S, \text{letrec } E_2 \text{ in } [.]) \\
\{\text{gcT},2\} & : T[\text{letrec } E \text{ in } S] \implies T[S] \text{ where } E /\neg= \{\}, (S, \text{letrec } E \text{ in } [.])
\end{align*}
\]

3 Computing Diagrams and Automated Induction

For proving \( \gamma(\text{gcT}) \subseteq \leq_{\text{j}} \), we have to compute all overlaps between an answer and the left hand side of \( \text{gcT} \) (called answer overlaps\(^5\)) and all overlaps between the left hand sides of a standard reduction and of \( \text{gcT} \) (called forking overlaps\(^6\)). Clearly, computing the overlaps cannot be done using the concretizations w.r.t. \( \gamma \) but has to be done on the meta-syntax, i.e. by unifying the left hand sides of the meta-transformation with the left hand sides of the standard reductions and the answers, respecting the constraint tuples corresponding to the rules. An appropriate unification algorithm for LRSX was developed in [16] and implemented in the LRSX Tool. Calling the tool produces 99 (93, resp.) overlaps of \( \{\text{gcT},1\} \) (\( \{\text{gcT},2\} \) resp.) with all standard reductions and answers.

For joining the overlaps and computing so-called answer diagrams and forking diagrams (consisting of the overlap and a join), we have to apply standard reductions and transformation rules to the constrained expressions (again on the meta-syntax) of the overlaps until a common successor is found. For an answer \( s \) and an answer overlap \( s \xleftarrow{T,n'} t \), a join is a sequence \( t_k \xleftarrow{SR_{n_k}} \cdots \xleftarrow{SR_{n_1}} t \) where \( k \geq 0 \) and \( t_k \in \gamma(\text{Ans}) \). For a forking overlap \( s_1 \xleftarrow{SR} t \xrightarrow{T,n'} t_1 \), a join is a sequence \( s_1 \xrightarrow{SR_{n_k}} \cdots \xrightarrow{SR_{n_1}} s_k \xrightarrow{T,n_{k+1}} t_1 \)

\(^5\)Internally computing answer overlaps is done by adding special standard reduction rules of the form \( \ell \to \text{answer} \) where \( \ell \in \text{Ans} \) and answer is a new constant.

\(^6\)In the LRSX Tool the commands to overlap the left hand sides with all standard reductions are overlap (gcT,1).all and overlap (gcT,2).all.
The forking overlap together with a join builds a forking diagram which can be depicted as shown in Fig. 6 (where steps from the overlap are written with solid arrows, and (existentially quantified) steps of the join are written with dashed arrows).

To apply the letrec rewrite rules a matching algorithm for LRSX is used which is described in [13]. A peculiarity of the matching problem is, that constrained expressions of the overlap have to be matched against meta-expressions from the rewrite rule which also come with constraint tuples, and thus the algorithm has to guarantee that the given constraints imply the needed constraints before delivering a matcher. A further specialty is that the rewrite mechanism has to guarantee completeness w.r.t. ground instances, i.e. each rewrite step on the meta-level (applying meta rewrite rules to constrained expressions) must also be possible for all ground instances. The LRSX Tool uses an iterative and depth-bounded depth first search to bound the number of applied transformations and reductions. Since sometimes no join is found, since a possible rewriting requires more knowledge on the (non-)emptiness of environment and context variables, the LRSX Tool uses backtracking: If no join is found for an overlap, then first a case distinction for context variables in the problem is done (whether they are empty or non-empty) and then context variables, the LRSX Tool uses backtracking: If no join is found for an overlap, then first a case distinction for environment variables.

