

Information Flow Control via Stateful Intransitive Noninterference in Language IMP

Pasquale Noce

Senior Staff Firmware Engineer at HID Global, Italy

pasquale dot noce dot lavoro at gmail dot com

pasquale dot noce at hidglobal dot com

March 17, 2025

Abstract

The scope of information flow control via static type systems is in principle much broader than information flow security, since this concept promises to cope with information flow correctness in full generality. Such a correctness policy can be expressed by extending the notion of a single stateless level-based interference relation applying throughout a program – addressed by the static security type systems described by Volpano, Smith, and Irvine, and formalized in Nipkow and Klein’s book on formal programming language semantics (in the version of February 2023) – to that of a stateful interference function mapping program states to (generally) intransitive interference relations.

This paper studies information flow control via stateful intransitive noninterference. First, the notion of termination-sensitive information flow security with respect to a level-based interference relation is generalized to that of termination-sensitive information flow correctness with respect to such a correctness policy. Then, a static type system is specified and is proven to be capable of enforcing such policies. Finally, the information flow correctness notion and the static type system introduced here are proven to degenerate to the counterparts formalized in Nipkow and Klein’s book in case of a stateless level-based information flow correctness policy. Although the operational semantics of the didactic programming language IMP employed in the book is used for this purpose, the introduced concepts apply to larger, real-world imperative programming languages as well.

Contents

1	Underlying concepts and formal definitions	2
1.1	Global context definitions	6
1.2	Local context definitions	7

2	Idempotence of the auxiliary type system meant for loop bodies	25
2.1	Global context proofs	26
2.2	Local context proofs	26
3	Overapproximation of program semantics by the type system	38
3.1	Global context proofs	39
3.2	Local context proofs	39
4	Sufficiency of well-typedness for information flow correctness	66
4.1	Global context proofs	66
4.2	Local context proofs	74
5	Degeneracy to stateless level-based information flow control	134
5.1	Global context definitions and proofs	135
5.2	Local context definitions and proofs	137

1 Underlying concepts and formal definitions

```
theory Definitions
  imports HOL-IMP.Small-Step
begin
```

In a passage of his book *Clean Architecture: A Craftsman's Guide to Software Structure and Design* (Prentice Hall, 2017), Robert C. Martin defines a computer program as “a detailed description of the policy by which inputs are transformed into outputs”, remarking that “indeed, at its core, that’s all a computer program actually is”. Accordingly, the scope of information flow control via static type systems is in principle much broader than language-based information flow security, since this concept promises to cope with information flow correctness in full generality.

This is already shown by a basic program implementing the Euclidean algorithm, in Donald Knuth’s words “the granddaddy of all algorithms, because it is the oldest nontrivial algorithm that has survived to the present day” (from *The Art of Computer Programming, Volume 2: Seminumerical Algorithms*, third edition, Addison-Wesley, 1997). Here below is a sample such C program, where variables `a` and `b` initially contain two positive integers and `a` will finally contain the output, namely the greatest common divisor of those integers.

```

1  do
2  {
3      r = a % b;
4      a = b;
5      b = r;
6  } while (b);

```

Even in a so basic program, information is not allowed to indistinctly flow from any variable to any other one, on pain of the program being incorrect. If an incautious programmer swapped `a` for `b` in the assignment at line 4, the greatest common divisor output for any two inputs `a` and `b` would invariably match `a`, whereas swapping the sides of the assignment at line 5 would give rise to an endless loop. Indeed, despite the marked differences in the resulting program behavior, both of these potential errors originate in information flowing between variables along paths other than the demanded ones. A sound implementation of the Euclidean algorithm does not provide for any information flow from `a` to `b`, or from `b` to `r`.

The static security type systems addressed in [11], [10], and [7] restrict the information flows occurring in a program based on a mapping of each of its variables to a *domain* along with an *interference relation* between such domains, including any pair of domains such that the former may interfere with the latter. Accordingly, if function *dom* stands for such a mapping, and infix notation $u \rightsquigarrow v$ denotes the inclusion of any pair of domains (u, v) in such a relation (both notations are borrowed from [9]), the above errors would be detected at compile time by a static type system enforcing an interference relation such that:

- $\text{dom } a \rightsquigarrow \text{dom } r, \text{dom } b \rightsquigarrow \text{dom } r$ (line 3),
- $\text{dom } b \rightsquigarrow \text{dom } a$ (line 4),
- $\text{dom } r \rightsquigarrow \text{dom } b$ (line 5),

and ruling out any other pair of distinct domains. Such an interference relation would also embrace the implicit information flow from `b` to the other two variables arising from the loop's termination condition (line 6).

Remarkably, as $\text{dom } a \rightsquigarrow \text{dom } r$ and $\text{dom } r \rightsquigarrow \text{dom } b$ but $\neg \text{dom } a \rightsquigarrow \text{dom } b$, this interference relation turns out to be intransitive. Therefore, unlike the security static type systems studied in [11] and [10], which deal with *level-based*, and then *transitive*, interference relations, a static type system aimed at enforcing information flow correctness in full generality must be capable of dealing with *intransitive* interference relations as well. This should come as no surprise, since [9] shows that this is the general

case already for interference relations expressing information flow security policies.

But the bar can be raised further. Considering the above program again, the information flows needed for its operation, as listed above, need not be allowed throughout the program. Indeed, information needs to flow from a and b to r at line 3, from b to a at line 4, from r to b at line 5, and then (implicitly) from b to the other two variables at line 6. Based on this observation, error detection at compile time can be made finer-grained by rewriting the program as follows, where i is a further integer variable introduced for this purpose.

```

1  do
2  {
3       $i = 0$ ;
4       $r = a \% b$ ;
5       $i = 1$ ;
6       $a = b$ ;
7       $i = 2$ ;
8       $b = r$ ;
9       $i = 3$ ;
10 } while ( $b$ );

```

In this program, i serves as a state variable whose value in every execution step can be determined already at compile time. Since a distinct set of information flows is allowed for each of its values, a finer-grained information flow correctness policy for this program can be expressed by extending the concept of a single, *stateless* interference relation applying throughout the program to that of a *stateful interference function* mapping program states to interference relations (in this case, according to the value of i). As a result of this extension, for each program state, a distinct interference relation – that is, the one to which the applied interference function maps that state – can be enforced at compile time by a suitable static type system.

If mixfix notation $s: u \rightsquigarrow v$ denotes the inclusion of any pair of domains (u , v) in the interference relation associated with any state s , a finer-grained information flow correctness policy for this program can then be expressed as an interference function such that:

- $s: \text{dom } a \rightsquigarrow \text{dom } r, s: \text{dom } b \rightsquigarrow \text{dom } r$ for any s where $i = 0$ (line 4),
- $s: \text{dom } b \rightsquigarrow \text{dom } a$ for any s where $i = 1$ (line 6),
- $s: \text{dom } r \rightsquigarrow \text{dom } b$ for any s where $i = 2$ (line 8),
- $s: \text{dom } b \rightsquigarrow \text{dom } a, s: \text{dom } b \rightsquigarrow \text{dom } r, s: \text{dom } b \rightsquigarrow \text{dom } i$ for any s where $i = 3$ (line 10),

and ruling out any other pair of distinct domains in any state.

Notably, to enforce such an interference function, a static type system would not need to keep track of the full program state in every program execution step (which would be unfeasible, as the values of *a*, *b*, and *r* cannot be determined at compile time), but only of the values of some specified state variables (in this case, of *i* alone). Accordingly, term *state variable* will henceforth refer to any program variable whose value may affect that of the interference function expressing the information flow correctness policy in force, namely the interference relation to be applied.

Needless to say, there would be something artificial about the introduction of such a state variable into the above sample program, since it is indeed so basic as not to provide for a state machine on its own, so that *i* would be aimed exclusively at enabling the enforcement of such an information flow correctness policy. Yet, real-world imperative programs, for which error detection at compile time is truly meaningful, *do* typically provide for state machines such that only a subset of all the potential information flows is allowed in each state; and even for those which do not, the addition of some *ad hoc* state variable to enforce such a policy could likely be an acceptable trade-off.

Accordingly, the goal of this paper is to study information flow control via stateful intransitive noninterference. First, the notion of termination-sensitive information flow security with respect to a level-based interference relation, as defined in [7], section 9.2.6, is generalized to that of termination-sensitive information flow correctness with respect to a stateful interference function having (generally) intransitive interference relations as values. Then, a static type system is specified and is proven to be capable of enforcing such information flow correctness policies. Finally, the information flow correctness notion and the static type system introduced here are proven to degenerate to the counterparts addressed in [7], section 9.2.6, in case of a stateless level-based information flow correctness policy.

Although the operational semantics of the didactic imperative programming language IMP employed in [7] is used for this purpose, the introduced concepts are applicable to larger, real-world imperative programming languages as well, by just affording the additional type system complexity arising from richer language constructs. Accordingly, the informal explanations accompanying formal content in what follows will keep making use of sample C code snippets.

For further information about the formal definitions and proofs contained in this paper, see Isabelle documentation, particularly [8], [4], [2], [3], and [1].

