Formalisation and Analysis of Component Dependencies

Maria Spichkova

September 19, 2015

Abstract

This set of theories presents a formalisation in Isabelle/HOL [3] of data dependencies between components. The approach allows to analyse system structure oriented towards efficient checking of system: it aims at elaborating for a concrete system, which parts of the system (or system model) are necessary to check a given property.

Contents

1 Introduction 2

2 Case Study: Definitions 7

3 Inter-/Intracomponent dependencies 14
   3.1 Direct and indirect data dependencies between components  18
   3.2 Components that are elementary wrt. data dependencies . . . 23
   3.3 Set of components needed to check a specific property . . . . 24
   3.4 Additional properties: Remote Computation . . . . . . . . . . 26

4 Case Study: Verification of Properties 26
   4.1 Correct composition of components . . . . . . . . . . . . . 26
   4.2 Correct specification of the relations between channels . . . . 31
   4.3 Elementary components . . . . . . . . . . . . . . . . . . . . 35
   4.4 Source components . . . . . . . . . . . . . . . . . . . . . . . 37
   4.5 Minimal sets of components to prove certain properties . . . 45
1 Introduction

In general, we don’t need complete information about the system as to check its certain property. An additional information about the system can slow the whole process down or even make it infeasible. In this theory we define constraints that allow to find/check the minimal model (and the minimal extent of the system) needed to verify a specific property. Our approach focuses on data dependencies between system components. Dependencies’ analysis results in a decomposition that gives rise to a logical system architecture, which is the most appropriate for the case of remote monitoring, testing and/or verification.

Let $CSet$ be a set of components on a certain abstraction level $L$ of logical architecture (i.e. level of refinement/decomposition, data type $\text{AbstrLevelsID}$ in our Isabelle formalisation). We denote the sets of input and output streams of a component $S$ by $\mathbb{I}(S)$ (function $IN : CSet \Rightarrow \text{chanID set}$ in Isabelle) and $\mathbb{O}(S)$ (function $OUT : CSet \Rightarrow \text{chanID set}$ in Isabelle). The set of local variables of components is defined in Isabelle by $\text{VAR}$, and the function to map component identifiers to the corresponding variables is defined by $\text{VAR} : CSet \Rightarrow \text{varID set}$.

Please note that concrete values for these functions cannot be specified in general, because they strongly depend on a concrete system. In this paper we present a small case study in the theories $\text{DataDependenciesConcreteValues.thy}$ (specification of the system architecture on several abstraction levels) and $\text{DataDependenciesCaseStudy.thy}$ (proofs of system architectures’ properties).

Function $\text{subcomp} : CSet \Rightarrow \text{CSet set}$ maps components to a (possibly empty) set of its subcomponents.

We specify the components’ dependencies by the function

$$\text{Sources}^L : CSet^L \rightarrow (CSet^L)^*$$

which returns for any component identifier $A$ the corresponding (possibly empty) list of components (names) $B_1, \ldots, B_N$ that are the sources for the input data streams of $A$ (direct or indirect):

$$\text{Sources}^L(C) = DSources^L(C) \cup \bigcup_{S \in DSources^L(C)} \{S_1 \mid S_1 \in \text{Sources}^L(S)\}$$

Direct data dependencies are defined by the function

$$DSources^L : CSet^L \rightarrow (CSet^L)^*$$

$$DSources^L(C) = \{S \mid \exists x \in \mathbb{I}(C) \land x \in \mathbb{O}(S)\}$$
For example, $C_1 \in DSources^L(C_2)$ means that at least one of the output channels of $C_1$ is directly connected to some of input channels of $C_2$.

$\mathbb{I}^D(C, y)$ denotes the subset of $\mathbb{I}(C)$ that output channel $y$ depends upon, directly (specified in Isabelle by function $OUTfromCh :: chanID \Rightarrow chanID\ \text{set}$ or via local variables (specified by function $OUTfromV :: chanID \Rightarrow varID\ \text{set}$). For example, let the values of the output channel $y$ of component $C$ depend only on the value of the local variable $st$ that represents the current state of $C$ and is updated depending to the input messages the component receives via the channel $x$, then $\mathbb{I}^D(C, y) = \{x\}$. In Isabelle, $\mathbb{I}^D(C, y)$ is specified by function $OUTfrom :: chanID \Rightarrow varID\ \text{set}$.

Based on the definition above, we can decompose system’s components to have for each component’s output channel the minimal subcomponent computing the corresponding results (we call them *elementary components*). An elementary component either

- should have a single output channel (in this case this component can have no local variables), or
- all it output channels are correlated, i.e. mutually depend on the same local variable(s).

If after this decomposition a single component is too complex, we can apply the decomposition strategy presented in [5].

For any component $C$, the dual function $\mathbb{O}^D$ returns the corresponding set $\mathbb{O}^D(C, x)$ of output channels depending on input $x$. This is useful for tracing, e.g., if there are some changes in the specification, properties, constraints, etc. for $x$, we can trace which other channels can be affected by these changes.

If the input part of the component’s interface is specified correctly in the sense that the component does not have any “unused” input channels, the following relation will hold: $\forall x \in \mathbb{I}(C).\ \mathbb{O}^D(C, x) \neq \emptyset$.

We illustrate the presented ideas by a small case study: we show how system’s components can be decomposed to optimise the data dependencies within each single component, and after that we optimise architecture of the whole system. System $S$ (cf. also Fig. 1) has 5 components, the set $CSet$ on the level $L_0$ is defined by $\{A_1, \ldots, A_9\}$. The sets $\mathbb{I}^D$ of data dependencies between the components are defined in the theory `DataDependenciesConcreteValues.thy`. We represent the dependencies graphically using dashed lines over the component box.
Now we can decompose the system’s components according to the given $I^D$ specification. This results into the next abstraction level $L_1$ of logical architecture (cf. Fig. 2), on which all components are elementary. Thus, we obtain a (flat) architecture of system. The main feature of this architecture is that each output channel (within the system) belongs the minimal sub-component of a system computing the corresponding results. We represent this (flat) architecture as a directed graph (components become vertices and channels become edges) and apply one of the existing distributed algorithms for the decomposition into its strongly connected components, e.g. FB [2], OBF [1], or the colouring algorithm [4]. Fig. 3 presents the result of the architecture optimisation.

After optimisation of system’s architecture, we can find the minimal part of the system needed to check a specific property (cf. theory DataDependencies). A property can be represented by relations over data flows on the system’s channels, and first of all we should check the property itself, whether it reflect a real relation within a system. Let for a relation $r$, $I_r$, $O_r$ be the sets of input and output channels of the system used in this relation. For each channel from $O_r$ we recursively compute all the sets of the dependent components and corresponding input channels. Their union, restricted to the input channels of the system, should be equal to $I_r$, otherwise we should check whether the property was specified correctly.

Thus, from $O_r$ we obtain the set $outSetOfComponents$ of components having these channels as outputs, and compute the union of corresponding sources’ sets. This union together with $outSetOfComponents$ give us the minimal part of the system needed to check the property $r$: we formalise it in Isabelle by the predicate $minSetOfComponents$. 
For each channel and elementary component (i.e. for any component on the abstraction level $L_1$) we specify the following measures:

- measure for costs of the data transfer/upload to the cloud $\text{UplSize}(f)$: size of messages (data packages) within a data flow $f$ and frequency they are produced. This measure can be defined on the level of logical modelling, where we already know the general type of the data and can also analyse the corresponding component (or environment) model to estimate the frequency the data are produced;

- measure for requirement of using high-performance computing and cloud virtual machines, $\text{Perf}(X)$: complexity of the computation within a component $X$, which can be estimated on the level of logical modelling as well.

On this basis, we build a system architecture, optimised for remote computation. The $\text{UplSize}$ measure should be analysed only for the channels that aren’t local for the components on abstraction levels $L_2$ and $L_3$. 

Figure 2: Components’ decomposition (level $L_1$)
Using graphical representation, we denote the channels with $UplSize$ measure higher than a predefined value by thick red arrows (cf. also set $UplSizeHighLoad$ in Isabelle theory $DataDependenciesConcreteValues.thy$), and the components with $Perf$ measure higher than a predefined value by light green colour (cf. also set $HighPerfSet$ in Isabelle theory $DataDependenciesConcreteValues.thy$), where all other channel and components are marked blue.

Fig. 4 represents a system architecture, optimised for remote computation: components from the abstraction level $L_2$ are composed together on the abstraction level $L_3$, if they are connected by at least one channel with $UplSize$ measure higher than a predefined value. The components $S'_4$ and $S'_7$ have $Perf$ measure higher than a predefined value, i.e. using high-performance computing and cloud virtual machines is required.

Figure 3: Architecture of $S$ (level $L_2$)
2 Case Study: Definitions

theory DataDependenciesConcreteValues
import Main
begin

datatype CSet = sA1 | sA2 | sA3 | sA4 | sA5 | sA6 | sA7 | sA8 | sA9 |
              sA11 | sA12 | sA21 | sA22 | sA31 | sA32 | sA41 | sA42 |
              sA71 | sA72 | sA81 | sA82 | sA91 | sA92 | sA93 |
              sS1 | sS2 | sS3 | sS4 | sS5 | sS6 | sS7 | sS8 | sS9 | sS10 | sS11 |
              sS12 | sS13 | sS14 | sS15 | sS1opt | sS4opt | sS7opt | sS11opt

datatype chanID = data1 | data2 | data3 | data4 | data5 | data6 | data7 |
                   data8 | data9 | data10 | data11 | data12 | data13 | data14 | data15 |
                   data16 | data17 | data18 | data19 | data20 | data21 | data22 | data23 | data24

datatype varID = stA1 | stA2 | stA4 | stA6

datatype AbstrLevelsID = level0 | level1 | level2 | level3

— function IN maps component ID to the set of its input channels
fun IN :: CSet ⇒ chanID set
where
  IN sA1 = { data1 }
\[
\begin{align*}
\text{IN } sA2 &= \{ \text{data2, data3} \} \\
\text{IN } sA3 &= \{ \text{data4, data5} \} \\
\text{IN } sA4 &= \{ \text{data6, data7, data13} \} \\
\text{IN } sA5 &= \{ \text{data8} \} \\
\text{IN } sA6 &= \{ \text{data14} \} \\
\text{IN } sA7 &= \{ \text{data15, data16} \} \\
\text{IN } sA8 &= \{ \text{data17, data18, data19, data22} \} \\
\text{IN } sA9 &= \{ \text{data20, data21} \} \\
\text{IN } sA11 &= \{ \text{data1} \} \\
\text{IN } sA12 &= \{ \text{data1} \} \\
\text{IN } sA21 &= \{ \text{data2} \} \\
\text{IN } sA22 &= \{ \text{data2, data3} \} \\
\text{IN } sA23 &= \{ \text{data2} \} \\
\text{IN } sA31 &= \{ \text{data4} \} \\
\text{IN } sA32 &= \{ \text{data5} \} \\
\text{IN } sA41 &= \{ \text{data6, data7} \} \\
\text{IN } sA42 &= \{ \text{data13} \} \\
\text{IN } sA71 &= \{ \text{data15} \} \\
\text{IN } sA72 &= \{ \text{data16} \} \\
\text{IN } sA81 &= \{ \text{data17, data22} \} \\
\text{IN } sA82 &= \{ \text{data18, data19} \} \\
\text{IN } sA91 &= \{ \text{data20} \} \\
\text{IN } sA92 &= \{ \text{data20} \} \\
\text{IN } sA93 &= \{ \text{data21} \} \\
\text{IN } sS1 &= \{ \text{data1} \} \\
\text{IN } sS2 &= \{ \text{data1} \} \\
\text{IN } sS3 &= \{ \text{data2} \} \\
\text{IN } sS4 &= \{ \text{data2} \} \\
\text{IN } sS5 &= \{ \text{data5} \} \\
\text{IN } sS6 &= \{ \text{data2, data7} \} \\
\text{IN } sS7 &= \{ \text{data13} \} \\
\text{IN } sS8 &= \{ \text{data8} \} \\
\text{IN } sS9 &= \{ \text{data14} \} \\
\text{IN } sS10 &= \{ \text{data15} \} \\
\text{IN } sS11 &= \{ \text{data16} \} \\
\text{IN } sS12 &= \{ \text{data17} \} \\
\text{IN } sS13 &= \{ \text{data20} \} \\
\text{IN } sS14 &= \{ \text{data18, data19} \} \\
\text{IN } sS15 &= \{ \text{data21} \} \\
\text{IN } sS1opt &= \{ \text{data1} \} \\
\text{IN } sS4opt &= \{ \text{data2} \} \\
\text{IN } sS7opt &= \{ \text{data13} \} \\
\text{IN } sS11opt &= \{ \text{data16, data19} \}
\end{align*}
\]