For checking if a join is found, we have to test equivalence of constrained expressions. A simple check is testing \( t \sim_{let} s \) which also implies \( t \sim_{<ANSWER>} s \) with \( t \) and \( s \) ground expressions. If the given constraints imply the needed constraints before delivering a matcher. For our example, the computed forking diagrams are shown in Fig. 8 and a pictorial representation of the forking diagrams is in Fig. 7. In a pen-and-paper proof of \( \forall (gcT) \subseteq \downarrow \), an induction on the length of a converging reduction sequence \( s \rightarrow_{SR,T} s' \) for \( s \) with \( \gamma(gcT) \) to \( t \) is used to show that \( t \) converges. The induction base is covered by the answer diagrams, and for the induction step, let \( s \rightarrow_{SR,T} s' \). Applying a forking diagram to \( s \rightarrow_{SR,T} t \) shows existence of some \( t' \) with \( s \rightarrow_{geT} t' \) or \( s \rightarrow_{geT} t' = t \) and by the induction hypothesis \( t' \downarrow \) which also implies \( t \downarrow \). This induction

\[ \begin{align*}
\text{Figure 7: Diagrams for (gcT), pictorial} \\
&\text{Figure 8: Diagrams for (gcT), textual} \\
&\text{Figure 9: Obtained TRS for (gcT)}
\end{align*} \]
(even with more complex induction measures) can be automatized by interpreting the answer and forking diagrams as term rewrite system and by showing (innermost) termination of them (see [11]). From the obtained answer and forking diagrams for \((gcT)\), the LRSX Tool generates the term rewrite system show in Fig. 9 which is shown to be innermost terminating using the prover AProVE and the certifier CeTA.

4 Extended Techniques and Limitations of the Method

The previous example (proving \(\gamma(gcT) \subseteq \leq_1\)) is quite simple where unification and matching for LRSX-expressions and usual term rewrite systems for the automated induction are successful. However, the LRSX Tool provides more sophisticated techniques that are for instance required when proving the remaining part, i.e. \(\gamma(gcT) \subseteq \geq_1\), to complete the correctness proof of garbage collection. First observe that the diagram technique works as before with the difference that the reversal of \((gcT)\) is used (i.e. with writing \((gcT)^-\) for reversing the transformation \((gcT)\) we have to show \(\gamma((gcT)^- \subseteq \leq_1)\). However, this means that we have to overlap left hand sides of standard reductions and answers with right hand sides of \((gcT)\). The obtained overlaps are called answer and commuting diagrams. Computing the overlaps results in 99 overlaps for \((gcT,1)\) and 203 overlaps for \((gcT,2)\). However, using the presented techniques for computing joins fails. An overlap (we omit the constraints) which cannot be joined is

\[
A[(\lambda X . S) \ T[letrec \ E_1 \ in \ S']] \xrightarrow{gcT,1} A[(\lambda X . S) \ T[letrec E_1; E_2 \ in \ S']] \\
A[letrec \ X . T[letrec \ E_1 \ in \ S'] \ in \ S]
\]

The automated method cannot apply a \((SR,\beta)\)-reduction to the upper-right expression, since it cannot infer that variable \(X\) does not occur in \(E_2\). However, this problem can be solved by \(\alpha\)-renaming the expression such that the DVC holds. That is why symbolic \(\alpha\)-renaming (see [12]) is built into the LRSX Tool which is quite more complex than usual \(\alpha\)-renaming, since it has to be performed on the meta syntax, e.g. internally symbolic renamings of the form \(\alpha \cdot S\) are required. Even with \(\alpha\)-renaming, the LRSX Tool cannot join all overlaps. E.g., for the overlap (we omit the constraints)

\[
A[letrec \ X . S' \ in \ S] \xrightarrow{SR,\beta,1} A[(\lambda X . S) \ S'] \xrightarrow{gcT,2} A[(letrec \ E \ in \ (\lambda X . S)) \ S']
\]

a meta-argument is required to close the overlap stating that the standard reduction moves the environment \(E\) to the top of the expression, i.e. a sequence \(A[(letrec \ E \ in \ (\lambda X . S)) \ S'] \xrightarrow{SR,\beta} letrec \ E \ in \ A[(\lambda X . S)) \ S']\) where \(\xrightarrow{SR,\beta}\) is the transitive closure of \(\xrightarrow{SR,\beta}\). In the LRSX Tool such transitive closures can be defined and with these rules it is able to compute a complete set of commuting diagrams for the \((gcT)\)-transformation. A pictorial representation of the commuting diagrams for \(a \in \{\beta, cp, III\}\) is shown in Fig. 10.