1.1 Global context definitions

declare $[[\text{syntax-ambiguity-warning} = \text{false}]]$

datatype *com-flow* =
 Assign *vname aexp* $(\langle - ::= - \rangle [1000, 61] 70) \mid$
 Observe *vname set* $(\langle \langle - \rangle \rangle [61] 70)$

type-synonym *flow* = *com-flow list*

type-synonym *config* = *state set* \times *vname set*

type-synonym *scope* = *config set* \times *bool*

abbreviation *eq-states* :: *state* \Rightarrow *state* \Rightarrow *vname set* \Rightarrow *bool*
 $(\langle - = - \rangle (\subseteq -)) \rangle [51, 51] 50$ **where**
 $s = t (\subseteq X) \equiv \forall x \in X. s\ x = t\ x$

abbreviation *univ-states* :: *state set* \Rightarrow *vname set* \Rightarrow *state set*
 $(\langle (Univ - \rangle (\subseteq -)) \rangle [51] 75)$ **where**
 $Univ\ A (\subseteq X) \equiv \{s. \exists t \in A. s = t (\subseteq X)\}$

abbreviation *univ-vars-if* :: *state set* \Rightarrow *vname set* \Rightarrow *vname set*
 $(\langle (Univ?? - -) \rangle [51, 75] 75)$ **where**
 $Univ??\ A\ X \equiv \text{if } A = \{\} \text{ then } UNIV \text{ else } X$

abbreviation *tl2 xs* $\equiv tl\ (tl\ xs)$

fun *run-flow* :: *flow* \Rightarrow *state* \Rightarrow *state* **where**
 $run-flow\ (x ::= a \# cs)\ s = run-flow\ cs\ (s(x := aval\ a\ s)) \mid$
 $run-flow\ (- \# cs)\ s = run-flow\ cs\ s \mid$
 $run-flow\ -\ s = s$

primrec *no-upd* :: *flow* \Rightarrow *vname* \Rightarrow *bool* **where**
 $no-upd\ (c \# cs)\ x =$
 $((case\ c\ of\ y ::= - \Rightarrow y \neq x \mid - \Rightarrow True) \wedge no-upd\ cs\ x) \mid$
 $no-upd\ []\ - = True$

primrec *avars* :: *aexp* \Rightarrow *vname set* **where**
 $avars\ (N\ i) = \{\}$ \mid
 $avars\ (V\ x) = \{x\}$ \mid
 $avars\ (Plus\ a_1\ a_2) = avars\ a_1 \cup avars\ a_2$

primrec *bvars* :: *bexp* \Rightarrow *vname set* **where**
 $bvars\ (Bc\ v) = \{\}$ \mid
 $bvars\ (Not\ b) = bvars\ b \mid$
 $bvars\ (And\ b_1\ b_2) = bvars\ b_1 \cup bvars\ b_2 \mid$
 $bvars\ (Less\ a_1\ a_2) = avars\ a_1 \cup avars\ a_2$

```

fun flow-aux :: com list  $\Rightarrow$  flow where
flow-aux ((x ::= a) # cs) = (x ::= a) # flow-aux cs |
flow-aux ((IF b THEN - ELSE -) # cs) =  $\langle$ bvars b $\rangle$  # flow-aux cs |
flow-aux ((c;; -) # cs) = flow-aux (c # cs) |
flow-aux (- # cs) = flow-aux cs |
flow-aux [] = []

```

definition *flow* :: (*com* \times *state*) *list* \Rightarrow *flow* **where**
flow *cfs* = flow-*aux* (map *fst* *cfs*)

```

function small-stepsl ::
  com  $\times$  state  $\Rightarrow$  (com  $\times$  state) list  $\Rightarrow$  com  $\times$  state  $\Rightarrow$  bool
  ( $\langle$ (-  $\rightarrow^*$  '{-}') - $\rangle$  [51, 51] 55)
where
cf  $\rightarrow^*$ {[]} cf' = (cf = cf') |
cf  $\rightarrow^*$ {cfs @ [cf']} cf'' = (cf  $\rightarrow^*$ {cfs} cf'  $\wedge$  cf'  $\rightarrow$  cf'')

```

by (*atomize-elim*, *auto intro: rev-cases*)
termination by *lexicographic-order*

lemmas small-steps_l-induct = small-steps_l.induct [split-format(*complete*)]

1.2 Local context definitions

In what follows, stateful intransitive noninterference will be formalized within the local context defined by means of a *locale* [1], named *noninterf*. Later on, this will enable to prove the degeneracy of the following definitions to the stateless level-based counterparts addressed in [11], [10], and [7], and formalized in [5] and [6], via a suitable locale interpretation.

Locale *noninterf* contains three parameters, as follows.

- A stateful interference function *interf* mapping program states to *interference predicates* of two domains, intended to be true just in case the former domain is allowed to interfere with the latter.
- A function *dom* mapping program variables to their respective domains.
- A set *state* collecting all state variables.

As the type of the domains is modeled using a type variable, it may be assigned arbitrarily by any locale interpretation, which will enable to set it to *nat* upon proving degeneracy. Moreover, the above mixfix notation $s: u \rightsquigarrow v$ is adopted to express the fact that any two domains u, v satisfy the interference predicate *interf* s associated with any state s , namely the fact that u is allowed to interfere with v in state s .

Locale *noninterf* also contains an assumption, named *interf-state*, which serves the purpose of supplying parameter *state* with its intended semantics, namely standing for the set of all state variables. The assumption is that function *interf* maps any two program states agreeing on the values of all the variables in set *state* to the same interference predicate. Correspondingly, any locale interpretation instantiating parameter *state* as the empty set must instantiate parameter *interf* as a function mapping any two program states, even if differing in the values of all variables, to the same interference predicate – namely, as a constant function. Hence, any such locale interpretation refers to a single, stateless interference predicate applying throughout the program. Unsurprisingly, this is the way how those parameters will be instantiated upon proving degeneracy.

The one just mentioned is the only locale assumption. Particularly, the following formalization does not rely upon the assumption that the interference predicates returned by function *interf* be *reflexive*, although this will be the case for any meaningful real-world information flow correctness policy.

```

locale noninterf =
  fixes
    interf :: state  $\Rightarrow$  'd  $\Rightarrow$  'd  $\Rightarrow$  bool
    ( $\langle \cdot \vdash - \rightsquigarrow - \rangle$  [51, 51, 51] 50) and
    dom :: vname  $\Rightarrow$  'd and
    state :: vname set
  assumes
    interf-state:  $s = t \ (\subseteq \textit{state}) \Longrightarrow \textit{interf} \ s = \textit{interf} \ t$ 

```

```

context noninterf
begin

```

Locale parameters *interf* and *dom* are provided with their intended semantics by the definitions of functions *sources* and *correct*, which are formalized here below based on the following underlying ideas.

As long as a stateless transitive interference relation between domains is considered, the condition for the correctness of the value of a variable resulting from a full or partial program execution need not take into account the execution flow producing it, but rather the initial program state only. In fact, this is what happens with the stateless level-based correctness condition addressed in [11], [10], and [7]: the resulting value of a variable of level *l* is correct if the same value is produced for any initial state agreeing with the given one on the value of every variable of level not higher than *l*.

Things are so simple because, for any variables *x*, *y*, and *z*, if *dom* *z* \rightsquigarrow *dom* *y* and *dom* *y* \rightsquigarrow *dom* *x*, transitivity entails *dom* *z* \rightsquigarrow *dom* *x*, and these interference relationships hold statelessly. Therefore, *z* may be counted among

the variables whose initial values are allowed to affect x independently of whether some intermediate value of y may affect x within the actual execution flow.

Unfortunately, switching to stateful intransitive interference relations puts an end to that happy circumstance – indeed, even statefulness or intransitivity alone would suffice for this sad ending. In this context, deciding about the correctness of the resulting value of a variable x still demands the detection of the variables whose initial values are allowed to interfere with x , but the execution flow leading from the initial program state to the resulting one needs to be considered to perform such detection.

This is precisely the task of function *sources*, so named after its finite state machine counterpart defined in [9]. It takes as inputs an execution flow cs , an initial program state s , and a variable x , and outputs the set of the variables whose values in s are allowed to affect the value of x in the state s' into which cs turns s , according to cs as well as to the information flow correctness policy expressed by parameters *interf* and *dom*.

In more detail, execution flows are modeled as lists comprising items of two possible kinds, namely an assignment of the value of an arithmetic expression a to a variable z or else an *observation* of the values of the variables in a set X , denoted through notations $z ::= a$ (same as with assignment commands) and $\langle X \rangle$ and keeping track of explicit and implicit information flows, respectively. Particularly, item $\langle X \rangle$ refers to the act of observing the values of the variables in X leaving the program state unaltered. During the execution of an IMP program, this happens upon any evaluation of a boolean expression containing all and only the variables in X .

Function *sources* is defined along with an auxiliary function *sources-aux* by means of mutual recursion. Based on this definition, *sources cs s x* contains a variable y if there exist a descending sequence of left sublists $cs_{n+1}, cs_n @ [c_n], \dots, cs_1 @ [c_1]$ of cs and a sequence of variables y_{n+1}, \dots, y_1 , where $n \geq 1$, $cs_{n+1} = cs$, $y_{n+1} = x$, and $y_1 = y$, satisfying the following conditions.

- For each positive integer $i \leq n$, c_i is an assignment $y_{i+1} ::= a_i$ where:

- $y_i \in avars\ a_i$,
- *run-flow* $cs_i\ s$: $dom\ y_i \rightsquigarrow dom\ y_{i+1}$, and
- the right sublist of cs_{i+1} complementary to $cs_i @ [c_i]$ does not comprise any assignment to variable y_{i+1} (as assignment c_i would otherwise be irrelevant),

or else an observation $\langle X_i \rangle$ where:

- $y_i \in X_i$ and
- *run-flow* $cs_i\ s$: $dom\ y_i \rightsquigarrow dom\ y_{i+1}$.