---

function OUT maps component ID to the set of its output channels

\[
\text{fun } \text{OUT} :: \ CSet \to \ \text{chanID set}
\]

where

\[
\text{OUT } sA1 = \{ \text{data2, data10} \} \\
\text{OUT } sA2 = \{ \text{data4, data5, data11, data12} \}
\]

8
| OUT sA3 = { data6, data7 } |
| OUT sA4 = { data3, data8 } |
| OUT sA5 = { data9 } |
| OUT sA6 = { data15, data16 } |
| OUT sA7 = { data17, data18 } |
| OUT sA8 = { data20, data21 } |
| OUT sA9 = { data22, data23, data24 } |
| OUT sA11 = { data2 } |
| OUT sA12 = { data10 } |
| OUT sA21 = { data11 } |
| OUT sA22 = { data4, data12 } |
| OUT sA23 = { data5 } |
| OUT sA31 = { data6 } |
| OUT sA32 = { data7 } |
| OUT sA41 = { data3 } |
| OUT sA42 = { data8 } |
| OUT sA71 = { data17 } |
| OUT sA72 = { data18 } |
| OUT sA81 = { data20 } |
| OUT sA82 = { data21 } |
| OUT sA91 = { data22 } |
| OUT sA92 = { data23 } |
| OUT sA93 = { data24 } |
| OUT sS1 = { data10 } |
| OUT sS2 = { data2 } |
| OUT sS3 = { data11 } |
| OUT sS4 = { data5 } |
| OUT sS5 = { data7 } |
| OUT sS6 = { data12 } |
| OUT sS7 = { data8 } |
| OUT sS8 = { data9 } |
| OUT sS9 = { data15, data16 } |
| OUT sS10 = { data17 } |
| OUT sS11 = { data18 } |
| OUT sS12 = { data20 } |
| OUT sS13 = { data23 } |
| OUT sS14 = { data21 } |
| OUT sS15 = { data24 } |
| OUT sS1opt = { data2, data10 } |
| OUT sS4opt = { data12 } |
| OUT sS7opt = { data9 } |
| OUT sS11opt = { data24 } |

-- function VAR maps component IDs to the set of its local variables

fun VAR :: CSet ⇒ varID set

where

  VAR sA1 = { stA1 }
  | VAR sA2 = { stA2 }
VAR sA3 = {}
VAR sA4 = { stA4 }
VAR sA5 = {}
VAR sA6 = { stA6 }
VAR sA7 = {}
VAR sA8 = {}
VAR sA9 = {}
VAR sA11 = {}
VAR sA12 = { stA1 }
VAR sA21 = {}
VAR sA22 = { stA2 }
VAR sA23 = {}
VAR sA31 = {}
VAR sA32 = {}
VAR sA41 = { stA4 }
VAR sA42 = {}
VAR sA71 = {}
VAR sA72 = {}
VAR sA81 = {}
VAR sA82 = {}
VAR sA91 = {}
VAR sA92 = {}
VAR sA93 = {}
VAR sS1 = { stA1 }
VAR sS2 = {}
VAR sS3 = {}
VAR sS4 = {}
VAR sS5 = {}
VAR sS6 = { stA2, stA4 }
VAR sS7 = {}
VAR sS8 = {}
VAR sS9 = { stA6 }
VAR sS10 = {}
VAR sS11 = {}
VAR sS12 = {}
VAR sS13 = {}
VAR sS14 = {}
VAR sS15 = {}
VAR sS1opt = { stA1 }
VAR sS4opt = { stA2, stA4 }
VAR sS7opt = {}
VAR sS11opt = {}

— function subcomp maps component ID to the set of its subcomponents

fun subcomp :: CSet ⇒ CSet set
where
  subcomp sA1 = { sA11, sA12 }
  subcomp sA2 = { sA21, sA22, sA23 }
subcomp sA3 = { sA31, sA32 }
subcomp sA4 = { sA41, sA42 }
subcomp sA5 = {}
subcomp sA6 = {}
subcomp sA7 = { sA71, sA72 }
subcomp sA8 = { sA81, sA82 }
subcomp sA9 = { sA91, sA92, sA93 }
subcomp sA11 = {}
subcomp sA12 = {}
subcomp sA21 = {}
subcomp sA22 = {}
subcomp sA23 = {}
subcomp sA31 = {}
subcomp sA32 = {}
subcomp sA41 = {}
subcomp sA42 = {}
subcomp sA71 = {}
subcomp sA72 = {}
subcomp sA81 = {}
subcomp sA82 = {}
subcomp sA91 = {}
subcomp sA92 = {}
subcomp sA93 = {}
subcomp sS1 = { sA12 }
subcomp sS2 = { sA11 }
subcomp sS3 = { sA21 }
subcomp sS4 = { sA23 }
subcomp sS5 = { sA32 }
subcomp sS6 = { sA22, sA31, sA41 }
subcomp sS7 = { sA42 }
subcomp sS8 = { sA5 }
subcomp sS9 = { sA6 }
subcomp sS10 = { sA71 }
subcomp sS11 = { sA72 }
subcomp sS12 = { sA81, sA91 }
subcomp sS13 = { sA92 }
subcomp sS14 = { sA82 }
subcomp sS15 = { sA93 }
subcomp sS1opt = { sA11, sA12 }
subcomp sS4opt = { sA22, sA23, sA31, sA32, sA41 }
subcomp sS7opt = { sA42, sA5 }
subcomp sS11opt = { sA72, sA82, sA93 }

— function AbstrLevel maps abstraction level ID to the corresponding set of components

axiomatization
AbstrLevel :: AbstrLevelsID ⇒ CSet set

where
AbstrLevel0:
AbstrLevel level0 = \{ sA1, sA2, sA3, sA4, sA5, sA6, sA7, sA8, sA9 \}

and

AbstrLevel level1:
AbstrLevel level1 = \{ sA11, sA12, sA21, sA22, sA23, sA31, sA32, sA41, sA42, sA5, sA6, sA71, sA72, sA81, sA82, sA91, sA92, sA93 \}

and

AbstrLevel2:
AbstrLevel level2 = \{ sS1, sS2, sS3, sS4, sS5, sS6, sS7, sS8, sS9, sS10, sS11, sS12, sS13, sS14, sS15 \}

and

AbstrLevel3:
AbstrLevel level3 = \{ sS1opt, sS3, sS4opt, sS7opt, sS9, sS10, sS11opt, sS12, sS13 \}

— function VARfrom maps variable ID to the set of input channels it depends from

\textbf{fun} \ VARfrom :: \varID \Rightarrow \text{chanID set}
\textbf{where}
\quad \VARfrom \ stA1 = \{ data1 \}
\quad \VARfrom \ stA2 = \{ data3 \}
\quad \VARfrom \ stA4 = \{ data6, data7 \}
\quad \VARfrom \ stA6 = \{ data14 \}

— function VARto maps variable ID to the set of output channels depending from
this variable

\textbf{fun} \ VARto :: \varID \Rightarrow \text{chanID set}
\textbf{where}
\quad \VARto \ stA1 = \{ data10 \}
\quad \VARto \ stA2 = \{ data4, data12 \}
\quad \VARto \ stA4 = \{ data3 \}
\quad \VARto \ stA6 = \{ data15, data16 \}

— function OUTfromCh maps channel ID to the set of input channels
— from which it depends directly;
— an empty set means that the channel is either input of the system or
— its values are computed from local variables or are generated
— within some component independently

\textbf{fun} \ OUTfromCh :: \chanID \Rightarrow \text{chanID set}
\textbf{where}
\quad \OUTfromCh \ data1 = \{ \}
\quad \OUTfromCh \ data2 = \{ data1 \}
\quad \OUTfromCh \ data3 = \{ \}
\quad \OUTfromCh \ data4 = \{ data2 \}
\quad \OUTfromCh \ data5 = \{ data2 \}
\quad \OUTfromCh \ data6 = \{ data4 \}
\quad \OUTfromCh \ data7 = \{ data5 \}
\quad \OUTfromCh \ data8 = \{ data13 \}
\quad \OUTfromCh \ data9 = \{ data8 \}
\quad \OUTfromCh \ data10 = \{ \}
| OUTfromCh data11 = {data2} |
| OUTfromCh data12 = {} |
| OUTfromCh data13 = {} |
| OUTfromCh data14 = {} |
| OUTfromCh data15 = {} |
| OUTfromCh data16 = {} |
| OUTfromCh data17 = {data15} |
| OUTfromCh data18 = {data16} |
| OUTfromCh data19 = {} |
| OUTfromCh data20 = {data17, data22} |
| OUTfromCh data21 = {data18, data19} |
| OUTfromCh data22 = {data20} |
| OUTfromCh data23 = {data21} |
| OUTfromCh data24 = {} |

— function OUTfromV maps channel ID to the set of local variables it depends from

fun OUTfromV :: chanID ⇒ varID set

where

| OUTfromV data1 = {} |
| OUTfromV data2 = {} |
| OUTfromV data3 = {stA1} |
| OUTfromV data4 = {stA2} |
| OUTfromV data5 = {} |
| OUTfromV data6 = {} |
| OUTfromV data7 = {} |
| OUTfromV data8 = {} |
| OUTfromV data9 = {} |
| OUTfromV data10 = {stA1} |
| OUTfromV data11 = {} |
| OUTfromV data12 = {stA2} |
| OUTfromV data13 = {} |
| OUTfromV data14 = {} |
| OUTfromV data15 = {stA6} |
| OUTfromV data16 = {stA6} |
| OUTfromV data17 = {} |
| OUTfromV data18 = {} |
| OUTfromV data19 = {} |
| OUTfromV data20 = {} |
| OUTfromV data21 = {} |
| OUTfromV data22 = {} |
| OUTfromV data23 = {} |
| OUTfromV data24 = {} |

— Set of channels channels which have UplSize measure greater than the predefined value HighLoad

definition

UplSizeHighLoad :: chanID set

where
UplSizeHighLoad \equiv \{data1, data4, data5, data6, data7, data8, data18, data21\}