The automated induction has to treat the transitive closure in the rules. A naive encoding leads to term rewrite systems with infinitely many rules. The LRSX Tool generates a term rewrite system with
### Table 1: Statistics of executing the LRSX Tool

<table>
<thead>
<tr>
<th>Calculus</th>
<th># overlaps</th>
<th># meta joins</th>
<th># meta joins with α-renaming</th>
<th>diagram computation time</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>forking</td>
<td>answer</td>
<td>forking</td>
<td>answer</td>
</tr>
<tr>
<td>(L_{\text{need}}) (11 SR rules, 16 transformations, 2 answers)</td>
<td>2215</td>
<td>27</td>
<td>5398</td>
<td>27</td>
</tr>
<tr>
<td></td>
<td>2963</td>
<td>38</td>
<td>7235</td>
<td>38</td>
</tr>
<tr>
<td>(L_{\text{need}}^{+\text{seq}}) (17 SR rules, 18 transformations, 2 answers)</td>
<td>4869</td>
<td>29</td>
<td>14700</td>
<td>29</td>
</tr>
<tr>
<td></td>
<td>6394</td>
<td>43</td>
<td>18046</td>
<td>43</td>
</tr>
<tr>
<td>(L_{\text{LR}}) (76 SR rules, 43 transformations, 17 answers)</td>
<td>85455</td>
<td>1586</td>
<td>389678</td>
<td>1586</td>
</tr>
<tr>
<td></td>
<td>105053</td>
<td>2280</td>
<td>426664</td>
<td>2440</td>
</tr>
</tbody>
</table>

The Haskell-implementation of the automated diagram method to prove correctness of program transformation is available as a Cabal-package from [http://goethe.link/LRSXTOOL61](http://goethe.link/LRSXTOOL61). We tested our implementation with three different program calculi and a lot of program transformations. The tested calculi are the calculus \(L_{\text{need}}\) – a minimal call-by-need lambda calculus with \texttt{letrec} – the calculus \(L_{\text{need}}^{+\text{seq}}\) which extends \(L_{\text{need}}\) by the \texttt{seq}-operator, where \texttt{seq }e_1 \texttt{ e_2} first evaluates the first argument \(e_1\) and after

5 Implementation and Experiments

The Haskell-implementation of the automated diagram method to prove correctness of program transformation is available as a Cabal-package from [http://goethe.link/LRSXTOOL61](http://goethe.link/LRSXTOOL61). We tested our implementation with three different program calculi and a lot of program transformations. The tested calculi are the calculus \(L_{\text{need}}\) – a minimal call-by-need lambda calculus with \texttt{letrec} – the calculus \(L_{\text{need}}^{+\text{seq}}\) which extends \(L_{\text{need}}\) by the \texttt{seq}-operator, where \texttt{seq }e_1 \texttt{ e_2} first evaluates the first argument \(e_1\) and after
obtaining a successful result it evaluates argument \( e_2 \), and the calculus LR \([18]\) which extends \( L_{\text{seq}}^{\text{new}} \) by data constructors for lists, booleans and pairs together with corresponding case-expressions, and can be seen as an untyped core language of Haskell. The tested program transformations include all calculus reductions which can be summarized as “partial evaluation”, several copying transformations and rules for removing garbage and inlining of let-bindings which are referenced only once.

The results of our experiments are in Table 1 where we also list the numbers of standard reductions, transformations, and answers in the input. The table shows the numbers of computed overlaps, corresponding joins (which is higher due to the branching in unsuccessful cases), joins which use the \( \alpha \)-renaming procedure. The row marked with \( \rightarrow \) represent the forking diagrams, and \( \leftarrow \) represent the reversed transformations, i.e. commuting diagrams. In all cases, termination of the termination problems was proved by AProVE and certified by CeTA. The last column lists the execution time\(^8\) for calculating the overlaps and the joins. The time to compute (more) joins in the calculus LR for commuting diagrams than for computing forking diagrams, can be explained: we optimized the diagram computation (but cutting down unusual search paths) for the commuting case much more than for the forking case.