- cs_1 does not comprise any assignment to variable y .

In addition, $sources\ cs\ s\ x$ contains variable x also if cs does not comprise any assignment to variable x .

function

$sources :: flow \Rightarrow state \Rightarrow vname \Rightarrow vname\ set$ **and**
 $sources\ aux :: flow \Rightarrow state \Rightarrow vname \Rightarrow vname\ set$ **where**

$sources\ (cs\ @\ [c])\ s\ x = (case\ c\ of$
 $z ::= a \Rightarrow if\ z = x$
 $\quad then\ sources\ aux\ cs\ s\ x \cup \bigcup \{sources\ cs\ s\ y \mid y.$
 $\quad \quad run\ flow\ cs\ s: dom\ y \rightsquigarrow dom\ x \wedge y \in avars\ a\}$
 $\quad else\ sources\ cs\ s\ x \mid$
 $\langle X \rangle \Rightarrow$
 $\quad sources\ cs\ s\ x \cup \bigcup \{sources\ cs\ s\ y \mid y.$
 $\quad \quad run\ flow\ cs\ s: dom\ y \rightsquigarrow dom\ x \wedge y \in X\}) \mid$

$sources\ [] - x = \{x\} \mid$

$sources\ aux\ (cs\ @\ [c])\ s\ x = (case\ c\ of$
 $- ::= - \Rightarrow$
 $\quad sources\ aux\ cs\ s\ x \mid$
 $\langle X \rangle \Rightarrow$
 $\quad sources\ aux\ cs\ s\ x \cup \bigcup \{sources\ cs\ s\ y \mid y.$
 $\quad \quad run\ flow\ cs\ s: dom\ y \rightsquigarrow dom\ x \wedge y \in X\}) \mid$

$sources\ aux\ [] - - = \{\}$

proof (*atomize-elim*)

fix $a :: flow \times state \times vname + flow \times state \times vname$
{

assume

$\forall cs\ c\ s\ x. a \neq Inl\ (cs\ @\ [c], s, x)$ **and**

$\forall s\ x. a \neq Inl\ ([], s, x)$ **and**

$\forall s\ x. a \neq Inr\ ([], s, x)$

hence $\exists cs\ c\ s\ x. a = Inr\ (cs\ @\ [c], s, x)$

by (*metis obj-sumE prod-cases3 rev-exhaust*)

}

thus

$(\exists cs\ c\ s\ x. a = Inl\ (cs\ @\ [c], s, x)) \vee$

$(\exists s\ x. a = Inl\ ([], s, x)) \vee$

$(\exists cs\ c\ s\ x. a = Inr\ (cs\ @\ [c], s, x)) \vee$

$(\exists s\ x. a = Inr\ ([], s, x))$

by *blast*

qed *auto*

termination by *lexicographic-order*

lemmas *sources-induct* = *sources-sources-aux.induct*

Predicate *correct* takes as inputs a program c , a set of program states A , and a set of variables X . Its truth value equals that of the following termination-sensitive information flow correctness condition: for any state s agreeing with a state in A on the values of the state variables in X , if the *small-step* program semantics turns configuration (c, s) into configuration (c_1, s_1) , and (c_1, s_1) into configuration (c_2, s_2) , then for any state t_1 agreeing with s_1 on the values of the variables in *sources cs s₁ x*, where *cs* is the execution flow leading from (c_1, s_1) to (c_2, s_2) , the small-step semantics turns (c_1, t_1) into some configuration (c_2', t_2) such that:

- $c_2' = \text{SKIP}$ (namely, (c_2', t_2) is a *final* configuration) just in case $c_2 = \text{SKIP}$, and
- the value of variable x in state t_2 is the same as in state s_2 .

Here below are some comments about this definition.

- As *sources cs s₁ x* is the set of the variables whose values in s_1 are allowed to affect the value of x in s_2 , this definition requires any state t_1 indistinguishable from s_1 in the values of those variables to produce a state where variable x has the same value as in s_2 in the continuation of program execution.
- Configuration (c_2', t_2) must be the same one for *any* variable x such that s_1 and t_1 agree on the values of any variable in *sources cs s₁ x*. Otherwise, even if states s_2 and t_2 agreed on the value of x , they could be distinguished all the same based on a discrepancy between the respective values of some other variable. Likewise, if state t_2 alone had to be the same for any such x , while command c_2' were allowed to vary, state t_1 could be distinguished from s_1 based on the continuation of program execution. This is the reason why the universal quantification over x is nested within the existential quantification over both c_2' and t_2 .
- The state machine for a program typically provides for a set of initial states from which its execution is intended to start. In any such case, information flow correctness need not be assessed for arbitrary initial states, but just for those complying with the settled tuples of initial values for state variables. The values of any other variables do not matter, as they do not affect function *interf*'s ones. This is the motivation for parameter A , which then needs to contain just one state for each of such tuples, while parameter X enables to exclude the state variables, if any, whose initial values are not settled.

- If locale parameter *state* matches the empty set, *s* will be any state agreeing with some state in *A* on the value of possibly even no variable at all, that is, a fully arbitrary state provided that *A* is nonempty. This makes *s* range over all possible states, as required for establishing the degeneracy of the present definition to the stateless level-based counterpart addressed in [7], section 9.2.6.

Why express information flow correctness in terms of the small-step program semantics, instead of resorting to the big-step one as happens with the stateless level-based correctness condition in [7], section 9.2.6? The answer is provided by the following sample C programs, where *i* is a state variable.

```

1 y = i;
2 i = (i) ? 1 : 0;
3 x = i + y;

```

```

1 x = 0;
2 if (i == 10)
3 {
4   x = 10;
5 }
6 i = (i) ? 1 : 0;
7 x += i;

```

Let *i* be allowed to interfere with *x* just in case *i* matches 0 or 1, and *y* be never allowed to do so. If *s*₁ were constrained to be the initial state, for both programs *i* would be included among the variables on which *t*₁ needs to agree with *s*₁ in order to be indistinguishable from *s*₁ in the value of *x* resulting from the final assignment. Thus, both programs would fail to be labeled as wrong ones, although in both of them the information flow blatantly bypasses the sanitization of the initial value of *i*, respectively due to an illegal explicit flow and an illegal implicit flow. On the contrary, the present information flow correctness definition detects any such illegal information flow by checking every partial program execution on its own.

abbreviation *ok-flow* :: *com* ⇒ *com* ⇒ *state* ⇒ *state* ⇒ *flow* ⇒ *bool* **where**

ok-flow *c*₁ *c*₂ *s*₁ *s*₂ *cs* ≡

∀ *t*₁. ∃ *c*₂' *t*₂. ∀ *x*.

*s*₁ = *t*₁ (⊆ *sources cs s*₁ *x*) →

(*c*₁, *t*₁) →* (*c*₂', *t*₂) ∧ (*c*₂ = *SKIP*) = (*c*₂' = *SKIP*) ∧ *s*₂ *x* = *t*₂ *x*

definition *correct* :: *com* ⇒ *state set* ⇒ *vname set* ⇒ *bool* **where**

correct c A X ≡

$$\begin{aligned} & \forall s \in \text{Univ } A (\subseteq \text{state} \cap X). \forall c_1 c_2 s_1 s_2 cfs. \\ & (c, s) \rightarrow^* (c_1, s_1) \wedge (c_1, s_1) \rightarrow^* \{cfs\} (c_2, s_2) \longrightarrow \\ & \text{ok-flow } c_1 c_2 s_1 s_2 (\text{flow } cfs) \end{aligned}$$

abbreviation *interf-set* :: *state set* \Rightarrow *'d set* \Rightarrow *'d set* \Rightarrow *bool*

($\langle \cdot \rangle$ [51, 51, 51] 50) **where**

A: $U \rightsquigarrow W \equiv \forall s \in A. \forall u \in U. \forall w \in W. s: u \rightsquigarrow w$

abbreviation *ok-flow-aux* ::

config set \Rightarrow *com* \Rightarrow *com* \Rightarrow *state* \Rightarrow *state* \Rightarrow *flow* \Rightarrow *bool* **where**

ok-flow-aux *U c₁ c₂ s₁ s₂ cs* \equiv

($\forall t_1. \exists c_2' t_2. \forall x.$

($s_1 = t_1 (\subseteq \text{sources-aux } cs s_1 x) \longrightarrow$

($c_1, t_1) \rightarrow^* (c_2', t_2) \wedge (c_2 = \text{SKIP}) = (c_2' = \text{SKIP})) \wedge$

($s_1 = t_1 (\subseteq \text{sources } cs s_1 x) \longrightarrow s_2 x = t_2 x)) \wedge$

($\forall x. (\exists p \in U. \text{case } p \text{ of } (B, Y) \Rightarrow$

$\exists s \in B. \exists y \in Y. \neg s: \text{dom } y \rightsquigarrow \text{dom } x) \longrightarrow \text{no-upd } cs x)$

The next step is defining a static type system guaranteeing that well-typed programs satisfy this information flow correctness criterion. Whenever defining a function, and the pursued type system is obviously no exception, the primary question that one has to answer is: which inputs and outputs should it provide for? The type system formalized in [6] simply makes a pass/fail decision on an input program, based on an input security level, and outputs the verdict as a boolean value. Is this still enough in the present case? The answer can be found by considering again the above C program that computes the greatest common divisor of two positive integers *a*, *b* using a state variable *i*, along with its associated stateful interference function. For the reader's convenience, the program is reported here below.

```

1  do
2  {
3      i = 0;
4      r = a % b;
5      i = 1;
6      a = b;
7      i = 2;
8      b = r;
9      i = 3;
10 } while (b);

```

As $s: \text{dom } a \rightsquigarrow \text{dom } r$ only for a state *s* where *i* = 0, the type system cannot determine that the assignment $r = a \% b$ at line 4 is well-typed without knowing that *i* = 0 whenever that step is executed. Consequently, upon

checking the assignment $i = 0$ at line 3, the type system must output information indicating that $i = 0$ as a result of its execution. This information will then be input to the type system when it is recursively invoked to check line 4, so as to enable the well-typedness of the next assignment to be ascertained.