— Set of components from the abstraction level 1 for which the Perf measure is
greater than the predefined value HighPerf

definition
HighPerfSet :: CSet set
where
HighPerfSet \equiv \{sA22, sA23, sA41, sA42, sA72, sA93\}

end

3 Inter-/Intracomponent dependencies

definition DataDependencies
imports DataDependenciesConcreteValues
begin
— component and its subcomponents should be defined on different abstraction
levels
definition correctCompositionDiffLevels :: CSet \Rightarrow bool
where
correctCompositionDiffLevels S \equiv
\forall C \in \text{subcomp } S. \forall i. S \in \text{AbstrLevel } i \rightarrow C \notin \text{AbstrLevel } i

— General system’s property: for all abstraction levels and all components should
hold
— component and its subcomponents should be defined on different abstraction
levels
definition correctCompositionDiffLevelsSYSTEM :: bool
where
correctCompositionDiffLevelsSYSTEM \equiv
(\forall S::CSet. (correctCompositionDiffLevelsSYSTEM S))

— if a local variable belongs to one of the subcomponents, it also belongs to the
composed component
definition correctCompositionVAR :: CSet \Rightarrow bool
where
correctCompositionVAR S \equiv
\forall C \in \text{subcomp } S. \forall v \in \text{VAR } C. v \in \text{VAR } S

— General system’s property: for all abstraction levels and all components should
hold
— if a local variable belongs to one of the subcomponents, it also belongs to the
composed component

definition correctCompositionVARSYSTEM :: bool
where  
\[ \text{correctCompositionVARSYSTEM} \equiv \forall S :: \text{CSet}. \ (\text{correctCompositionVAR} \ S) \]

— after correct decomposition of a component each of its local variable can belong only to one of its subcomponents

definition  
\[ \text{correctDeCompositionVAR} :: \text{CSet} \Rightarrow \text{bool} \]
where  
\[ \text{correctDeCompositionVAR} \ S \equiv \forall v \in \text{VAR} \ S. \ \forall C1 \in \text{subcomp} \ S. \forall C2 \in \text{subcomp} \ S. \ v \in \text{VAR} \ C1 \land v \in \text{VAR} \ C2 \rightarrow C1 = C2 \]

— General system’s property: for all abstraction levels and all components should hold

— after correct decomposition of a component each of its local variable can belong only to one of its subcomponents

definition  
\[ \text{correctDeCompositionVARSYSTEM} :: \text{bool} \]
where  
\[ \text{correctDeCompositionVARSYSTEM} \equiv (\forall S :: \text{CSet}. \ (\text{correctDeCompositionVAR} \ S)) \]

— if x is an output channel of a component C on some abstraction level, it cannot be an output of another component on the same level

definition  
\[ \text{correctCompositionOUT} :: \text{chanID} \Rightarrow \text{bool} \]
where  
\[ \text{correctCompositionOUT} \ x \equiv \forall C i. \ x \in \text{OUT} \ C \land C \in \text{AbstrLevel} \ i \rightarrow (\forall S \in \text{AbstrLevel} \ i. \ x \not\in \text{OUT} \ S) \]

— General system’s property: for all abstraction levels and all channels should hold

definition  
\[ \text{correctCompositionOUTSYSTEM} :: \text{bool} \]
where  
\[ \text{correctCompositionOUTSYSTEM} \equiv (\forall x. \ \text{correctCompositionOUT} \ x) \]

— if X is a subcomponent of a component C on some abstraction level, it cannot be a subcomponent of another component on the same level

definition  
\[ \text{correctCompositionSubcomp} :: \text{CSet} \Rightarrow \text{bool} \]
where  
\[ \text{correctCompositionSubcomp} \ X \equiv \forall C i. \ X \in \text{subcomp} \ C \land C \in \text{AbstrLevel} \ i \rightarrow (\forall S \in \text{AbstrLevel} \ i. \ (S \neq C \rightarrow X \not\in \text{subcomp} \ S)) \]

— General system’s property: for all abstraction levels and all components should hold
definition
correctCompositionSubcompSYSTEM :: bool
where
  correctCompositionSubcompSYSTEM ≡ (∀ X. correctCompositionSubcomp X)

— If a component belongs is defined in the set CSet, it should belong to at least
one abstraction level
definition
allComponentsUsed :: bool
where
  allComponentsUsed ≡ ∀ C. ∃ i. C ∈ AbstrLevel i

— If a component does not have any local variables, none of its subcomponents has
any local variables
lemma correctDeCompositionVARempty:
  assumes correctCompositionVAR S
  and VAR S = {}
  shows ∀ C ∈ subcomp S. VAR C = {}
  ⟨proof⟩
  definition OUTfrom :: chanID ⇒ chanID set
  where
    OUTfrom x ≡ (OUTfromCh x) ∪ { y. ∃ v. v ∈ (OUTfromV x) ∧ y ∈ (VARfrom v) }

— If x depends from some input channel(s) directly, then exists
— A component which has them as input channels and x as an output channel
definition
  OUTfromChCorrect :: chanID ⇒ bool
  where
    OUTfromChCorrect x ≡
      (OUTfromCh x ≠ {} →
       (∃ Z . (x ∈ (OUT Z) ∧ (∀ y ∈ (OUTfromCh x). y ∈ IN Z )))

— General system’s property: for channels in the system should hold:
— If x depends from some input channel(s) directly, then exists
— A component which has them as input channels and x as an output channel
definition
  OUTfromChCorrectSYSTEM :: bool
  where
    OUTfromChCorrectSYSTEM ≡ (∀ x::chanID. (OUTfromChCorrect x))

— If x depends from some local variables, then exists a component
— To which these variables belong and which has x as an output channel
definition
  OUTfromVCorrect1 :: chanID ⇒ bool
  where
    OUTfromVCorrect1 x ≡
      (OUTfromV x ≠ {} →
\[
\exists Z . \ (x \in (OUT \ Z) \land (\forall \ v \in (OUTfromV \ x). \ v \in \VAR \ Z))
\]

— General system’s property: for channels in the system should hold the above property:
definition
\(OUTfromVCorrect1SYSTEM :: \text{bool}\)
where
\(OUTfromVCorrect1SYSTEM \equiv (\forall \ x::\CHAN. \ (OUTfromVCorrect1 \ x))\)

— if \(x\) does not depend from any local variables, then it does not belong to any set \VARfrom

definition
\(OUTfromVCorrect2 :: \CHAN \Rightarrow \text{bool}\)
where
\(\begin{align*}
\text{OUTfromVCorrect2 } x \equiv \\
(OOUTfromV \ x = \{} \longrightarrow (\forall \ v::\VARID. \ x \notin (\VARto \ v))
\end{align*}\)

— General system’s property: for channels in the system should hold the above property:
definition
\(OUTfromVCorrect2SYSTEM :: \text{bool}\)
where
\(\begin{align*}
\text{OUTfromVCorrect2SYSTEM } \equiv \\
(\forall \ x::\CHAN. \ (OUTfromVCorrect2 \ x))
\end{align*}\)

— General system’s property:
— definitions \(\text{OUTfromV}\) and \(\VARto\) should give equivalent mappings
definition
\(OUTfromV-VARto :: \text{bool}\)
where
\(\begin{align*}
\text{OUTfromV-VARto } \equiv \\
(\forall \ x::\CHAN. \ (v::\VARID. \ (v \in \VARfrom \ x \iff x \in (\VARto \ v))))
\end{align*}\)

— General system’s property for abstraction levels 0 and 1
— if a variable \(v\) belongs to a component, then all the channels \(v\)
— depends from should be input channels of this component
definition
\VARfromCorrectSYSTEM :: \text{bool}\)
where
\(\begin{align*}
\VARfromCorrectSYSTEM \equiv \\
(\forall \ v::\VARID. \ (\forall \ Z \in ((\text{AbstrLevel level0}) \cup (\text{AbstrLevel level1})). \ (v \in \VAR Z) \longrightarrow (\forall \ x \in \VARfrom \ v. \ x \in \IN \ Z)))
\end{align*}\)

— General system’s property for abstraction levels 0 and 1
— if a variable \(v\) belongs to a component, then all the channels \(v\)
— provides value to should be input channels of this component
definition
\VARtoCorrectSYSTEM :: \text{bool}\)
where
\(\begin{align*}
\VARtoCorrectSYSTEM \equiv \\
\end{align*}\)
\[(\forall \ v::\text{varID}, \ \forall \ Z \in ((\text{AbstrLevel level0}) \cup (\text{AbstrLevel level1})). (\ v \in \text{VAR} Z \rightarrow (\forall \ x \in \text{VARto} \ v. \ x \in \text{OUT} Z)))\]

— to detect local variables, unused for computation of any output

**definition**

\[\text{VARusefulSYSTEM} :: \text{bool}\]

**where**

\[\text{VARusefulSYSTEM} \equiv (\forall \ v::\text{varID}. (\text{VARto} \ v \neq \{\}))\]

**lemma**

\[\text{OUTfromV-VARto-lemma:}\]

**assumes** \[\text{OUTfromV} \ x \neq \{\} \text{ and OUTfromV-VARto}\]

**shows** \[\exists \ v::\text{varID}. \ x \in (\text{VARto} \ v)\]

**⟨proof⟩**

3.1 Direct and indirect data dependencies between components

— The component C should be defined on the same abstraction
— level we are searching for its direct or indirect sources,
— otherwise we get an empty set as result

**definition**

\[\text{DSources} :: \text{AbstrLevelsID} \Rightarrow \text{CSet} \Rightarrow \text{CSet set}\]

**where**

\[\text{DSources} \ i \ C \equiv \{Z. \ \exists \ x. \ x \in (\text{IN} C) \wedge x \in (\text{OUT} Z) \wedge Z \in (\text{AbstrLevel} i) \wedge C \in (\text{AbstrLevel} i)\}\]

**lemma** \[\text{DSourcesLevelX}:\]

\[(\text{DSources} \ i \ X) \subseteq (\text{AbstrLevel} i)\]

**⟨proof⟩**

**definition**

\[\text{DAcc} :: \text{AbstrLevelsID} \Rightarrow \text{CSet} \Rightarrow \text{CSet set}\]

**where**

\[\text{DAcc} \ i \ C \equiv \{Z. \ \exists \ x. \ x \in (\text{OUT} C) \wedge x \in (\text{IN} Z) \wedge Z \in (\text{AbstrLevel} i) \wedge C \in (\text{AbstrLevel} i)\}\]

**axiomatization**

\[\text{Sources} :: \text{AbstrLevelsID} \Rightarrow \text{CSet} \Rightarrow \text{CSet set}\]

**where**

\[\text{SourcesDef}:\]

\[(\text{Sources} \ i \ C) = (\text{DSources} \ i \ C) \cup (\bigcup S \in (\text{Sources} \ i \ C). (\text{Sources} \ i \ S))\]

**and**

\[\text{SourceExistsDSource}:\]

\[S \in (\text{Sources} \ i \ C) \rightarrow (\exists \ Z. \ S \in (\text{Sources} \ i \ Z))\]

**and**

\[\text{NDSourceExistsDSource}:\]

\[S \in (\text{Sources} \ i \ C) \wedge S \notin (\text{Sources} \ i \ C) \rightarrow (\exists \ Z. \ S \in (\text{Sources} \ i \ Z) \wedge Z \in (\text{Sources} \ i \ C))\]