6 Conclusion

We presented a system to automatically prove correctness of program transformations which is implemented as the LRSX Tool. We illustrated its use by an example and discussed peculiarities of its design and its implementation. By providing the results of experiments, we demonstrated the success of the method and the tool. Future work is to extend the tool to prove correctness of program translations where source and target language are different.

Acknowledgments. We thank René Thiemann for support on AProVE and CeTA.

References


---

\(^8\)Tests ran on a system with Intel i7-4790 CPU 3.60GHz, 8 GB memory using GHC’s \(-N\) option for parallel execution.


Appendix

A Soundness of the Diagram Method

Proposition A.1. Let \((\text{SR}, \text{Ans})\) be a program calculus and \(s \xrightarrow{T,n,T} t\) be a letrec rewrite rule such that no Ch-variable occurs in \(\ell\) and \(r\) and the transformation is closed w.r.t. a sufficient context class for contextual equivalence. Assume that \(s_1 \xrightarrow{T,n} s_2\) implies that for all \(s'_1 \sim_\alpha s_1\) such that \(s'_1\) fulfills the DVC also \(s'_1 \xrightarrow{T,n} s'_2\) for some \(s'_2 \sim_\alpha s_2\). Assume also that \(s_1 \xrightarrow{T,n} s_2\) for \(s_1 \in \gamma(\text{Ans})\) implies that for all \(s'_1 \sim_\alpha s_1\) also \(s'_1 \xrightarrow{T,n} s'_2\) holds for some \(s'_2 \sim_\alpha s_2\). Then \(s \xrightarrow{T,n,T} t\) is overlapable.

We show soundness of the diagram method, where it is important to verify that our conditions in Definition 2.5 imply that it suffices to consider overlaps of standard reductions and transformations without performing \(\alpha\)-renaming.

Let \((\text{SR}, \text{Ans})\) be a program calculus, OTR be a set of overlapable meta transformations, and \(\text{TR} \supset OTR\) be a set of meta transformations such that each \((\ell \xrightarrow{\gamma(T,n)} r) \in \text{TR}\) there exists \((\ell \xrightarrow{\gamma(T,n')} r) \in OTR\) with \(\gamma(\ell \xrightarrow{\gamma(T,n)} r) \subseteq \gamma((\ell \xrightarrow{\gamma(T,n')} r))\) (we say that \(n'\) subsumes \(n\) w.r.t. \(\gamma\)).

A set of forking and answer diagrams is complete for a set OTR iff for all forking overlaps of transformations in OTR with standard reductions and every answer overlap, a diagram in the set is applicable. Applicability means that the concrete overlap is an instance of the overlap described by the diagram, and that the existentially quantified expressions, reductions, and transformations can accordingly be instantiated.

Already, in [11] it was shown that proving termination of the string rewrite system with infinitely many rules can be automated by using automated termination provers for term rewrite systems and showing termination of the integer term rewrite system (or a term rewrite system with free variables on the right hand side that represent arbitrary constructor terms). Thus, we do not repeat this technique here, and formulate our soundness result in terms of the string rewrite system which is induced by the diagrams:

Theorem A.2. If a complete set of forking and answer diagrams for OTR is terminating as a string rewrite system, then all \(\ell \xrightarrow{T,n,T} r \in \text{TR}\) are convergence equivalent.

Proof. Since transformations in TR are subsumed by the transformations in OTR it is sufficient to consider \(\ell \xrightarrow{T,n,T} r \in OTR\). Assume that \(s \xrightarrow{T,n} t\) and \(s_1\). Then there exists a sequence \(s'_k \sim_\alpha s_k \xleftarrow{\text{SR}'} \cdots \xleftarrow{\text{SR}'} s_1 \xrightarrow{T,n} t\) where \(s'_k \in \gamma(\text{Ans})\). We apply modifications to the sequence and replace overlaps by joins according to the following rules:

1. If the sequence contains a transformation step \(s_1 \xrightarrow{T,n'} s_2\) where \(\xrightarrow{T,n'} \in (\text{TR} \setminus \text{OTR})\), then there exists \(\xrightarrow{T,n''} \in \text{OTR}\) with \(s_1 \xrightarrow{T,n'} s_2 \in \gamma\). Replace \(s_1 \xrightarrow{T,n'} s_2\) by \(s_1 \xrightarrow{T,n''} s_2\).