Therefore, in addition to the program under scrutiny, the type system needs to take a set of program states as input, and as long as the program is well-typed, the output must include a set of states covering any change to the values of the state variables possibly triggered by the input program. In other words, the type system has to *simulate* the execution of the input program at compile time as regards the values of its state variables. In the following formalization, this results in making the type system take an input of type *state set* and output a value of the same type. Yet, since state variables alone are relevant, a real-world implementation of the type system would not need to work with full *state* values, but just with tuples of state variables' values.

Is the input/output of a set of program states sufficient to keep track of the possible values of the state variables at each execution step? Here below is a sample C program helping find an answer, which determines the minimum of two integers a , b and assigns it to variable a using a state variable i .

```

1  i = (a > b) ? 1 : 0;
2  if (i > 0)
3  {
4    a = b;
5  }

```

Assuming that the initial value of i is 0, the information flow correctness policy for this program will be such that:

- $s: \text{dom } a \rightsquigarrow \text{dom } i, s: \text{dom } b \rightsquigarrow \text{dom } i$ for any program state s where $i = 0$ (line 1),
- $s: \text{dom } i \rightsquigarrow \text{dom } a$ for any s where $i = 0$ or $i = 1$ (line 2, more on this later),
- $s: \text{dom } b \rightsquigarrow \text{dom } a$ for any s where $i = 1$ (line 4),

ruling out any other pair of distinct domains in any state.

So far, everything has gone smoothly. However, what happens if the program is changed as follows?

```

1  i = a - b;

```

```

2  if (i > 0)
3  {
4      a = b;
5  }

```

Upon simulating the execution of the former program, the type system can determine the set $\{0, 1\}$ of the possible values of variable i arising from the conditional assignment $i = (a > b) ? 1 : 0$ at line 1. On the contrary, in the case of the latter program, the possible values of i after the assignment $i = a - b$ at line 1 must be marked as being *indeterminate*, since they depend on the initial values of variables a and b , which are unknown at compile time. Hence, the type system needs to provide for an additional input/output parameter of type *vname set*, whose input and output values shall collect the variables whose possible values before and after the execution of the input program are *determinate*.

The correctness of the simulation of program execution by the type system can be expressed as the following condition. Suppose that the type system outputs a *state set* A' and a *vname set* X' when it is input a program c , a *state set* A , and a *vname set* X . Then, for any state s agreeing with some state in A on the value of every state variable in X , if $(c, s) \Rightarrow s'$, s' must agree with some state in A' on the value of every state variable in X' . This can be summarized by saying that the type system must *overapproximate* program semantics, since any algorithm simulating program execution cannot but be imprecise (see [7], *incipit* of chapter 13).

In turn, if the outputs for c , A' , X' are A'' , X'' and $(c, s') \Rightarrow s''$, s'' must agree with some state in A'' on the value of every state variable in X'' . But if c is a loop and $(c, s) \Rightarrow s'$, then $(c, s') \Rightarrow s''$ just in case $s' = s''$, so that the type system is guaranteed to overapproximate the semantics of c only if states consistent with A' , X' are also consistent with A'' , X'' and vice versa. Thus, the type system needs to be *idempotent* if c is a loop, that is, it must be such that $A' = A''$ and $X' = X''$ in this case. Since idempotence is not required for control structures other than loops, the main type system *ctyping2* formalized in what follows will delegate the simulation of the execution of loop bodies to an auxiliary, idempotent type system *ctyping1*.

This type system keeps track of the program state updates possibly occurring in its input program using sets of lists of functions of type *vname* \Rightarrow *val option option*. Command *SKIP* is mapped to a singleton made of the empty list, as no state update takes place. An assignment to a variable x is mapped to a singleton made of a list comprising a single function, whose value is *Some* (*Some* i) or *Some None* for x if it is a state variable and the right-hand side is a constant $N i$ or a non-constant expression, respectively, and *None* otherwise. That is, *None* stands for *unchanged/non-state variable*

(remember, only state variable updates need to be tracked), whereas *Some None* stands for *indeterminate variable*, since the value of a non-constant expression in a loop iteration (remember, *ctyping1* is meant for simulating the execution of loop bodies) is in general unknown at compile time.

At first glance, a conditional statement could simply be mapped to the union of the sets tracking the program state updates possibly occurring in its branches. However, things are not so simple, as shown by the sample C loop here below, which has a conditional statement as its body.

```
1  for (i = 0; i < 2; i++)
2  {
3      if (n % 2)
4      {
5          a = 1;
6          b = 1;
7          n++;
8      }
9      else
10     {
11         a = 2;
12         c = 2;
13         n++;
14     }
15 }
```

If the initial value of the integer variable *n* is even, the final values of variables *a*, *b*, and *c* will be 1, 1, 2, whereas if the initial value of *n* is odd, the final values of the aforesaid variables will be 2, 1, 2. Assuming that their initial value is 0, the potential final values tracked by considering each branch individually are 1, 1, 0 and 2, 0, 2 instead. These are exactly the values generated by a single loop iteration; if they are fed back into the loop body along with the increased value of *n*, the actual final values listed above are produced.

As a result, a mere union of the sets tracking the program state updates possibly occurring in each branch would not be enough for the type system to be idempotent. The solution is to rather construct every possible alternate concatenation without repetitions of the lists contained in each set, which is referred to as *merging* those sets in the following formalization. In fact, alternating the state updates performed by each branch in the previous example produces the actual final values listed above. Since the latest occurrence of a state update makes any previous occurrence irrelevant for the final state, repetitions need not be taken into account, which ensures the finiteness of the construction provided that the sets being merged are finite. In the special case where the boolean condition can be evaluated at

compile time, considering the picked branch alone is of course enough.

Another case trickier than what one could expect at first glance is that of sequential composition. This is shown by the sample C loop here below, whose body consists of the sequential composition of some assignments with a conditional statement.

```
1  for (i = 0; i < 2; i++)
2  {
3      a = 1;
4      b = 1;
5      if (n % 2)
6      {
7          a = 2;
8          c = 2;
9          n++;
10     }
11     else
12     {
13         b = 3;
14         d = 3;
15         n++;
16     }
17 }
```

If the initial value of the integer variable n is even, the final values of variables a , b , c , and d will be 2, 1, 2, 3, whereas if the initial value of n is odd, the final values of the aforesaid variables will be 1, 3, 2, 3. Assuming that their initial value is 0, the potential final values tracked by considering the sequences of the state updates triggered by the starting assignments with the updates, simulated as described above, possibly triggered by the conditional statement rather are:

- 2, 1, 2, 0,
- 1, 3, 0, 3,
- 2, 3, 2, 3.

The first two tuples of values match the ones generated by a single loop iteration, and produce the actual final values listed above if they are fed back into the loop body along with the increased value of n .

Hence, concatenating the lists tracking the state updates possibly triggered by the first command in the sequence (the starting assignment sequence in the previous example) with the lists tracking the updates possibly triggered by the second command in the sequence (the conditional statement in

the previous example) would not suffice for the type system to be idempotent. The solution is to rather append the latter lists to those constructed by *merging* the sets tracking the state updates possibly performed by each command in the sequence. Again, provided that such sets are finite, this construction is finite, too. In the special case where the latter set is a singleton, the aforesaid merging is unnecessary, as it would merely insert a preceding occurrence of the single appended list into the resulting concatenated lists, and such repetitions are irrelevant as observed above.

Surprisingly enough, the case of loops is actually simpler than possible first-glance expectations. A loop defines two branches, namely its body and an implicit alternative branch doing nothing. Thus, it can simply be mapped to the union of the set tracking the state updates possibly occurring in its body with a singleton made of the empty list. As happens with conditional statements, in the special case where the boolean condition can be evaluated at compile time, considering the selected branch alone is obviously enough.

Type system *ctyping1* uses the set of lists resulting from this recursion over the input command to construct a set F of functions of type $vname \Rightarrow val\ option\ option$, as follows: for each list ys in the former set, F contains the function mapping any variable x to the rightmost occurrence, if any, of pattern *Some v* to which x is mapped by any function in ys (that is, to the latest update, if any, of x tracked in ys), or else to *None*. Then, if A , X are the input *state set* and *vname set*, and B , Y the output ones:

- B is the set of the program states constructed by picking a function f and a state s from F and A , respectively, and mapping any variable x to i if $f\ x = Some\ (Some\ i)$, or else to $s\ x$ if $f\ x = None$ (namely, to its value in the initial state s if f marks it as being unchanged).
- Y is *UNIV* if $A = \{\}$ (more on this later), or else the set of the variables not mapped to *Some None* (that is, not marked as being indeterminate) by any function in F , and contained in X (namely, being initially determinate) if mapped to *None* (that is, if marked as being unchanged) by some function in F .