**and**

18
SourcesTrans:
\[(C \in \text{Sources } i S \land S \in \text{Sources } i Z) \rightarrow C \in \text{Sources } i Z\]
and
SourcesLevelX:
\[(\text{Sources } i X) \subseteq (\text{AbstrLevel } i)\]
and
SourcesLoop:
\[(\text{Sources } i C) = (X S \cup (\text{Sources } i S)) \land (\text{Sources } i S) = (Z S \cup (\text{Sources } i C))
\rightarrow (\text{Sources } i C) = X S \cup Z S \cup \{ C, S \}\]
— if we have a loop in the dependencies we need to cut it for counting the sources

axiomatization
\[\text{Acc } :: \text{AbstrLevelsID } \Rightarrow \text{CSet } \Rightarrow \text{CSet set}\]
where
\[\text{AccDef}: (\text{Acc } i C) = (\text{DAcc } i C) \cup (\bigcup S \in (\text{DAcc } i C). (\text{Acc } i S))\]
and
\[\text{Acc-Sources}: (X \in \text{Acc } i C) = (C \in \text{Sources } i X)\]
and
\[\text{Acc-SingleLoop}: (\text{DAcc } i C) = \{ S \} \land (\text{DAcc } i S) = \{ C \} \rightarrow \text{Acc } i C = \{ C, S \}\]
and
\[\text{AccLoop}: (\text{Acc } i C) = (X S \cup (\text{Acc } i S)) \land (\text{Acc } i S) = (Z S \cup (\text{Acc } i C))
\rightarrow (\text{Acc } i C) = X S \cup Z S \cup \{ C, S \}\]
— if we have a loop in the dependencies we need to cut it for counting the accessors

lemma Acc-SourcesNOT: \((X \notin \text{Acc } i C) = (C \notin \text{Sources } i X)\)
(proof)
definition isNotDSource :: AbstrLevelsID \Rightarrow \text{CSet } \Rightarrow \text{bool}
where
\[\text{isNotDSource } i S C \equiv (\forall x \in (\text{OUT } S). (\forall Z \in (\text{AbstrLevel } i). (x \notin (\text{IN } Z))))\]
— component S is not a source for a component Z on the abstraction level i
definition isNotDSourceX :: AbstrLevelsID \Rightarrow \text{CSet } \Rightarrow \text{CSet } \Rightarrow \text{bool}
where
\[\text{isNotDSourceX } i S C \equiv (\forall x \in (\text{OUT } S). (C \notin (\text{AbstrLevel } i) \land (x \notin (\text{IN } C))))\]
lemma isNotSource-isNotSourceX:
isNotDSource i S C \equiv (\forall C. \text{isNotDSourceX } i S C)
(proof)

lemma DAcc-DSources:
\((X \in \text{DAcc } i C) = (C \in \text{DSources } i X)\)
(proof)
lemma \textit{DAcc-DSourcesNOT}:
\[(X \notin \text{DAcc}_i C) = (C \notin \text{DSources}_i X)\]
\(\langle\text{proof}\rangle\)

lemma \textit{DSource-level}:
\begin{itemize}
  \item \textbf{assumes} \(S \in (\text{DSources}_i C)\)
  \item \textbf{shows} \(C \in (\text{AbstrLevel}_i)\)
\end{itemize}
\(\langle\text{proof}\rangle\)

lemma \textit{SourceExistsDSource-level}:
\begin{itemize}
  \item \textbf{assumes} \(S \in (\text{Sources}_i C)\)
  \item \textbf{shows} \(\exists Z \in (\text{AbstrLevel}_i). (S \in (\text{DSources}_i Z))\)
\end{itemize}
\(\langle\text{proof}\rangle\)

lemma \textit{Sources-DSources}:
\[(\text{DSources}_i C) \subseteq (\text{Sources}_i C)\]
\(\langle\text{proof}\rangle\)

lemma \textit{NoDSource-NoSource}:
\begin{itemize}
  \item \textbf{assumes} \(S \notin (\text{Sources}_i C)\)
  \item \textbf{shows} \(S \notin (\text{DSources}_i C)\)
\end{itemize}
\(\langle\text{proof}\rangle\)

lemma \textit{DSourcesEmptySources}:
\begin{itemize}
  \item \textbf{assumes} \(\text{DSources}_i C = \{\}\)
  \item \textbf{shows} \(\text{Sources}_i C = \{\}\)
\end{itemize}
\(\langle\text{proof}\rangle\)

lemma \textit{DSource-Sources}:
\begin{itemize}
  \item \textbf{assumes} \(S \in (\text{DSources}_i C)\)
  \item \textbf{shows} \((\text{Sources}_i S) \subseteq (\text{Sources}_i C)\)
\end{itemize}
\(\langle\text{proof}\rangle\)

lemma \textit{SourcesOnlyDSources}:
\begin{itemize}
  \item \textbf{assumes} \(\forall X . (X \in (\text{DSources}_i C) \rightarrow (\text{DSources}_i X) = \{\})\)
  \item \textbf{shows} \(\text{Sources}_i C = \text{DSources}_i C\)
\end{itemize}
\(\langle\text{proof}\rangle\)

lemma \textit{SourcesEmptyDSources}:
\begin{itemize}
  \item \textbf{assumes} \(\text{Sources}_i C = \{\}\)
  \item \textbf{shows} \(\text{DSources}_i C = \{\}\)
\end{itemize}
\(\langle\text{proof}\rangle\)

lemma \textit{NotDSource}:
\begin{itemize}
  \item \textbf{assumes} \(\forall x \in (\text{OUT} S). (\forall Z \in \text{AbstrLevel}_i . (x \notin (\text{IN} Z)))\)
  \item \textbf{shows} \(\forall C \in \text{AbstrLevel}_i . S \notin (\text{DSources}_i C)\)
\end{itemize}
\(\langle\text{proof}\rangle\)
lemma allNotDSource-NotSource:
assumes \( \forall C. S \not\in (D\text{Sources}\ i\ C) \)
shows \( \forall Z. S \not\in (\text{Sources}\ i\ Z) \)
(proof)

lemma NotDSource-NotSource:
assumes \( \forall C \in (\text{AbstrLevel}\ i). S \not\in (D\text{Sources}\ i\ C) \)
shows \( \forall Z \in (\text{AbstrLevel}\ i). S \not\in (\text{Sources}\ i\ Z) \)
(proof)

lemma isNotSource-Sources:
assumes isNotDSource i S
shows \( \forall C \in (\text{AbstrLevel}\ i). S \not\in (\text{Sources}\ i\ C) \)
(proof)

lemma SourcesAbstrLevel:
assumes \( x \in \text{Sources}\ i\ S \)
shows \( x \in \text{AbstrLevel}\ i \)
(proof)

lemma DSourceIsSource:
assumes \( C \in D\text{Sources}\ i\ S \)
shows \( C \in \text{Sources}\ i\ S \)
(proof)

lemma DSourceOfDSource:
assumes \( Z \in D\text{Sources}\ i\ S \)
and \( S \in D\text{Sources}\ i\ C \)
shows \( Z \in \text{Sources}\ i\ C \)
(proof)

lemma SourceOfDSource:
assumes \( Z \in \text{Sources}\ i\ S \)
and \( S \in D\text{Sources}\ i\ C \)
shows \( Z \in \text{Sources}\ i\ C \)
(proof)

lemma DSourceOfSource:
assumes \( cDS: C \in D\text{Sources}\ i\ S \)
and \( sS:S \in \text{Sources}\ i\ Z \)
shows \( C \in \text{Sources}\ i\ Z \)
(proof)

lemma Sources-singleDSource:
assumes \( D\text{Sources}\ i\ S = \{ C \} \)
shows \( \text{Sources}\ i\ S = \{ C \} \cup \text{Sources}\ i\ C \)
(proof)

lemma Sources-2DSources:
assumes $DSources \ i \ S = \{C_1, C_2\}$
shows $Sources \ i \ S = \{C_1, C_2\} \cup Sources \ i \ C_1 \cup Sources \ i \ C_2$
⟨proof⟩

lemma $Sources-3DSources$:
assumes $DSources \ i \ S = \{C_1, C_2, C_3\}$
shows $Sources \ i \ S = \{C_1, C_2, C_3\} \cup Sources \ i \ C_1 \cup Sources \ i \ C_2 \cup Sources \ i \ C_3$
⟨proof⟩

lemma $singleDSourceEmpty\_isNotDSource$:
assumes $DAcc \ i \ C = \{S\}$ and $Z \neq S$
shows $C \notin (DSources \ i \ Z)$
⟨proof⟩

lemma $singleDSourceEmpty\_isNotDSource\_Level$:
assumes $DAcc \ i \ C = \{S\}$
shows $\forall Z \in (Abstr\_Level \ i). Z \neq S \rightarrow \ C \notin (DSources \ i \ Z)$
⟨proof⟩

lemma $isNotDSource-EmptyDAcc$:
assumes $isNotDSource \ i \ S$
shows $DAcc \ i \ S = \{}$
⟨proof⟩

lemma $isNotDSource-EmptyAcc$:
assumes $isNotDSource \ i \ S$
shows $Acc \ i \ S = \{}$
⟨proof⟩

lemma $singleDSourceEmpty\_Acc$:
assumes $DAcc \ i \ C = \{S\}$ and $isNotDSource \ i \ S$
shows $Acc \ i \ C = \{S\}$
⟨proof⟩

lemma $singleDSourceEmpty\_isNotSource$:
assumes $DAcc \ i \ C = \{S\}$ and $nSources:isNotDSource \ i \ S$
and $Z \neq S$
shows $C \notin (Sources \ i \ Z)$
⟨proof⟩

lemma $singleDSourceEmpty\_isNotSource\_Level$:
assumes $DAcc \ i \ C = \{S\}$ and $nSources:isNotDSource \ i \ S$
shows $\forall Z \in (Abstr\_Level \ i). Z \neq S \rightarrow \ C \notin (Sources \ i \ Z)$
22
lemma singleDSourceLoop:
assumes DAcc i C = {S}
and DAcc i S = {C}
shows ∀ Z ∈ (AbstrLevel i). (Z ≠ S ∧ Z ≠ C → C ∉ (Sources i Z))
⟨proof⟩

3.2 Components that are elementary wrt. data dependencies
— two output channels of a component C are correlated, if they mutually depend on the same local variable(s)
definition outPairCorelated :: CSet ⇒ chanID ⇒ chanID ⇒ bool
where
outPairCorelated C x y ≡
(x ∈ OUT C) ∧ (y ∈ OUT C) ∧
(OUTfromV x) ∩ (OUTfromV y) ≠ {}
— We call a set of output channels of a component correlated to it output channel x, — if they mutually depend on the same local variable(s)
definition outSetCorelated :: chanID ⇒ chanID set
where
outSetCorelated x ≡
{ y::chanID . ∃ v::varID. (v ∈ (OUTfromV x) ∧ (y ∈ VARto v)) }
— Elementary component according to the data dependencies.
— This constraint should hold for all components on the abstraction level 1
definition elementaryCompDD :: CSet ⇒ bool
where
elementaryCompDD C ≡
((∃ x. (OUT C) = {x}) ∨
(∀ x ∈ (OUT C). ∀ y ∈ (OUT C). ((outSetCorelated x) ∩ (outSetCorelated y)
≠ {})))
— the set (outSetCorelated x) is empty if x does not depend from any variable
lemma outSetCorelatedEmpty1:
assumes OUTfromV x = {}
shows outSetCorelated x = {}
⟨proof⟩
lemma outSetCorelatedNonemptyX:
assumes OUTfromV x ≠ {} and correct3:OUTfromV-VARto
shows x ∈ outSetCorelated x
⟨proof⟩
lemma outSetCorelatedEmpty2:
assumes outSetCorelated x = {} and correct3: OUTfromV-VARto
shows OUTfromV x = {}