2. If the sequence contains a step \(s_1 \xleftarrow{\text{SR}'} s_2\), i.e. \(s_1 \xleftarrow{\text{SR}'} s'_2 \sim_\alpha s_2\), and \(s'_2\) does not fulfill the DVC, then replace \(s'_2\) by an expression \(s_2'' \sim_\alpha s_2\) such that \(s_2''\) fulfills the DVC. By Definition of standard reductions, the standard reduction \(s_1 \xleftarrow{\text{SR}'} s''_2\) with \(s'_2 \sim_\alpha s_1\) exists. Replace \(s_1 \xleftarrow{\text{SR}'} s''_2\sim_\alpha s_2\) by \(s_1 \sim_\alpha s_1' \xleftarrow{\text{SR}'} s''_2\sim_\alpha s_2\).

3. If the sequence contains \(s_1 \xleftarrow{\text{SR}'} s_2 \xrightarrow{\text{SR}} s_3\), then the calculus is deterministic and thus \(s_1 \sim_\alpha s_3\) holds. Replace the \(s_1 \xleftarrow{\text{SR}'} s_2 \xrightarrow{\text{SR}} s_3\) by \(s_1 \sim_\alpha s_3\).
4. If the sequence has a prefix \( s_1 \xrightarrow{\alpha} s_3 \) where \( s_1 \) is an answer, then the calculus is deterministic and \( s_3 \) is answer and we replace the prefix \( s_1 \xrightarrow{\alpha} s_3 \) by \( s_3 \).
5. Subsequences \( s_1 \sim_\alpha s_2 \sim_\alpha s_3 \) are replaced by \( s_1 \sim_\alpha s_3 \).
6. If the left-most expression of the sequence is \( s_1 \in \gamma(\text{Ans}) \) and does not fulfill the DVC, then replace \( s_1 \) by \( s'_1 \sim_\alpha s_1 \) such that \( s'_1 \) fulfills the DVC. Note that due to our assumption on answers, \( s'_1 \in \gamma(\text{Ans}) \).

7. If the sequence has a prefix \( t_1 \sim_\alpha s_1 \xrightarrow{T.n} s_2 \), where \( t_1 \) fulfills the DVC and \( t_1 \in \gamma(\text{Ans}) \), then first apply Condition [1] of Definition 2.5 i.e. replace the prefix by \( t_1 \sim_\alpha s'_1 \xrightarrow{T.n} s'_2 \sim_\alpha s_2 \) where \( s'_1 \in \gamma(\text{Ans}) \) and \( s'_1 \sim_\alpha t_1 \). Now the answer overlap \( s'_1 \xrightarrow{T.n} s'_2 \) is replaced by the corresponding join.

8. If the sequence contains \( t_2 \xleftarrow{SR.n} t_1 \sim_\alpha s_1 \xrightarrow{T.n} s_2 \), then \( t_1 \) fulfills the DVC (by the modification in item 2) and we can use Condition 2 of Definition 2.5 and replace \( t_2 \xleftarrow{SR,n'} t_1 \sim_\alpha s_1 \xrightarrow{T.n} s_2 \) by \( t_2 \sim_\alpha t'_2 \xleftarrow{SR,n'} s'_1 \xrightarrow{T.n} s'_2 \sim_\alpha s_2 \). Now replace the forking overlap \( t'_2 \xleftarrow{SR,n'} s'_1 \xrightarrow{T.n} s'_2 \) by its join.

The modifications show that we can replace overlaps by joins until the sequence is of the form \( s_n \xleftarrow{\alpha} \cdots \xleftarrow{\alpha} t \). Termination of the string rewrite system and the observation that \( \xleftarrow{\alpha} \)-reductions which are introduced by joins can always be removed by the modifications (3) and (4), shows that the replacement together with the modifications terminates. Since, the last end of the sequence is always an expression in \( \gamma(\text{Ans}) \), this shows \( t \downarrow \).