When can *ctyping1* evaluate the boolean condition of a conditional statement or a loop, so as to possibly detect and discard some “dead” branch? This question can be answered by examining the following sample C loop, where n is a state variable, while integer j is unknown at compile time.

```

1  for (i = 0; i != j; i++)
2  {
3      if (n == 1)
4      {
5          n = 2;

```

```

6   }
7   else if (n == 0)
8   {
9       n = 1;
10  }
11 }

```

Assuming that the initial value of n is 0, its final value will be 0, 1, or 2 according to whether j matches 0, 1, or any other positive integer, respectively, whereas the loop will not even terminate if j is negative. Consequently, the type system cannot avoid tracking the state updates possibly triggered in every branch, on pain of failing to be idempotent. As a result, evaluating the boolean conditions in the conditional statement at compile time so as to discard some branch is not possible, even though they only depend on an initially determinate state variable. The conclusion is that *ctyping1* may generally evaluate boolean conditions just in case they contain constants alone, namely only if they are trivial enough to be possibly eliminated by program optimization. This is exactly what *ctyping1* does by passing any boolean condition found in the input program to the type system *btyping1* for boolean expressions, defined here below as well.

primrec *btyping1* :: *bexp* \Rightarrow *bool option* ($\langle \vdash - \rangle$ [51] 55) **where**

```

 $\vdash$  Bc  $v$  = Some  $v$  |

 $\vdash$  Not  $b$  = (case  $\vdash b$  of
    Some  $v \Rightarrow$  Some ( $\neg v$ ) |  $- \Rightarrow$  None) |

 $\vdash$  And  $b_1 b_2$  = (case ( $\vdash b_1, \vdash b_2$ ) of
    (Some  $v_1, \text{Some } v_2$ )  $\Rightarrow$  Some ( $v_1 \wedge v_2$ ) |  $- \Rightarrow$  None) |

 $\vdash$  Less  $a_1 a_2$  = (if avars  $a_1 \cup \text{avars } a_2 = \{\}$ 
    then Some (aval  $a_1$  ( $\lambda x. 0$ ) < aval  $a_2$  ( $\lambda x. 0$ )) else None)

```

type-synonym *state-upd* = *vname* \Rightarrow *val option option*

inductive-set *ctyping1-merge-aux* :: *state-upd list set* \Rightarrow
state-upd list set \Rightarrow (*state-upd list* \times *bool*) *list set*
(**infix** $\langle \sqcup \rangle$ 55) **for** *A* **and** *B* **where**

```

 $xs \in A \Longrightarrow [(xs, \text{True})] \in A \sqcup B$  |

 $ys \in B \Longrightarrow [(ys, \text{False})] \in A \sqcup B$  |

 $\llbracket ws \in A \sqcup B; \neg \text{snd} (\text{last } ws); xs \in A; (xs, \text{True}) \notin \text{set } ws \rrbracket \Longrightarrow$ 

```

$ws @ [(xs, True)] \in A \sqcup B \mid$

$\llbracket ws \in A \sqcup B; snd (last\ ws); ys \in B; (ys, False) \notin set\ ws \rrbracket \implies$
 $ws @ [(ys, False)] \in A \sqcup B$

declare *ctyping1-merge-aux.intros* [intro]

definition *ctyping1-append* ::
 $state\text{-}upd\ list\ set \Rightarrow state\text{-}upd\ list\ set \Rightarrow state\text{-}upd\ list\ set$
 (infixl $\langle @ \rangle$ 55) **where**
 $A @ B \equiv \{xs @ ys \mid xs\ ys.\ xs \in A \wedge ys \in B\}$

definition *ctyping1-merge* ::
 $state\text{-}upd\ list\ set \Rightarrow state\text{-}upd\ list\ set \Rightarrow state\text{-}upd\ list\ set$
 (infixl $\langle \sqcup \rangle$ 55) **where**
 $A \sqcup B \equiv \{concat\ (map\ fst\ ws) \mid ws.\ ws \in A \sqcup B\}$

definition *ctyping1-merge-append* ::
 $state\text{-}upd\ list\ set \Rightarrow state\text{-}upd\ list\ set \Rightarrow state\text{-}upd\ list\ set$
 (infixl $\langle \sqcup @ \rangle$ 55) **where**
 $A \sqcup @ B \equiv (if\ card\ B = Suc\ 0\ then\ A\ else\ A \sqcup B) @ B$

primrec *ctyping1-aux* :: $com \Rightarrow state\text{-}upd\ list\ set$
 ($\langle \vdash - \rangle$ [51] 60) **where**

$\vdash SKIP = \{\}\mid$

$\vdash y ::= a = \{[\lambda x.\ if\ x = y \wedge y \in state$
 $\quad then\ if\ avars\ a = \{\} then\ Some\ (Some\ (aval\ a\ (\lambda x.\ 0))) else\ Some\ None$
 $\quad else\ None]\}\mid$

$\vdash c_1;; c_2 = \vdash c_1 \sqcup @ \vdash c_2 \mid$

$\vdash IF\ b\ THEN\ c_1\ ELSE\ c_2 = (let\ f = \vdash b\ in$
 $\quad (if\ f \in \{Some\ True, None\} then\ \vdash c_1\ else\ \{\}) \sqcup$
 $\quad (if\ f \in \{Some\ False, None\} then\ \vdash c_2\ else\ \{\})) \mid$

$\vdash WHILE\ b\ DO\ c = (let\ f = \vdash b\ in$
 $\quad (if\ f \in \{Some\ False, None\} then\ \{\}\ else\ \{\}) \cup$
 $\quad (if\ f \in \{Some\ True, None\} then\ \vdash c\ else\ \{\}))$

definition *ctyping1-seq* :: $state\text{-}upd \Rightarrow state\text{-}upd \Rightarrow state\text{-}upd$
 (infixl $\langle ;; \rangle$ 55) **where**
 $S;; T \equiv \lambda x.\ case\ T\ x\ of\ None \Rightarrow S\ x \mid Some\ v \Rightarrow Some\ v$

definition *ctyping1* :: $com \Rightarrow state\ set \Rightarrow vname\ set \Rightarrow config$
 ($\langle \vdash - '(\subseteq -, -)' \rangle$ [51] 55) **where**
 $\vdash c (\subseteq A, X) \equiv let\ F = \{\lambda x.\ foldl\ (;;)\ (\lambda x.\ None)\ ys\ x \mid ys.\ ys \in \vdash c\}\ in$

$$\begin{aligned}
& (\{\lambda x. \text{case } f \ x \text{ of } \text{None} \Rightarrow s \ x \mid \text{Some } \text{None} \Rightarrow t \ x \mid \text{Some } (\text{Some } i) \Rightarrow i \mid \\
& \quad f \ s \ t. f \in F \wedge s \in A\}, \\
& \text{Univ}^{??} A \ \{x. \forall f \in F. f \ x \neq \text{Some } \text{None} \wedge (f \ x = \text{None} \longrightarrow x \in X)\})
\end{aligned}$$

A further building block propaedeutic to the definition of the main type system *ctyping2* is the definition of its own companion type system *btyping2* for boolean expressions. The goal of *btyping2* is splitting, whenever feasible at compile time, an input *state set* into two complementary subsets, respectively comprising the program states making the input boolean expression true or false. This enables *ctyping2* to apply its information flow correctness checks to conditional branches by considering only the program states in which those branches are executed.

As opposed to *btyping1*, *btyping2* may evaluate its input boolean expression even if it contains variables, provided that all of their values are known at compile time, namely that all of them are determinate state variables – hence *btyping2*, like *ctyping2*, needs to take a *vname set* collecting determinate variables as an additional input. In fact, in the case of a loop body, the dirty work of covering any nested branch by skipping the evaluation of non-constant boolean conditions is already done by *ctyping1*, so that any *state set* and *vname set* input to *btyping2* already encompass every possible execution flow.

primrec *btyping2-aux* :: *bexp* \Rightarrow *state set* \Rightarrow *vname set* \Rightarrow *state set option*
 ($\langle \models - '(\subseteq -, -') \rangle$ [51] 55) **where**

$$\models Bc \ v \ (\subseteq A, -) = \text{Some } (\text{if } v \text{ then } A \text{ else } \{\}) \mid$$

$$\models \text{Not } b \ (\subseteq A, X) = (\text{case } \models b \ (\subseteq A, X) \text{ of } \\ \text{Some } B \Rightarrow \text{Some } (A - B) \mid - \Rightarrow \text{None}) \mid$$

$$\models \text{And } b_1 \ b_2 \ (\subseteq A, X) = (\text{case } (\models b_1 \ (\subseteq A, X), \models b_2 \ (\subseteq A, X)) \text{ of } \\ (\text{Some } B_1, \text{Some } B_2) \Rightarrow \text{Some } (B_1 \cap B_2) \mid - \Rightarrow \text{None}) \mid$$

$$\models \text{Less } a_1 \ a_2 \ (\subseteq A, X) = (\text{if } \text{avars } a_1 \cup \text{avars } a_2 \subseteq \text{state} \cap X \\ \text{then } \text{Some } \{s. s \in A \wedge \text{aval } a_1 \ s < \text{aval } a_2 \ s\} \text{ else } \text{None})$$

definition *btyping2* :: *bexp* \Rightarrow *state set* \Rightarrow *vname set* \Rightarrow
state set \times *state set*

($\langle \models - '(\subseteq -, -') \rangle$ [51] 55) **where**
 $\models b \ (\subseteq A, X) \equiv \text{case } \models b \ (\subseteq A, X) \text{ of } \\ \text{Some } A' \Rightarrow (A', A - A') \mid - \Rightarrow (A, A)$

It is eventually time to define the main type system *ctyping2*. Its output consists of the *state set* of the final program states and the *vname set* of the finally determinate variables produced by simulating the execution of

the input program, based on the *state set* of initial program states and the *vname set* of initially determinate variables taken as inputs, if information flow correctness checks are passed; otherwise, the output is *None*.