⟨proof⟩

3.3 Set of components needed to check a specific property
— set of components specified on abstraction level i, which input channels belong to the set chSet
definition inSetOfComponents :: AbstrLevelsID ⇒ chanID set ⇒ CSet set
where
inSetOfComponents i chSet ≡
{X. (((IN X) ∩ chSet ≠ {}) ∧ X ∈ (AbstrLevel i))}
— Set of components from the abstraction level i, which output channels belong to the set chSet
definition outSetOfComponents :: AbstrLevelsID ⇒ chanID set ⇒ CSet set
where
outSetOfComponents i chSet ≡
{Y. (((OUT Y) ∩ chSet ≠ {}) ∧ Y ∈ (AbstrLevel i))}
— Set of components from the abstraction level i,
— which have output channels from the set chSet or are sources for such components
definition minSetOfComponents :: AbstrLevelsID ⇒ chanID set ⇒ CSet set
where
minSetOfComponents i chSet ≡
(outSetOfComponents i chSet) ∪
(∪ S ∈ (outSetOfComponents i chSet). (Sources i S))
— Please note that a system output cannot beat the same time a local channel.
— channel x is a system input on an abstraction level i
definition systemIN :: chanID ⇒ AbstrLevelsID ⇒ bool
where
systemIN x i ≡ (∃ C1 ∈ (AbstrLevel i). x ∈ (IN C1)) ∧ (∀ C2 ∈ (AbstrLevel i). x ∉ (OUT C2))
— channel x is a system input on an abstraction level i
definition systemOUT :: chanID ⇒ AbstrLevelsID ⇒ bool
where
systemOUT x i ≡ (∀ C1 ∈ (AbstrLevel i). x ∉ (IN C1)) ∧ (∃ C2 ∈ (AbstrLevel i). x ∈ (OUT C2))
— channel x is a system local channel on an abstraction level i
definition systemLOC :: chanID ⇒ AbstrLevelsID ⇒ bool
where

\[ \text{systemLOC } x \ i \equiv (\exists \ C1 \in (\text{AbstrLevel } i). \ x \in (\text{IN } C1)) \land (\exists \ C2 \in (\text{AbstrLevel } i). \ x \in (\text{OUT } C2)) \]

lemma systemIN-noOUT:
  assumes systemIN \ x \ i
  shows \ \neg \ \text{systemOUT } x \ i
  ⟨proof⟩

lemma systemOUT-noIN:
  assumes systemOUT \ x \ i
  shows \ \neg \ \text{systemIN } x \ i
  ⟨proof⟩

lemma systemIN-noLOC:
  assumes systemIN \ x \ i
  shows \ \neg \ \text{systemLOC } x \ i
  ⟨proof⟩

lemma systemLOC-noIN:
  assumes systemLOC \ x \ i
  shows \ \neg \ \text{systemIN } x \ i
  ⟨proof⟩

lemma systemOUT-noLOC:
  assumes systemOUT \ x \ i
  shows \ \neg \ \text{systemLOC } x \ i
  ⟨proof⟩

lemma systemLOC-noOUT:
  assumes systemLOC \ x \ i
  shows \ \neg \ \text{systemOUT } x \ i
  ⟨proof⟩

definition
  noIrrelevantChannels :: AbstrLevelsID ⇒ chanID set ⇒ bool
  where
  noIrrelevantChannels \ i \ chSet ≡
  \forall \ x \in \ chSet. ((\text{systemIN } x \ i) \rightarrow
  (\exists \ Z \in (\text{minSetOfComponents } i \ chSet). \ x \in (\text{IN } Z)))

definition
  allNeededINChannels :: AbstrLevelsID ⇒ chanID set ⇒ bool
  where
  allNeededINChannels \ i \ chSet ≡
  (\forall \ Z \in (\text{minSetOfComponents } i \ chSet). \ x \in (\text{IN } Z). ((\text{systemIN } x \ i) \rightarrow (x \in \ chSet)))
— the set \((\text{outSetOfComponents } i \text{ chSet})\) should be a subset of all components specified on the abstraction level \(i\)

**lemma** \(\text{outSetOfComponentsLimit}\):

\[\text{outSetOfComponents } i \text{ chSet} \subseteq \text{AbstrLevel } i\]

**proof**

**lemma** \(\text{inSetOfComponentsLimit}\):

\[\text{inSetOfComponents } i \text{ chSet} \subseteq \text{AbstrLevel } i\]

**proof**

**lemma** \(\text{SourcesLevelLimit}\):

\[\left(\bigcup S \in (\text{outSetOfComponents } i \text{ chSet}), (\text{Sources } i S)\right) \subseteq \text{AbstrLevel } i\]

**proof**

**lemma** \(\text{minSetOfComponentsLimit}\):

\[\text{minSetOfComponents } i \text{ chSet} \subseteq \text{AbstrLevel } i\]

**proof**

### 3.4 Additional properties: Remote Computation

— The value of \(UplSizeHighLoad x\) is True if its \(UplSize\) measure is greater than a predefined value

**definition** \(UplSizeHighLoadCh :: \text{chanID } \Rightarrow \text{bool}\)

**where**

\[UplSizeHighLoadCh x \equiv (x \in UplSizeHighLoad)\]

— if the \(Perf\) measure of at least one subcomponent is greater than a predefined value,

— the \(Perf\) measure of this component is greater than \(HighPerf\) too

**axiomatization** \(HighPerfComp :: \text{CSet } \Rightarrow \text{bool}\)

**where**

\[HighPerfComDef:\]

\[HighPerfComp C =\]

\[\left(((C \in \text{HighPerfSet}) \lor (\exists Z \in \text{subcomp } C, \text{HighPerfComp } Z))\right)\]

end

### 4 Case Study: Verification of Properties

**theory** DataDependenciesCaseStudy

**imports** DataDependencies

**begin**

#### 4.1 Correct composition of components

— the lemmas \(\text{AbstrLevels } X Y\) with corresponding proofs can be composable

— and proven automatically, their proofs are identical

**lemma** \(\text{AbstrLevels-A1-A11}\):

**assumes** \(sA1 \in \text{AbstrLevel } i\)

**shows** \(sA1 \notin \text{AbstrLevel } i\)

**proof**
lemma AbstrLevels-A1-A12: 
assumes $sA1 \in \text{AbstrLevel } i$
shows $sA12 \notin \text{AbstrLevel } i$ 
⟨proof⟩

lemma AbstrLevels-A2-A21: 
assumes $sA2 \in \text{AbstrLevel } i$
shows $sA21 \notin \text{AbstrLevel } i$ 
⟨proof⟩

lemma AbstrLevels-A2-A22: 
assumes $sA2 \in \text{AbstrLevel } i$
shows $sA22 \notin \text{AbstrLevel } i$ 
⟨proof⟩

lemma AbstrLevels-A2-A23: 
assumes $sA2 \in \text{AbstrLevel } i$
shows $sA23 \notin \text{AbstrLevel } i$ 
⟨proof⟩

lemma AbstrLevels-A3-A31: 
assumes $sA3 \in \text{AbstrLevel } i$
shows $sA31 \notin \text{AbstrLevel } i$ 
⟨proof⟩

lemma AbstrLevels-A3-A32: 
assumes $sA3 \in \text{AbstrLevel } i$
shows $sA32 \notin \text{AbstrLevel } i$ 
⟨proof⟩

lemma AbstrLevels-A4-A41: 
assumes $sA4 \in \text{AbstrLevel } i$
shows $sA41 \notin \text{AbstrLevel } i$ 
⟨proof⟩

lemma AbstrLevels-A4-A42: 
assumes $sA4 \in \text{AbstrLevel } i$
shows $sA42 \notin \text{AbstrLevel } i$ 
⟨proof⟩

lemma AbstrLevels-A7-A71: 
assumes $sA7 \in \text{AbstrLevel } i$
shows $sA71 \notin \text{AbstrLevel } i$ 
⟨proof⟩

lemma AbstrLevels-A7-A72: 
assumes $sA7 \in \text{AbstrLevel } i$
shows $sA72 \notin \text{AbstrLevel } i$ 
⟨proof⟩

lemma AbstrLevels-A8-A81: 
assumes $sA8 \in \text{AbstrLevel } i$
shows $sA81 \notin \text{AbstrLevel } i$ 
⟨proof⟩

lemma AbstrLevels-A8-A82: 
assumes $sA8 \in \text{AbstrLevel } i$
shows $sA82 \notin \text{AbstrLevel } i$ 
⟨proof⟩

lemma AbstrLevels-A9-A91: 
assumes $sA9 \in \text{AbstrLevel } i$
shows \( sA9 \notin AbstrLevel\ i \)

**lemma AbstrLevels-A9-A92:**
assumes \( \ sA9 \in AbstrLevel\ i \)
shows \( sA92 \notin AbstrLevel\ i \)

**lemma AbstrLevels-A9-A93:**
assumes \( \ sA9 \in AbstrLevel\ i \)
shows \( sA93 \notin AbstrLevel\ i \)

**lemma AbstrLevels-S1-A12:**
assumes \( \ sS1 \in AbstrLevel\ i \)
shows \( sA12 \notin AbstrLevel\ i \)

**lemma AbstrLevels-S2-A11:**
assumes \( \ sS2 \in AbstrLevel\ i \)
shows \( sA11 \notin AbstrLevel\ i \)

**lemma AbstrLevels-S3-A21:**
assumes \( \ sS3 \in AbstrLevel\ i \)
shows \( sA21 \notin AbstrLevel\ i \)

**lemma AbstrLevels-S4-A23:**
assumes \( \ sS4 \in AbstrLevel\ i \)
shows \( sA23 \notin AbstrLevel\ i \)

**lemma AbstrLevels-S5-A32:**
assumes \( \ sS5 \in AbstrLevel\ i \)
shows \( sA32 \notin AbstrLevel\ i \)

**lemma AbstrLevels-S6-A22:**
assumes \( \ sS6 \in AbstrLevel\ i \)
shows \( sA22 \notin AbstrLevel\ i \)

**lemma AbstrLevels-S6-A31:**
assumes \( \ sS6 \in AbstrLevel\ i \)
shows \( sA31 \notin AbstrLevel\ i \)

**lemma AbstrLevels-S6-A41:**
assumes \( \ sS6 \in AbstrLevel\ i \)
shows \( sA41 \notin AbstrLevel\ i \)

**lemma AbstrLevels-S7-A42:**
assumes \( \ sS7 \in AbstrLevel\ i \)
shows \( sA42 \notin AbstrLevel\ i \)

**lemma AbstrLevels-S8-A5:**
assumes \( \ sS8 \in AbstrLevel\ i \)
shows \( sA5 \notin AbstrLevel\ i \)
lemma AbstrLevels-S9-A6:
  assumes \( sS9 \in \text{AbstrLevel } i \)
  shows \( sA6 \not\in \text{AbstrLevel } i \) (proof)

lemma AbstrLevels-S10-A71:
  assumes \( sS10 \in \text{AbstrLevel } i \)
  shows \( sA71 \not\in \text{AbstrLevel } i \) (proof)