\section{Checking Equivalence of Constrained Expressions}

We define an NCC-implication check for constrained expressions. Before providing the implication check, we define how to split NCCs into \textit{atomic NCCs} \((u,v)\) such that \(u,v\) are variables or meta-variables. For a set \( \mathcal{S} \) of NCCs, let \( \text{split}_{ncc}(\mathcal{S}) := \mathcal{S} \cup \varnothing \cup \text{Var}_A(s) \times \text{Var}_M(d) \) where \( \text{Var}_A(s) = \text{MV}(s) \cup \text{Var}(s) \), and \( \text{CV}_M \) collects all concrete variables that capture variables of the context hole, and all meta-variables which may have concretizations that introduce capture variables. A ground substitution \( \rho \) \textit{satisfies an atomic NCC} \((u,v)\) iff \( \text{Var}(\rho(u)) \cap \text{CV}_A(\rho(v)) = \emptyset \) where \( \text{CV}_A(x) = \{x\} \) for all variables \( x \) and \( \text{CV}_A(r) = \text{CV}(r) \) for all other constructs \( r \). It is easy to verify that for a set of NCCs \( \mathcal{S} \), \( \rho \) satisfies all constraints in \( \mathcal{S} \) if and only if \( \rho \) satisfies all atomic NCCs in \( \text{split}_{ncc}(\mathcal{S}) \).

We now define the NCC-implication check.

\begin{definition}
Let \((s, \nabla)\) and \((t, \Delta)\) be constrained expressions with \( s \sim_{let} t, \gamma(s, \nabla) \neq \emptyset, \gamma(t, \Delta) \neq \emptyset \) and \( \text{MV}(s) = \text{MV}(t) \). Then \( \nabla \text{ implies } \Delta \) iff i) for all \( D \in \Delta_1 : D \in \nabla_1 \), ii) for all \( E \in \Delta_2 : E \in \nabla_2 \), and iii) for all \((u,v)\) in \( \text{split}_{ncc}(\Delta_3) \cup \text{NCC}_{dvc}(t) \) one of the following cases holds:
\begin{enumerate}
\item \( u = x \) and \( v = y \) where \( x \neq y \).
\item \((u,v) \in \text{split}_{ncc}(\nabla_3) \cup \text{NCC}_{dvc}(s)\).
\item \( u = v, u \in \text{MV}(\Delta) \setminus \text{MV}(\nabla) \) and \( u \in \{Ch,D,E\} \) such that \( E \notin \Delta_2 \).
\item \( u \neq v, u \in \text{MV}(\Delta) \setminus \text{MV}(\nabla) \) and \( u = Ch, or u = S, or u = D \) or \( u = E, or u = X \).
\item \( u \neq v, v \in \text{MV}(\Delta) \setminus \text{MV}(\nabla) \) and \( v \in \{Ch,D,E,X\} \).
\item \( u = E \) or \( u = Ch \) with \( \text{cl}(Ch) = \text{Triv} \), and \((u,u) \in \text{split}_{ncc}(\nabla_3) \cup \text{NCC}_{dvc}(s)\).
\end{enumerate}
\end{definition}
7. \( v \in \{ E, Ch, D \} \) and \((v,v) \in \text{split}_{\text{ncc}}(\nabla_3) \cup \text{NCC}_{dvc}(s)\).

8. \((u,v)\) is of the form \((X,y), (x,Y), (X,Y), (x,D), (x,E), (x,Ch), (x,Ch), (Ch_1,x), (Ch_1,E), (Ch_1,D), \) or \((Ch_1,Ch_2)\) where \(cl(Ch_1) = \text{Triv}\) and in all cases \((v,u) \in \text{split}_{\text{ncc}}(\nabla_3) \cup \text{NCC}_{dvc}(s)\).

We call \((s,\nabla)\) and \((t,\Delta)\) \textit{NCC-equivalent} iff \(\Delta\) implies \(\nabla\) and \(\nabla\) implies \(\Delta\).

**Proposition B.2.** \textit{NCC-equivalence of \((s,\nabla)\) and \((t,\Delta)\) implies} \(\gamma(s,\nabla) = \gamma(t,\Delta)\).