An additional input is the counterpart of the level input to the security type systems formalized in [6], in that it specifies the *scope* in which information flow correctness is validated. It consists of a set of *state set* \times *vname set* pairs and a boolean flag. The set keeps track of the variables contained in the boolean conditions, if any, nesting the input program, in association with the program states in which they are evaluated. The flag is *False* if the input program is nested in a loop, in which case state variables set to non-constant expressions are marked as being indeterminate (as observed previously, the value of a non-constant expression in a loop iteration is in general unknown at compile time).

In the recursive definition of *ctyping2*, the equations dealing with conditional branches, namely those applying to conditional statements and loops, construct the output *state set* and *vname set* respectively as the *union* and the *intersection* of the sets computed for each branch. In fact, a possible final state is any one resulting from either branch, and a variable is finally determinate just in case it is such regardless of the branch being picked. Yet, a “dead” branch should have no impact on the determinateness of variables, as it only depends on the other branch. Accordingly, provided that information flow correctness checks are passed, the cases where the output is constructed non-recursively, namely those of *SKIP*, assignments, and loops, return *UNIV* as *vname set* if the input *state set* is empty. In the case of a loop, the *state set* and the *vname set* resulting from one or more iterations of its body are computed using the auxiliary type system *ctyping1*. This explains why *ctyping1* returns *UNIV* as *vname set* if the input *state set* is empty, as mentioned previously.

As happens with the syntax-directed security type system formalized in [6], the cases performing non-recursive information flow correctness checks are those of assignments and loops. In the former case, *ctyping2* verifies that the sets of variables contained in the scope, as well as any variable occurring in the expression on the right-hand side of the assignment, are allowed to interfere with the variable on the left-hand side, respectively in their associated sets of states and in the input *state set*. In the latter case, *ctyping2* verifies that the sets of variables contained in the scope, as well as any variable occurring in the boolean condition of the loop, are allowed to interfere with *every* variable, respectively in their associated sets of states and in the states in which the boolean condition is evaluated. In both cases, if the applying interference relation is unknown as some state variable is indeterminate, each of those checks must be passed for *any* possible state (unless the respective set of states is empty).

Why do the checks performed for loops test interference with *every* variable?

The answer is provided by the following sample C program, which sets variables *a* and *b* to the terms in the zero-based positions *j* and *j* + 1 of the Fibonacci sequence.

```

1  a = 0;
2  b = 1;
3  for (i = 0; i != j; i++)
4  {
5      c = b;
6      b += a;
7      a = c;
8  }
```

The loop in this program terminates for any nonnegative value of *j*. For any variable *x*, suppose that *j* is not allowed to interfere with *x* in such an initial state, say *s*. According to the above information flow correctness definition, any initial state *t* differing from *s* in the value of *j* must make execution terminate all the same in order for the program to be correct. However, this is not the case, since execution does not terminate for any negative value of *j*. Thus, the type system needs to verify that *j* may interfere with *x*, on pain of returning a wrong *pass* verdict.

The cases that change the scope upon recursively calling the type system are those of conditional statements and loops. In the latter case, the boolean flag is set to *False*, and the set of *state set* \times *vname set* pairs is empty as the whole scope nesting the loop body, including any variable occurring in the boolean condition of the loop, must be allowed to interfere with every variable. In the former case, for both branches, the boolean flag is left unchanged, whereas the set of pairs is extended with the pair composed of the input *state set* (or of *UNIV* if some state variable is indeterminate, unless the input *state set* is empty) and of the set of the variables, if any, occurring in the boolean condition of the statement.

Why is the scope extended with the whole input *state set* for both branches, rather than just with the set of states in which each single branch is selected? Once more, the question can be answered by considering a sample C program, namely a previous one determining the minimum of two integers *a* and *b* using a state variable *i*. For the reader's convenience, the program is reported here below.

```

1  i = (a > b) ? 1 : 0;
2  if (i > 0)
3  {
4      a = b;
5  }
```

Since the branch changing the value of variable a is executed just in case $i = 1$, suppose that in addition to b , i also is not allowed to interfere with a for $i = 0$, and let s be any initial state where $a \leq b$. Based on the above information flow correctness definition, any initial state t differing from s in the value of b (not bound by the interference of i with a) must produce the same final value of a in order for the program to be correct. However, this is not the case, as the final value of a will change for any state t where $a > b$. Therefore, the type system needs to verify that i may interfere with a for $i = 0$, too, on pain of returning a wrong *pass* verdict. This is the reason why, as mentioned previously, an information flow correctness policy for this program should be such that $s: \text{dom } i \rightsquigarrow \text{dom } a$ even for any state s where $i = 0$.

An even simpler example explains why, in the case of an assignment or a loop, the information flow correctness checks described above need to be applied to the set of *state set* \times *vname set* pairs in the scope even if the input *state set* is empty, namely even if the assignment or the loop are nested in a “dead” branch. Here below is a sample C program showing this.

```

1  if (i)
2  {
3    a = 1;
4  }

```

Assuming that the initial value of i is 0, the assignment nested within the conditional statement is not executed, so that the final value of a matches the initial one, say 0. Suppose that i is not allowed to interfere with a in such an initial state, say s . According to the above information flow correctness definition, any initial state t differing from s in the value of i must produce the same final value of a in order for the program to be correct. However, this is not the case, as the final value of a is 1 for any nonzero value of i . Therefore, the type system needs to verify that i may interfere with a in state s even though the conditional branch is not executed in that state, on pain of returning a wrong *pass* verdict.

abbreviation $\text{atyping} :: \text{bool} \Rightarrow \text{aexp} \Rightarrow \text{vname set} \Rightarrow \text{bool}$
 $(\langle(- \models -'(\subseteq -')\rangle [51, 51] 50) \text{ where}$
 $v \models a (\subseteq X) \equiv \text{avars } a = \{\} \vee \text{avars } a \subseteq \text{state} \cap X \wedge v$

definition $\text{univ-states-if} :: \text{state set} \Rightarrow \text{vname set} \Rightarrow \text{state set}$
 $(\langle(\text{Univ?} - -) \rangle [51, 75] 75) \text{ where}$
 $\text{Univ? } A \ X \equiv \text{if } \text{state} \subseteq X \text{ then } A \text{ else } \text{Univ } A (\subseteq \{\})$


```

fun ctyping2 :: scope  $\Rightarrow$  com  $\Rightarrow$  state set  $\Rightarrow$  vname set  $\Rightarrow$  config option
  ( $\langle \cdot \models \cdot \text{ ' } (\subseteq \cdot, \cdot) \rangle$ ) [51, 51] 55) where

 $\cdot \models \text{SKIP } (\subseteq A, X) = \text{Some } (A, \text{Univ}?? A X) \mid$ 

( $U, v \models x ::= a (\subseteq A, X) =$ 
  (if ( $\forall (B, Y) \in \text{insert } (\text{Univ}?? A X, \text{avars } a) U. B: \text{dom } \cdot Y \rightsquigarrow \{\text{dom } x\}$ )
    then Some (if  $x \in \text{state} \wedge A \neq \{\}$ 
      then if  $v \models a (\subseteq X)$ 
        then ( $\{s(x := \text{aval } a s) \mid s. s \in A\}, \text{insert } x X)$  else  $(A, X - \{x\})$ 
        else  $(A, \text{Univ}?? A X)$ 
      else None)  $\mid$ 

( $U, v \models c_1;; c_2 (\subseteq A, X) =$ 
  (case ( $U, v \models c_1 (\subseteq A, X)$ ) of
    Some  $(B, Y) \Rightarrow (U, v \models c_2 (\subseteq B, Y) \mid \cdot \Rightarrow \text{None}) \mid$ 

( $U, v \models \text{IF } b \text{ THEN } c_1 \text{ ELSE } c_2 (\subseteq A, X) =$ 
  (case ( $\text{insert } (\text{Univ}?? A X, \text{bvars } b) U, \models b (\subseteq A, X)$ ) of  $(U', B_1, B_2) \Rightarrow$ 
    case ( $(U', v \models c_1 (\subseteq B_1, X), (U', v \models c_2 (\subseteq B_2, X))$ ) of
       $(\text{Some } (C_1, Y_1), \text{Some } (C_2, Y_2)) \Rightarrow \text{Some } (C_1 \cup C_2, Y_1 \cap Y_2) \mid$ 
       $\cdot \Rightarrow \text{None}) \mid$ 

( $U, v \models \text{WHILE } b \text{ DO } c (\subseteq A, X) = (\text{case } \models b (\subseteq A, X) \text{ of } (B_1, B_2) \Rightarrow$ 
  case  $\vdash c (\subseteq B_1, X)$  of  $(C, Y) \Rightarrow \text{case } \models b (\subseteq C, Y)$  of  $(B_1', B_2') \Rightarrow$ 
    if  $\forall (B, W) \in \text{insert } (\text{Univ}?? A X \cup \text{Univ}?? C Y, \text{bvars } b) U.$ 
       $B: \text{dom } \cdot W \rightsquigarrow \text{UNIV}$ 
      then case  $((\{\}, \text{False}) \models c (\subseteq B_1, X), (\{\}, \text{False}) \models c (\subseteq B_1', Y))$  of
         $(\text{Some } \cdot, \text{Some } \cdot) \Rightarrow \text{Some } (B_2 \cup B_2', \text{Univ}?? B_2 X \cap Y) \mid$ 
         $\cdot \Rightarrow \text{None}$ 
      else None)