lemma AbstrLevels-S11-A72:
  assumes \( sS11 \in \text{AbstrLevel } i \)
  shows \( sA72 \not\in \text{AbstrLevel } i \) (proof)

lemma AbstrLevels-S12-A81:
  assumes \( sS12 \in \text{AbstrLevel } i \)
  shows \( sA81 \not\in \text{AbstrLevel } i \) (proof)

lemma AbstrLevels-S12-A91:
  assumes \( sS12 \in \text{AbstrLevel } i \)
  shows \( sA91 \not\in \text{AbstrLevel } i \) (proof)

lemma AbstrLevels-S13-A92:
  assumes \( sS13 \in \text{AbstrLevel } i \)
  shows \( sA92 \not\in \text{AbstrLevel } i \) (proof)

lemma AbstrLevels-S14-A82:
  assumes \( sS14 \in \text{AbstrLevel } i \)
  shows \( sA82 \not\in \text{AbstrLevel } i \) (proof)

lemma AbstrLevels-S15-A93:
  assumes \( sS15 \in \text{AbstrLevel } i \)
  shows \( sA93 \not\in \text{AbstrLevel } i \) (proof)

lemma AbstrLevels-S1opt-A11:
  assumes \( sS1opt \in \text{AbstrLevel } i \)
  shows \( sA11 \not\in \text{AbstrLevel } i \) (proof)

lemma AbstrLevels-S1opt-A12:
  assumes \( sS1opt \in \text{AbstrLevel } i \)
  shows \( sA12 \not\in \text{AbstrLevel } i \) (proof)

lemma AbstrLevels-S1opt-A23:
  assumes \( sS1opt \in \text{AbstrLevel } i \)
  shows \( sA23 \not\in \text{AbstrLevel } i \) (proof)

lemma AbstrLevels-S1opt-A32:
  assumes \( sS1opt \in \text{AbstrLevel } i \)
  shows \( sA32 \not\in \text{AbstrLevel } i \) (proof)
lemma AbstrLevels-S4opt-A22:
assumes $s_{4\text{opt}} \in \text{AbstrLevel}_i$
shows $s_{22} \notin \text{AbstrLevel}_i$(proof)

lemma AbstrLevels-S4opt-A31:
assumes $s_{4\text{opt}} \in \text{AbstrLevel}_i$
shows $s_{31} \notin \text{AbstrLevel}_i$(proof)

lemma AbstrLevels-S4opt-A41:
assumes $s_{4\text{opt}} \in \text{AbstrLevel}_i$
shows $s_{41} \notin \text{AbstrLevel}_i$(proof)

lemma AbstrLevels-S7opt-A42:
assumes $s_{7\text{opt}} \in \text{AbstrLevel}_i$
shows $s_{42} \notin \text{AbstrLevel}_i$(proof)

lemma AbstrLevels-S7opt-A5:
assumes $s_{7\text{opt}} \in \text{AbstrLevel}_i$
shows $s_{5} \notin \text{AbstrLevel}_i$(proof)

lemma AbstrLevels-S11opt-A72:
assumes $s_{11\text{opt}} \in \text{AbstrLevel}_i$
shows $s_{72} \notin \text{AbstrLevel}_i$(proof)

lemma AbstrLevels-S11opt-A82:
assumes $s_{11\text{opt}} \in \text{AbstrLevel}_i$
shows $s_{82} \notin \text{AbstrLevel}_i$(proof)

lemma AbstrLevels-S11opt-A93:
assumes $s_{11\text{opt}} \in \text{AbstrLevel}_i$
shows $s_{93} \notin \text{AbstrLevel}_i$(proof)

lemma correctCompositionDiffLevelsA1: correctCompositionDiffLevels sA1(proof)
lemma correctCompositionDiffLevelsA2: correctCompositionDiffLevels sA2(proof)
lemma correctCompositionDiffLevelsA3: correctCompositionDiffLevels sA3(proof)
lemma correctCompositionDiffLevelsA4: correctCompositionDiffLevels sA4(proof)
lemma correctCompositionDiffLevelsA5: correctCompositionDiffLevels sA5(proof)
lemma correctCompositionDiffLevelsA6: correctCompositionDiffLevels sA6(proof)
lemma correctCompositionDiffLevelsA7: correctCompositionDiffLevels sA7(proof)
lemma correctCompositionDiffLevelsA8: correctCompositionDiffLevels sA8(proof)
lemma correctCompositionDiffLevelsA9: correctCompositionDiffLevels sA9(proof)
lemma correctCompositionDiffLevelsA11: correctCompositionDiffLevels sA11(proof)
lemma correctCompositionDiffLevelsA12: correctCompositionDiffLevels sA12(proof)
lemma correctCompositionDiffLevelsA21: correctCompositionDiffLevels sA21(proof)
lemma correctCompositionDiffLevelsA22: correctCompositionDiffLevels sA22(proof)
4.2 Correct specification of the relations between channels

lemma \textit{OUTfromChCorrect-data1}: \textit{OUTfromChCorrect data1} (proof)

lemma \textit{OUTfromChCorrect-data2}: \textit{OUTfromChCorrect data2} (proof)
lemma OUTfromChCorrect-data3: OUTfromChCorrect data3
  ⟨proof⟩

lemma OUTfromChCorrect-data4: OUTfromChCorrect data4
  ⟨proof⟩

lemma OUTfromChCorrect-data5: OUTfromChCorrect data5
  ⟨proof⟩

lemma OUTfromChCorrect-data6: OUTfromChCorrect data6
  ⟨proof⟩

lemma OUTfromChCorrect-data7: OUTfromChCorrect data7
  ⟨proof⟩

lemma OUTfromChCorrect-data8: OUTfromChCorrect data8
  ⟨proof⟩

lemma OUTfromChCorrect-data9: OUTfromChCorrect data9
  ⟨proof⟩

lemma OUTfromChCorrect-data10: OUTfromChCorrect data10
  ⟨proof⟩

lemma OUTfromChCorrect-data11: OUTfromChCorrect data11
  ⟨proof⟩

lemma OUTfromChCorrect-data12: OUTfromChCorrect data12
  ⟨proof⟩

lemma OUTfromChCorrect-data13: OUTfromChCorrect data13
  ⟨proof⟩

lemma OUTfromChCorrect-data14: OUTfromChCorrect data14
  ⟨proof⟩

lemma OUTfromChCorrect-data15: OUTfromChCorrect data15
  ⟨proof⟩

lemma OUTfromChCorrect-data16: OUTfromChCorrect data16
  ⟨proof⟩

lemma OUTfromChCorrect-data17: OUTfromChCorrect data17
  ⟨proof⟩

lemma OUTfromChCorrect-data18: OUTfromChCorrect data18
  ⟨proof⟩
lemma OUTfromChCorrect-data19: OUTfromChCorrect data19 (proof)

lemma OUTfromChCorrect-data20: OUTfromChCorrect data20 (proof)

lemma OUTfromChCorrect-data21: OUTfromChCorrect data21 (proof)

lemma OUTfromChCorrect-data22: OUTfromChCorrect data22 (proof)

lemma OUTfromChCorrect-data23: OUTfromChCorrect data23 (proof)

lemma OUTfromChCorrect-data24: OUTfromChCorrect data24 (proof)

lemma OUTfromChCorrectSYSTEM-holds: OUTfromChCorrectSYSTEM (proof)

lemma OUTfromVCorrect1-data1: OUTfromVCorrect1 data1 (proof)

lemma OUTfromVCorrect1-data2: OUTfromVCorrect1 data2 (proof)

lemma OUTfromVCorrect1-data3: OUTfromVCorrect1 data3 (proof)

lemma OUTfromVCorrect1-data4: OUTfromVCorrect1 data4 (proof)

lemma OUTfromVCorrect1-data5: OUTfromVCorrect1 data5 (proof)

lemma OUTfromVCorrect1-data6: OUTfromVCorrect1 data6 (proof)

lemma OUTfromVCorrect1-data7: OUTfromVCorrect1 data7 (proof)

lemma OUTfromVCorrect1-data8: OUTfromVCorrect1 data8 (proof)

lemma OUTfromVCorrect1-data9: OUTfromVCorrect1 data9 (proof)

lemma OUTfromVCorrect1-data10: OUTfromVCorrect1 data10 (proof)
lemma OUTfromVCorrect1-data11: OUTfromVCorrect1 data11
(\text{proof})

lemma OUTfromVCorrect1-data12: OUTfromVCorrect1 data12
(\text{proof})

lemma OUTfromVCorrect1-data13: OUTfromVCorrect1 data13
(\text{proof})

lemma OUTfromVCorrect1-data14: OUTfromVCorrect1 data14
(\text{proof})

lemma OUTfromVCorrect1-data15: OUTfromVCorrect1 data15
(\text{proof})

lemma OUTfromVCorrect1-data16: OUTfromVCorrect1 data16
(\text{proof})

lemma OUTfromVCorrect1-data17: OUTfromVCorrect1 data17
(\text{proof})

lemma OUTfromVCorrect1-data18: OUTfromVCorrect1 data18
(\text{proof})

lemma OUTfromVCorrect1-data19: OUTfromVCorrect1 data19
(\text{proof})

lemma OUTfromVCorrect1-data20: OUTfromVCorrect1 data20
(\text{proof})

lemma OUTfromVCorrect1-data21: OUTfromVCorrect1 data21
(\text{proof})

lemma OUTfromVCorrect1-data22: OUTfromVCorrect1 data22
(\text{proof})

lemma OUTfromVCorrect1-data23: OUTfromVCorrect1 data23
(\text{proof})

lemma OUTfromVCorrect1-data24: OUTfromVCorrect1 data24
(\text{proof})

lemma OUTfromVCorrect1SYSTEM-holds: OUTfromVCorrect1SYSTEM
(\text{proof})

lemma OUTfromVCorrect2SYSTEM: OUTfromVCorrect2SYSTEM
(\text{proof})
lemma $\text{OUTfrom}V\text{-VARto-holds}$: 
$\text{OUTfrom}V\text{-VARto}$
⟨proof⟩

lemma $\text{VARfromCorrectSYSTEM-holds}$: 
$\text{VARfromCorrectSYSTEM}$
⟨proof⟩