**Proof.** It suffices to show that for \((s,\nabla)\) and \((t,\Delta)\) such that \(\nabla\) implies \(\Delta\), the inclusion \(\gamma(t,\Delta) \subseteq \gamma(s,\nabla)\) holds. Let \(\rho\) be a substitution such that \(\rho(s)\) satisfies the LVC and \(\rho\) satisfies \(\nabla\). We show that there exists a substitution \(\rho_0\) such that \(\rho_0 \circ \rho\) is ground for \((t,\Delta)\) and with \(\rho' = \rho_0 \circ \rho\), \(\rho'(t)\) satisfies the LVC and \(\rho'\) satisfies \(\Delta\).

Let \(\rho_0(Ch) = [\cdot, [\cdot]_2]\) for all \(Ch \in MV(t,\Delta) \setminus MV(s,\nabla)\). \(\rho_0(S) = \lambda x_S. x_S\) for a fresh variable \(x_S\) for all \(S \in MV(t,\Delta) \setminus MV(s,\nabla)\). For all \(D \in MV(t,\Delta) \setminus MV(s,\nabla)\), let \(\rho_0(D) = [\cdot]\) if \(D \not\in \Delta_1\), and \(\rho_0(D) = d\) where \(d\) is a context with \(CV(d) = \emptyset\). For all \(E \in MV(t,\Delta) \setminus MV(s,\nabla)\), let \(\rho_0(E) = [\cdot]_2\) if \(E \not\in \Delta_2\) and \(\rho_0(E) = x_E. \var x_E\), otherwise where \(x_E\) is a fresh variable; For all \(X \in MV(t,\Delta) \setminus MV(s,\nabla)\), let \(\rho_0(X) = x_X\) for a fresh variable \(x_X\).

By the definition of the NCC-implication check and the choice of \(\rho_0\), \(\rho'\) satisfies \(\Delta_1\) and \(\Delta_2\). For the remaining parts, we show that \(\rho'\) satisfies all atomic NCCs in \(\text{split}_{\text{ncc}}(\Delta_3) \cup \text{NCC}_{dvc}(t)\).

Let \((u,v) \in \text{split}_{\text{ncc}}(\Delta_3) \cup \text{NCC}_{dvc}(t)\). Then one of the cases of Definition \([B.1]\) holds. If \(u = x\) and \(v = y\) where \(x \neq y\), the \((\rho(u), \rho(v))\) is satisfied. If \((u,v) \in \text{split}_{\text{ncc}}(\nabla_3) \cup \text{NCC}_{dvc}(s)\) then \(\rho'\) satisfies \((u,v)\) since \(\rho\) satisfies \(\nabla_3\) or for \((u,v) \in \text{NCC}_{dvc}(s)\), \(u,v\) are let-variables of the same environment and thus \(\rho\) must map \(u\) and \(v\) to distinct concrete variables, since otherwise the LVC for \(\rho(s)\) is violated. If \(u = v\), \(u \in MV(\Delta) \setminus MV(\nabla)\) and \(u \in \{ Ch, D, E \}\) such that \(E \not\in \Delta_2\) we verify that \(\rho_0\) satisfies \((u,u)\) and thus \(\rho\) does. If \(u \neq v\), \(u \in MV(\Delta) \setminus MV(\nabla)\) and \(u = Ch\), or \(u = S\), or \(u = D\) or \(u = E\), or \(u = X\). \(\rho_0\) satisfies \((u,u)\) and thus \(\rho\) does. If \(u \neq v\), \(v \in MV(\Delta) \setminus MV(\nabla)\) and \(v \in \{ Ch, D, E, X \}\). \(\rho_0\) satisfies \((u,u)\) and thus \(\rho\) does. If \((u,v)\) is \((X,y), (x,Y), (X,Y), (x,D), (x,E), (x,E), (x,Ch), (x,Ch), (Ch_1,x), (Ch_1,E), (Ch_1,D), \) or \((Ch_1,Ch_2)\) where \(cl(Ch_1) = \text{Triv}\) and in all cases \((v,u) \in \text{split}_{\text{ncc}}(\nabla_3) \cup \text{NCC}_{dvc}(s)\), we verify that since \(\rho\) satisfies \((v,u)\), \(\rho\) also has to satisfy \((u,v)\). \(\square\)