```

end

end

2 Idempotence of the auxiliary type system meant for loop bodies

```

theory Idempotence
imports Definitions
begin

```

The purpose of this section is to prove that the auxiliary type system *ctyping1* used to simulate the execution of loop bodies is idempotent, namely that if its output for a given input is the pair composed of *state set* B and

vname set Y, then the same output is returned if *B* and *Y* are fed back into the type system (lemma *ctyping1-idem*).

2.1 Global context proofs

lemma *remdups-filter-last*:
 $\text{last } [x \leftarrow \text{remdups } xs. P \ x] = \text{last } [x \leftarrow xs. P \ x]$
by (*induction xs*, *auto simp: filter-empty-conv*)

lemma *remdups-append*:
 $\text{set } xs \subseteq \text{set } ys \implies \text{remdups } (xs @ ys) = \text{remdups } ys$
by (*induction xs*, *simp-all*)

lemma *remdups-concat-1*:
 $\text{remdups } (\text{concat } (\text{remdups } [])) = \text{remdups } (\text{concat } [])$
by *simp*

lemma *remdups-concat-2*:
 $\text{remdups } (\text{concat } (\text{remdups } xs)) = \text{remdups } (\text{concat } xs) \implies$
 $\text{remdups } (\text{concat } (\text{remdups } (x \# xs))) = \text{remdups } (\text{concat } (x \# xs))$
by (*simp*, *subst (2 3) remdups-append2 [symmetric]*, *clarsimp*,
subst remdups-append, *auto*)

lemma *remdups-concat*:
 $\text{remdups } (\text{concat } (\text{remdups } xs)) = \text{remdups } (\text{concat } xs)$
by (*induction xs*, *rule remdups-concat-1*, *rule remdups-concat-2*)

2.2 Local context proofs

context *noninterf*
begin

lemma *ctyping1-seq-last*:
 $\text{foldl } (;;) \ S \ xs = (\lambda x. \text{let } xs' = [T \leftarrow xs. T \ x \neq \text{None}] \text{ in}$
 $\text{if } xs' = [] \text{ then } S \ x \text{ else last } xs' \ x)$
by (*rule ext*, *induction xs rule: rev-induct*, *auto simp: ctyping1-seq-def*)

lemma *ctyping1-seq-remdups*:
 $\text{foldl } (;;) \ S \ (\text{remdups } xs) = \text{foldl } (;;) \ S \ xs$
by (*simp add: Let-def ctyping1-seq-last*, *subst remdups-filter-last*,
simp add: remdups-filter [symmetric])

lemma *ctyping1-seq-remdups-concat*:
 $\text{foldl } (;;) \ S \ (\text{concat } (\text{remdups } xs)) = \text{foldl } (;;) \ S \ (\text{concat } xs)$
by (*subst (1 2) ctyping1-seq-remdups [symmetric]*, *simp add: remdups-concat*)

lemma *ctyping1-seq-eq*:
assumes *A*: $\text{foldl } (;;) \ (\lambda x. \text{None}) \ xs = \text{foldl } (;;) \ (\lambda x. \text{None}) \ ys$

shows $\text{foldl } (;;) S xs = \text{foldl } (;;) S ys$
proof –
have $\forall x. ([T \leftarrow xs. T x \neq \text{None}] = [] \longleftrightarrow [T \leftarrow ys. T x \neq \text{None}] = []) \wedge$
 $\text{last } [T \leftarrow xs. T x \neq \text{None}] x = \text{last } [T \leftarrow ys. T x \neq \text{None}] x$
(is $\forall x. (?xs' x = [] \longleftrightarrow ?ys' x = []) \wedge -)$
proof
fix x
from A **have** $(\text{if } ?xs' x = [] \text{ then } \text{None} \text{ else } \text{last } (?xs' x) x) =$
 $(\text{if } ?ys' x = [] \text{ then } \text{None} \text{ else } \text{last } (?ys' x) x)$
by $(\text{drule-tac fun-cong } [\text{where } x = x], \text{auto simp: ctying1-seq-last})$
moreover have $?xs' x \neq [] \implies \text{last } (?xs' x) x \neq \text{None}$
by $(\text{drule last-in-set, simp})$
moreover have $?ys' x \neq [] \implies \text{last } (?ys' x) x \neq \text{None}$
by $(\text{drule last-in-set, simp})$
ultimately show $(?xs' x = [] \longleftrightarrow ?ys' x = []) \wedge$
 $\text{last } (?xs' x) x = \text{last } (?ys' x) x$
by $(\text{auto split: if-split-asm})$
qed
thus $?thesis$
by $(\text{auto simp: ctying1-seq-last})$
qed

lemma *ctying1-merge-aux-butlast*:
 $\llbracket ws \in A \sqcup B; \text{butlast } ws \neq [] \rrbracket \implies$
 $\text{snd } (\text{last } (\text{butlast } ws)) = (\neg \text{snd } (\text{last } ws))$
by $(\text{erule ctying1-merge-aux.cases, simp-all})$

lemma *ctying1-merge-aux-distinct*:
 $ws \in A \sqcup B \implies \text{distinct } ws$
by $(\text{induction rule: ctying1-merge-aux.induct, simp-all})$

lemma *ctying1-merge-aux-nonempty*:
 $ws \in A \sqcup B \implies ws \neq []$
by $(\text{induction rule: ctying1-merge-aux.induct, simp-all})$

lemma *ctying1-merge-aux-item*:
 $\llbracket ws \in A \sqcup B; w \in \text{set } ws \rrbracket \implies \text{fst } w \in (\text{if } \text{snd } w \text{ then } A \text{ else } B)$
by $(\text{induction rule: ctying1-merge-aux.induct, auto})$

lemma *ctying1-merge-aux-take-1* [elim]:
 $\llbracket \text{take } n \text{ } ws \in A \sqcup B; \neg \text{snd } (\text{last } ws); xs \in A; (xs, \text{True}) \notin \text{set } ws \rrbracket \implies$
 $\text{take } n \text{ } ws @ \text{take } (n - \text{length } ws) [(xs, \text{True})] \in A \sqcup B$
by $(\text{cases } n \leq \text{length } ws, \text{auto})$

lemma *ctying1-merge-aux-take-2* [elim]:
 $\llbracket \text{take } n \text{ } ws \in A \sqcup B; \text{snd } (\text{last } ws); ys \in B; (ys, \text{False}) \notin \text{set } ws \rrbracket \implies$
 $\text{take } n \text{ } ws @ \text{take } (n - \text{length } ws) [(ys, \text{False})] \in A \sqcup B$
by $(\text{cases } n \leq \text{length } ws, \text{auto})$

lemma *ctyping1-merge-aux-take*:
 $\llbracket ws \in A \sqcup B; 0 < n \rrbracket \implies take\ n\ ws \in A \sqcup B$
by (*induction rule: ctyping1-merge-aux.induct, auto*)

lemma *ctyping1-merge-aux-drop-1* [*elim*]:
assumes
 A: $xs \in A$ **and**
 B: $ys \in B$
shows $drop\ n\ [(xs, True)] @ [(ys, False)] \in A \sqcup B$
proof –
 from *A* **have** $[(xs, True)] \in A \sqcup B$..
 with *B* **have** $[(xs, True)] @ [(ys, False)] \in A \sqcup B$
 by *fastforce*
 with *B* **show** *?thesis*
 by (*cases n, auto*)
qed

lemma *ctyping1-merge-aux-drop-2* [*elim*]:
assumes
 A: $xs \in A$ **and**
 B: $ys \in B$
shows $drop\ n\ [(ys, False)] @ [(xs, True)] \in A \sqcup B$
proof –
 from *B* **have** $[(ys, False)] \in A \sqcup B$..
 with *A* **have** $[(ys, False)] @ [(xs, True)] \in A \sqcup B$
 by *fastforce*
 with *A* **show** *?thesis*
 by (*cases n, auto*)
qed