lemma $\text{VARtoCorrectSYSTEM-holds}$: 
$\text{VARtoCorrectSYSTEM}$
⟨proof⟩

lemma $\text{VARusefulSYSTEM-holds}$: 
$\text{VARusefulSYSTEM}$
⟨proof⟩

4.3 Elementary components
— On the abstraction level 0 only the components sA5 and sA6 are elementary

lemma $\neg \text{elementaryCompDD-sA1}$: ¬ elementaryCompDD sA1
⟨proof⟩

lemma $\neg \text{elementaryCompDD-sA2}$: ¬ elementaryCompDD sA2
⟨proof⟩

lemma $\neg \text{elementaryCompDD-sA3}$: ¬ elementaryCompDD sA3
⟨proof⟩

lemma $\neg \text{elementaryCompDD-sA4}$: ¬ elementaryCompDD sA4
⟨proof⟩

lemma $\text{elementaryCompDD-sA5}$: elementaryCompDD sA5
⟨proof⟩

lemma $\text{elementaryCompDD-sA6}$: elementaryCompDD sA6
⟨proof⟩

lemma $\neg \text{elementaryCompDD-sA7}$: ¬ elementaryCompDD sA7
⟨proof⟩

lemma $\neg \text{elementaryCompDD-sA8}$: ¬ elementaryCompDD sA8
⟨proof⟩

lemma $\neg \text{elementaryCompDD-sA9}$: ¬ elementaryCompDD sA9
⟨proof⟩

lemma $\text{elementaryCompDD-sA11}$: elementaryCompDD sA11

35
lemma elementaryCompDD-sA12: elementaryCompDD sA12
 ⟨proof⟩
lemma elementaryCompDD-sA21: elementaryCompDD sA21
 ⟨proof⟩
lemma elementaryCompDD-sA22: elementaryCompDD sA22
 ⟨proof⟩
lemma elementaryCompDD-sA23: elementaryCompDD sA23
 ⟨proof⟩
lemma elementaryCompDD-sA31: elementaryCompDD sA31
 ⟨proof⟩
lemma elementaryCompDD-sA32: elementaryCompDD sA32
 ⟨proof⟩
lemma elementaryCompDD-sA41: elementaryCompDD sA41
 ⟨proof⟩
lemma elementaryCompDD-sA42: elementaryCompDD sA42
 ⟨proof⟩
lemma elementaryCompDD-sA71: elementaryCompDD sA71
 ⟨proof⟩
lemma elementaryCompDD-sA72: elementaryCompDD sA72
 ⟨proof⟩
lemma elementaryCompDD-sA81: elementaryCompDD sA81
 ⟨proof⟩
lemma elementaryCompDD-sA82: elementaryCompDD sA82
 ⟨proof⟩
lemma elementaryCompDD-sA91: elementaryCompDD sA91
 ⟨proof⟩
lemma elementaryCompDD-sA92: elementaryCompDD sA92
 ⟨proof⟩
lemma elementaryCompDD-sA93: elementaryCompDD sA93
 ⟨proof⟩
4.4 Source components
— Abstraction level 0

**lemma** \texttt{A5-NotDSource-level0}: \texttt{isNotDSource level0 sA5}
\begin{proof}
\end{proof}

**lemma** \texttt{DSourcesA1-L0}: \texttt{DSources level0 sA1 = \{\}}
\begin{proof}
\end{proof}

**lemma** \texttt{DSourcesA2-L0}: \texttt{DSources level0 sA2 = \{ sA1, sA4 \}}
\begin{proof}
\end{proof}

**lemma** \texttt{DSourcesA3-L0}: \texttt{DSources level0 sA3 = \{ sA2 \}}
\begin{proof}
\end{proof}

**lemma** \texttt{DSourcesA4-L0}: \texttt{DSources level0 sA4 = \{ sA3 \}}
\begin{proof}
\end{proof}

**lemma** \texttt{DSourcesA5-L0}: \texttt{DSources level0 sA5 = \{ sA4 \}}
\begin{proof}
\end{proof}

**lemma** \texttt{DSourcesA6-L0}: \texttt{DSources level0 sA6 = \{\}}
\begin{proof}
\end{proof}

**lemma** \texttt{DSourcesA7-L0}: \texttt{DSources level0 sA7 = \{sA6\}}
\begin{proof}
\end{proof}

**lemma** \texttt{DSourcesA8-L0}: \texttt{DSources level0 sA8 = \{sA7, sA9\}}
\begin{proof}
\end{proof}

**lemma** \texttt{DSourcesA9-L0}: \texttt{DSources level0 sA9 = \{sA8\}}
\begin{proof}
\end{proof}

**lemma** \texttt{A1-DAcc-level0}: \texttt{DAcc level0 sA1 = \{ sA2 \}}
\begin{proof}
\end{proof}

**lemma** \texttt{A2-DAcc-level0}: \texttt{DAcc level0 sA2 = \{ sA3 \}}
\begin{proof}
\end{proof}

**lemma** \texttt{A3-DAcc-level0}: \texttt{DAcc level0 sA3 = \{ sA4 \}}
\begin{proof}
\end{proof}

**lemma** \texttt{A4-DAcc-level0}: \texttt{DAcc level0 sA4 = \{ sA2, sA5 \}}
\begin{proof}
\end{proof}

**lemma** \texttt{A5-DAcc-level0}: \texttt{DAcc level0 sA5 = \{\}}
\begin{proof}
\end{proof}

**lemma** \texttt{A6-DAcc-level0}: \texttt{DAcc level0 sA6 = \{ sA7 \}}
\begin{proof}
\end{proof}
lemma A7-DAcc-level0: \( \text{DAcc level0 } sA7 = \{ sA8 \} \)

lemma A8-DAcc-level0: \( \text{DAcc level0 } sA8 = \{ sA9 \} \)

lemma A9-DAcc-level0: \( \text{DAcc level0 } sA9 = \{ sA8 \} \)

lemma A8-NSources:
\( \forall C \in (\text{AbstrLevel level0}). (C \neq sA9 \land C \neq sA8 \rightarrow sA8 \notin (\text{Sources level0 } C)) \)

lemma A9-NSources:
\( \forall C \in (\text{AbstrLevel level0}). (C \neq sA9 \land C \neq sA8 \rightarrow sA9 \notin (\text{Sources level0 } C)) \)

lemma A7-Acc:
\( (\text{Acc level0 } sA7) = \{sA8, sA9\} \)

lemma A7-NSources:
\( \forall C \in (\text{AbstrLevel level0}). (C \neq sA9 \land C \neq sA8 \rightarrow sA7 \notin (\text{Sources level0 } C)) \)

lemma A5-Acc: \( (\text{Acc level0 } sA5) = \{ \} \)

lemma A6-Acc:
\( (\text{Acc level0 } sA6) = \{sA7, sA8, sA9\} \)

lemma A6-NSources:
\( \forall C \in (\text{AbstrLevel level0}). (C \neq sA9 \land C \neq sA8 \land C \neq sA7 \rightarrow sA6 \notin (\text{Sources level0 } C)) \)

lemma SourcesA1-L0: \( \text{Sources level0 } sA1 = \{ \} \)

lemma SourcesA2-L0: \( \text{Sources level0 } sA2 = \{ sA1, sA2, sA3, sA4 \} \)

lemma SourcesA3-L0: \( \text{Sources level0 } sA3 = \{ sA1, sA2, sA3, sA4 \} \)

lemma SourcesA4-L0: \( \text{Sources level0 } sA4 = \{ sA1, sA2, sA3, sA4 \} \)
\[\text{lemma \ SourcesA5-L0: Sources level0 } sA5 = \{ sA1, sA2, sA3, sA4 \} \]
\[\text{lemma \ SourcesA6-L0: Sources level0 } sA6 = \{ \} \]
\[\text{lemma \ SourcesA7-L0: Sources level0 } sA7 = \{ sA6 \} \]
\[\text{lemma \ SourcesA8-L0: Sources level0 } sA8 = \{ sA6, sA7, sA8, sA9 \} \]
\[\text{lemma \ SourcesA9-L0: Sources level0 } sA9 = \{ sA6, sA7, sA8, sA9 \} \]
\[\text{lemma \ A12-NotSource-level1: isNotDSource level1 } sA12 \]
\[\text{lemma \ A21-NotSource-level1: isNotDSource level1 } sA21 \]
\[\text{lemma \ A5-NotSource-level1: isNotDSource level1 } sA5 \]
\[\text{lemma \ A92-NotSource-level1: isNotDSource level1 } sA92 \]
\[\text{lemma \ A93-NotSource-level1: isNotDSource level1 } sA93 \]
\[\text{lemma \ A11-DAcc-level1: DAcc level1 } sA11 = \{ sA21, sA22, sA23 \} \]
\[\text{lemma \ A12-DAcc-level1: DAcc level1 } sA12 = \{ \} \]
\[\text{lemma \ A21-DAcc-level1: DAcc level1 } sA21 = \{ \} \]
\[\text{lemma \ A22-DAcc-level1: DAcc level1 } sA22 = \{ sA31 \} \]
\[\text{lemma \ A23-DAcc-level1: DAcc level1 } sA23 = \{ sA32 \} \]
lemma $\text{A31-DAcc-level1}$: $\text{DAcc level1 } sA31 = \{sA41\}$
(proof)

lemma $\text{A32-DAcc-level1}$: $\text{DAcc level1 } sA32 = \{sA41\}$
(proof)

lemma $\text{A41-DAcc-level1}$: $\text{DAcc level1 } sA41 = \{sA22\}$
(proof)

lemma $\text{A42-DAcc-level1}$: $\text{DAcc level1 } sA42 = \{sA5\}$
(proof)

lemma $\text{A5-DAcc-level1}$: $\text{DAcc level1 } sA5 = \{\}$
(proof)

lemma $\text{A6-DAcc-level1}$: $\text{DAcc level1 } sA6 = \{sA71, sA72\}$
(proof)

lemma $\text{A71-DAcc-level1}$: $\text{DAcc level1 } sA71 = \{sA81\}$
(proof)

lemma $\text{A72-DAcc-level1}$: $\text{DAcc level1 } sA72 = \{sA82\}$
(proof)

lemma $\text{A81-DAcc-level1}$: $\text{DAcc level1 } sA81 = \{sA91, sA92\}$
(proof)

lemma $\text{A82-DAcc-level1}$: $\text{DAcc level1 } sA82 = \{sA93\}$
(proof)

lemma $\text{A91-DAcc-level1}$: $\text{DAcc level1 } sA91 = \{sA81\}$
(proof)

lemma $\text{A92-DAcc-level1}$: $\text{DAcc level1 } sA92 = \{\}$
(proof)

lemma $\text{A93-DAcc-level1}$: $\text{DAcc level1 } sA93 = \{\}$
(proof)

lemma $\text{A42-NSources-L1}$:
$\forall C \in (\text{AbstrLevel level1}). C \neq sA5 \rightarrow sA42 \notin (\text{Sources level1 } C)$
(proof)

lemma $\text{A5-NotSourceSet-level1}$:
$\forall C \in (\text{AbstrLevel level1}). sA5 \notin (\text{Sources level1 } C)$
(proof)

lemma $\text{A92-NotSourceSet-level1}$:
$\forall C \in (\text{AbstrLevel level1}). sA92 \notin (\text{Sources level1 } C)$
(proof)
\begin{proof}

\textbf{lemma} \textit{A.93-NotSourceSet-level1} :

\[\forall\ C \in (\text{AbstrLevel level1}).\ sA93 \notin (\text{Sources level1} C)\]

\(\text{(proof)}\)

\textbf{lemma} \textit{DSourcesA11-L1} : \textit{DSources level1 sA11} = \{\}

\(\text{(proof)}\)

\textbf{lemma} \textit{DSourcesA12-L1} : \textit{DSources level1 sA12} = \{\}

\(\text{(proof)}\)

\textbf{lemma} \textit{DSourcesA21-L1} : \textit{DSources level1 sA21} = \{sA11\}

\(\text{(proof)}\)

\textbf{lemma} \textit{DSourcesA22-L1} : \textit{DSources level1 sA22} = \{sA11, sA41\}

\(\text{(proof)}\)

\textbf{lemma} \textit{DSourcesA23-L1} : \textit{DSources level1 sA23} = \{sA11\}

\(\text{(proof)}\)

\textbf{lemma} \textit{DSourcesA31-L1} : \textit{DSources level1 sA31} = \{sA22\}

\(\text{(proof)}\)

\textbf{lemma} \textit{DSourcesA32-L1} : \textit{DSources level1 sA32} = \{sA23\}

\(\text{(proof)}\)

\textbf{lemma} \textit{DSourcesA41-L1} : \textit{DSources level1 sA41} = \{sA31, sA32\}

\(\text{(proof)}\)

\textbf{lemma} \textit{DSourcesA42-L1} : \textit{DSources level1 sA42} = \{\}

\(\text{(proof)}\)

\textbf{lemma} \textit{DSourcesA5-L1} : \textit{DSources level1 sA5} = \{sA42\}

\(\text{(proof)}\)

\textbf{lemma} \textit{DSourcesA6-L1} : \textit{DSources level1 sA6} = \{\}

\(\text{(proof)}\)

\textbf{lemma} \textit{DSourcesA71-L1} : \textit{DSources level1 sA71} = \{sA6\}

\(\text{(proof)}\)

\textbf{lemma} \textit{DSourcesA72-L1} : \textit{DSources level1 sA72} = \{sA6\}

\(\text{(proof)}\)

\textbf{lemma} \textit{DSourcesA81-L1} : \textit{DSources level1 sA81} = \{sA71, sA91\}

\(\text{(proof)}\)

\end{proof}
lemma \( DSourcesA82-L1: DSources \text{ level1} sA82 = \{ sA72 \} \)
\( \langle \text{proof} \rangle \)

lemma \( DSourcesA91-L1: DSources \text{ level1} sA91 = \{ sA81 \} \)
\( \langle \text{proof} \rangle \)

lemma \( DSourcesA92-L1: DSources \text{ level1} sA92 = \{ sA81 \} \)
\( \langle \text{proof} \rangle \)

lemma \( DSourcesA93-L1: DSources \text{ level1} sA93 = \{ sA82 \} \)
\( \langle \text{proof} \rangle \)

lemma \( A82-Acc: (Acc \text{ level1} sA82) = \{sA93\} \)
\( \langle \text{proof} \rangle \)

lemma \( A82-NSources-L1: \forall C \in (AbstrLevel \text{ level1}). (C \neq sA93 \implies sA82 \notin (Sources \text{ level1} C)) \)
\( \langle \text{proof} \rangle \)

lemma \( A72-Acc: (Acc \text{ level1} sA72) = \{sA82, sA93\} \)
\( \langle \text{proof} \rangle \)

lemma \( A72-NSources-L1: \forall C \in (AbstrLevel \text{ level1}). (C \neq sA93 \land C \neq sA82 \implies sA72 \notin (Sources \text{ level1} C)) \)
\( \langle \text{proof} \rangle \)

lemma \( A92-Acc: (Acc \text{ level1} sA92) = \{\} \)
\( \langle \text{proof} \rangle \)

lemma \( A92-NSources-L1: \forall C \in (AbstrLevel \text{ level1}). (sA92 \notin (Sources \text{ level1} C)) \)
\( \langle \text{proof} \rangle \)

lemma \( A91-Acc: (Acc \text{ level1} sA91) = \{sA81, sA91, sA92\} \)
\( \langle \text{proof} \rangle \)

lemma \( A91-NSources-L1: \forall C \in (AbstrLevel \text{ level1}). (C \neq sA92 \land C \neq sA91 \land C \neq sA81 \implies sA91 \notin (Sources \text{ level1} C)) \)
\( \langle \text{proof} \rangle \)

lemma \( A81-Acc: (Acc \text{ level1} sA81) = \{sA81, sA91, sA92\} \)
\( \langle \text{proof} \rangle \)

lemma \( A81-NSources-L1: \forall C \in (AbstrLevel \text{ level1}). (C \neq sA92 \land C \neq sA91 \land C \neq sA81 \implies sA81 \notin (Sources \text{ level1} C)) \)
\( \langle \text{proof} \rangle \)

42
lemma A71-Acc: \((\text{Acc level1 } sA71) = \{sA81, sA91, sA92\}\)
⟨proof⟩

lemma A71-NSources-L1:
\(\forall C \in (\text{AbstrLevel level1}). (C \neq sA92 \land C \neq sA91 \land C \neq sA81 \rightarrow sA71 \notin (\text{Sources level1 } C)\)
⟨proof⟩

lemma A6-Acc-L1:
\((\text{Acc level1 } sA6) = \{sA71, sA72, sA81, sA82, sA91, sA92, sA93\}\)
⟨proof⟩

lemma A6-NSources-L1Acc:
\(\forall C \in (\text{AbstrLevel level1}). (C \notin (\text{Acc level1 } sA6) \rightarrow sA6 \notin (\text{Sources level1 } C)\)
⟨proof⟩

lemma A6-NSources-L1:
\(\forall C \in (\text{AbstrLevel level1}). (C \neq sA93 \land C \neq sA92 \land C \neq sA91 \land C \neq sA82 \land C \neq sA81 \land C \neq sA72 \land C \neq sA71 \rightarrow sA6 \notin (\text{Sources level1 } C)\)
⟨proof⟩

lemma A5-Acc-L1: \((\text{Acc level1 } sA5) = \{\}\)
⟨proof⟩

lemma SourcesA11-L1: \((\text{Sources level1 } sA11) = \{\}\)
⟨proof⟩

lemma SourcesA12-L1: \((\text{Sources level1 } sA12) = \{\}\)
⟨proof⟩

lemma SourcesA21-L1: \((\text{Sources level1 } sA21) = \{sA11\}\)
⟨proof⟩

lemma SourcesA22-L1: \((\text{Sources level1 } sA22) = \{sA11, sA22, sA23, sA31, sA32, sA41\}\)
⟨proof⟩

lemma SourcesA23-L1: \((\text{Sources level1 } sA23) = \{sA11\}\)
⟨proof⟩

lemma SourcesA31-L1: \((\text{Sources level1 } sA31) = \{sA11, sA22, sA23, sA31, sA32, sA41\}\)
⟨proof⟩

lemma SourcesA32-L1: \((\text{Sources level1 } sA32) = \{sA11, sA23\}\)
\(\langle \text{proof} \rangle\)

**Lemma** \text{SourcesA41-L1}: Sources level1 \(sA41 = \{sA11, sA22, sA23, sA31, sA32, sA41\}\)

\(\langle \text{proof} \rangle\)

**Lemma** \text{SourcesA42-L1}: Sources level1 \(sA42 = \{\}\)

\(\langle \text{proof} \rangle\)

**Lemma** \text{SourcesA5-L1}: Sources level1 \(sA5 = \{sA42\}\)

\(\langle \text{proof} \rangle\)

**Lemma** \text{SourcesA6-L1}: Sources level1 \(sA6 = \{\}\)

\(\langle \text{proof} \rangle\)

**Lemma** \text{SourcesA71-L1}: Sources level1 \(sA71 = \{sA5\}\)

\(\langle \text{proof} \rangle\)

**Lemma** \text{SourcesA81-L1}: Sources level1 \(sA81 = \{sA6, sA71, sA81, sA91\}\)

\(\langle \text{proof} \rangle\)

**Lemma** \text{SourcesA91-L1}: Sources level1 \(sA91 = \{sA6, sA71, sA81, sA91\}\)

\(\langle \text{proof} \rangle\)

**Lemma** \text{SourcesA92-L1}: Sources level1 \(sA92 = \{sA6, sA71, sA81, sA91\}\)

\(\langle \text{proof} \rangle\)

**Lemma** \text{SourcesA72-L1}: Sources level1 \(sA72 = \{sA6\}\)

\(\langle \text{proof} \rangle\)

**Lemma** \text{SourcesA82-L1}: Sources level1 \(sA82 = \{sA6, sA72\}\)

\(\langle \text{proof} \rangle\)

**Lemma** \text{SourcesA93-L1}: Sources level1 \(sA93 = \{sA6, sA72, sA82\}\)

\(\langle \text{proof} \rangle\)

**Lemma** \text{SourcesS1-L2}: Sources level2 \(sS1 = \{\}\)

\(\langle \text{proof} \rangle\)

**Lemma** \text{SourcesS2-L2}: Sources level2 \(sS2 = \{\}\)

\(\langle \text{proof} \rangle\)

**Lemma** \text{SourcesS3-L2}: Sources level2 \(sS3 = \{sS2\}\)

\(\langle \text{proof} \rangle\)

**Lemma** \text{SourcesS4-L2}: Sources level2 \(sS4 = \{sS2\}\)

\(\langle \text{proof} \rangle\)

44
lemma SourcesS5-L2: Sources level2 sS5 = \{sS2, sS4\}
⟨proof⟩

lemma SourcesS6-L2: Sources level2 sS6 = \{sS2, sS4, sS5\}
⟨proof⟩

lemma SourcesS7-L2: Sources level2 sS7 = \{\}
⟨proof⟩

lemma SourcesS8-L2:
Sources level2 sS8 = \{sS7\}
⟨proof⟩

lemma SourcesS9-L2:
Sources level2 sS9 = \{\}
⟨proof⟩

lemma SourcesS10-L2: Sources level2 sS10 = \{sS9\}
⟨proof⟩

lemma SourcesS11-L2: Sources level2 sS11 = \{sS9\}
⟨proof⟩

lemma SourcesS12-L2: Sources level2 sS12 = \{sS9, sS10\}
⟨proof⟩

lemma SourcesS13-L2: Sources level2 sS13 = \{sS9, sS10, sS12\}
⟨proof⟩

lemma SourcesS14-L2: Sources level2 sS14 = \{sS9, sS11\}
⟨proof⟩

lemma SourcesS15-L2: Sources level2 sS15 = \{sS9, sS11, sS14\}
⟨proof⟩

4.5 Minimal sets of components to prove certain properties

lemma minSetOfComponentsTestL2p1:
minSetOfComponents level2 \{data10, data13\} = \{sS1\}
⟨proof⟩

lemma NOT-noIrrelevantChannelsTestL2p1:
¬ noIrrelevantChannels level2 \{data10, data13\}
⟨proof⟩

lemma NOT-allNeededINChannelsTestL2p1:
¬ allNeededINChannels level2 \{data10, data13\}
⟨proof⟩
lemma minSetOfComponentsTestL2p2:
minSetOfComponents level2 \{data1, data12\} = \{sS2, sS4, sS5, sS6\} 
⟨proof⟩

lemma noIrrelevantChannelsTestL2p2:
noIrrelevantChannels level2 \{data1, data12\} 
⟨proof⟩

lemma allNeededINChannelsTestL2p2:
allNeededINChannels level2 \{data1, data12\} 
⟨proof⟩

lemma minSetOfComponentsTestL1p3:
minSetOfComponents level1 \{data1, data10, data11\} = \{sA12, sA11, sA21\} 
⟨proof⟩

lemma noIrrelevantChannelsTestL1p3:
noIrrelevantChannels level1 \{data1, data10, data11\} 
⟨proof⟩

lemma allNeededINChannelsTestL1p3:
allNeededINChannels level1 \{data1, data10, data11\} 
⟨proof⟩

lemma minSetOfComponentsTestL2p3:
minSetOfComponents level2 \{data1, data10, data11\} = \{sS1, sS2, sS3\} 
⟨proof⟩

lemma noIrrelevantChannelsTestL2p3:
noIrrelevantChannels level2 \{data1, data10, data11\} 
⟨proof⟩

lemma allNeededINChannelsTestL2p3:
allNeededINChannels level2 \{data1, data10, data11\} 
⟨proof⟩

dep

References