lemma *ctyping1-merge-aux-drop-3*:
assumes
 A: $\bigwedge xs\ v. (xs, True) \notin set\ (drop\ n\ ws) \implies$
 $xs \in A \implies v \implies drop\ n\ ws @ [(xs, True)] \in A \sqcup B$ **and**
 B: $xs \in A$ **and**
 C: $ys \in B$ **and**
 D: $(xs, True) \notin set\ ws$ **and**
 E: $(ys, False) \notin set\ (drop\ n\ ws)$
shows $drop\ n\ ws @ drop\ (n - length\ ws)\ [(xs, True)] @$
 $[(ys, False)] \in A \sqcup B$
proof –
 have $set\ (drop\ n\ ws) \subseteq set\ ws$
 by (*rule set-drop-subset*)
 hence $drop\ n\ ws @ [(xs, True)] \in A \sqcup B$
 using *A* **and** *B* **and** *D* **by** *blast*
 hence $(drop\ n\ ws @ [(xs, True)]) @ [(ys, False)] \in A \sqcup B$
 using *C* **and** *E* **by** *fastforce*

thus *?thesis*
using *C* **by** (*cases* $n \leq \text{length } ws$, *auto*)
qed

lemma *ctyping1-merge-aux-drop-4*:
assumes
 $A: \bigwedge ys \ v. (ys, False) \notin \text{set } (\text{drop } n \text{ } ws) \implies$
 $ys \in B \implies \neg v \implies \text{drop } n \text{ } ws @ [(ys, False)] \in A \sqcup B$ **and**
 $B: ys \in B$ **and**
 $C: xs \in A$ **and**
 $D: (ys, False) \notin \text{set } ws$ **and**
 $E: (xs, True) \notin \text{set } (\text{drop } n \text{ } ws)$
shows $\text{drop } n \text{ } ws @ \text{drop } (n - \text{length } ws) [(ys, False)] @$
 $[(xs, True)] \in A \sqcup B$
proof –
have $\text{set } (\text{drop } n \text{ } ws) \subseteq \text{set } ws$
by (*rule set-drop-subset*)
hence $\text{drop } n \text{ } ws @ [(ys, False)] \in A \sqcup B$
using *A* **and** *B* **and** *D* **by** *blast*
hence $(\text{drop } n \text{ } ws @ [(ys, False)]) @ [(xs, True)] \in A \sqcup B$
using *C* **and** *E* **by** *fastforce*
thus *?thesis*
using *C* **by** (*cases* $n \leq \text{length } ws$, *auto*)
qed

lemma *ctyping1-merge-aux-drop*:
 $\llbracket ws \in A \sqcup B; w \notin \text{set } (\text{drop } n \text{ } ws);$
 $\text{fst } w \in (\text{if } \text{snd } w \text{ then } A \text{ else } B); \text{snd } w = (\neg \text{snd } (\text{last } ws)) \rrbracket \implies$
 $\text{drop } n \text{ } ws @ [w] \in A \sqcup B$
proof (*induction arbitrary: w rule: ctyping1-merge-aux.induct*)
fix *xs ws w*
show
 $\llbracket ws \in A \sqcup B;$
 $\bigwedge w. w \notin \text{set } (\text{drop } n \text{ } ws) \implies$
 $\text{fst } w \in (\text{if } \text{snd } w \text{ then } A \text{ else } B) \implies$
 $\text{snd } w = (\neg \text{snd } (\text{last } ws)) \implies$
 $\text{drop } n \text{ } ws @ [w] \in A \sqcup B;$
 $\neg \text{snd } (\text{last } ws);$
 $xs \in A;$
 $(xs, True) \notin \text{set } ws;$
 $w \notin \text{set } (\text{drop } n \text{ } (ws @ [(xs, True)]));$
 $\text{fst } w \in (\text{if } \text{snd } w \text{ then } A \text{ else } B);$
 $\text{snd } w = (\neg \text{snd } (\text{last } (ws @ [(xs, True)]))) \rrbracket \implies$
 $\text{drop } n \text{ } (ws @ [(xs, True)]) @ [w] \in A \sqcup B$
by (*cases* *w*, *auto intro: ctyping1-merge-aux-drop-3*)
next
fix *ys ws w*
show
 $\llbracket ws \in A \sqcup B;$

$\bigwedge w. w \notin \text{set } (\text{drop } n \text{ } ws) \implies$
 $\text{fst } w \in (\text{if } \text{snd } w \text{ then } A \text{ else } B) \implies$
 $\text{snd } w = (\neg \text{snd } (\text{last } ws)) \implies$
 $\text{drop } n \text{ } ws @ [w] \in A \sqcup B;$
 $\text{snd } (\text{last } ws);$
 $ys \in B;$
 $(ys, \text{False}) \notin \text{set } ws;$
 $w \notin \text{set } (\text{drop } n \text{ } (ws @ [(ys, \text{False})]));$
 $\text{fst } w \in (\text{if } \text{snd } w \text{ then } A \text{ else } B);$
 $\text{snd } w = (\neg \text{snd } (\text{last } (ws @ [(ys, \text{False})]))) \implies$
 $\text{drop } n \text{ } (ws @ [(ys, \text{False})]) @ [w] \in A \sqcup B$
by (cases w, auto intro: ctying1-merge-aux-drop-4)
qed auto

lemma ctying1-merge-aux-closed-1:

assumes

$A: \forall vs. \text{length } vs \leq \text{length } us \longrightarrow$
 $(\forall ls \ rs. vs = ls @ rs \longrightarrow ls \in A \sqcup B \longrightarrow rs \in A \sqcup B \longrightarrow$
 $(\exists ws \in A \sqcup B. \text{foldl } (;;) (\lambda x. \text{None}) (\text{concat } (\text{map } \text{fst } ws)) =$
 $\text{foldl } (;;) (\lambda x. \text{None}) (\text{concat } (\text{map } \text{fst } (ls @ rs))) \wedge$
 $\text{length } ws \leq \text{length } (ls @ rs) \wedge \text{snd } (\text{last } ws) = \text{snd } (\text{last } rs)))$
 $(\text{is } \forall -. \longrightarrow (\forall ls \ rs. - \longrightarrow - \longrightarrow - \longrightarrow (\exists ws \in -. ?P \text{ } ws \text{ } ls \text{ } rs)))$ **and**

$B: us \in A \sqcup B$ **and**

$C: \text{fst } v \in (\text{if } \text{snd } v \text{ then } A \text{ else } B)$ **and**

$D: \text{snd } v = (\neg \text{snd } (\text{last } us))$

shows $\exists ws \in A \sqcup B. \text{foldl } (;;) (\lambda x. \text{None}) (\text{concat } (\text{map } \text{fst } ws)) =$
 $\text{foldl } (;;) (\lambda x. \text{None}) (\text{concat } (\text{map } \text{fst } (us @ [v]))) \wedge$
 $\text{length } ws \leq \text{Suc } (\text{length } us) \wedge \text{snd } (\text{last } ws) = \text{snd } v$

proof (cases v in set us, cases hd us = v)

assume E: hd us = v

moreover have distinct us

using B **by** (rule ctying1-merge-aux-distinct)

ultimately have $v \notin \text{set } (\text{drop } (\text{Suc } 0) \text{ } us)$

by (cases us, simp-all)

with B **have** $\text{drop } (\text{Suc } 0) \text{ } us @ [v] \in A \sqcup B$

(is ?ws in -)

using C **and** D **by** (rule ctying1-merge-aux-drop)

moreover have $\text{foldl } (;;) (\lambda x. \text{None}) (\text{concat } (\text{map } \text{fst } ?ws)) =$
 $\text{foldl } (;;) (\lambda x. \text{None}) (\text{concat } (\text{map } \text{fst } (us @ [v])))$

using E **by** (cases us, simp, subst (1 2) ctying1-seq-remdups-concat
[symmetric], simp)

ultimately show ?thesis

by fastforce

next

assume v in set us

then obtain ls **and** rs **where** E: $us = ls @ v \# rs \wedge v \notin \text{set } rs$

by (blast dest: split-list-last)

moreover assume $\text{hd } us \neq v$

ultimately have $ls \neq []$
by (*cases* ls , *simp-all*)
hence take $(length\ ls)\ us \in A \sqcup B$
by (*simp add: ctying1-merge-aux-take* B)
moreover have $v \notin set\ (drop\ (Suc\ (length\ ls))\ us)$
using E **by** *simp*
with B **have** $drop\ (Suc\ (length\ ls))\ us\ @\ [v] \in A \sqcup B$
using C **and** D **by** (*rule ctying1-merge-aux-drop*)
ultimately have $\exists\ ws \in A \sqcup B. ?P\ ws\ ls\ (rs\ @\ [v])$
using A **and** E **by** (*drule-tac spec [of - $ls\ @\ rs\ @\ [v]$],*
simp, drule-tac spec [of - ls], simp)
moreover have $foldl\ (;\;) (\lambda x. None)\ (concat\ (map\ fst\ (ls\ @\ rs\ @\ [v]))) =$
 $foldl\ (;\;) (\lambda x. None)\ (concat\ (map\ fst\ (us\ @\ [v])))$
using E **by** (*subst (1 2) ctying1-seq-remdups-concat [symmetric],*
simp, subst (1 2) remdups-append2 [symmetric], simp)
ultimately show *?thesis*
using E **by** *auto*
next
assume $E: v \notin set\ us$
show *?thesis*
proof (*rule bexI [of - $us\ @\ [v]$]*)
show $foldl\ (;\;) (\lambda x. None)\ (concat\ (map\ fst\ (us\ @\ [v]))) =$
 $foldl\ (;\;) (\lambda x. None)\ (concat\ (map\ fst\ (us\ @\ [v]))) \wedge$
 $length\ (us\ @\ [v]) \leq Suc\ (length\ us) \wedge$
 $snd\ (last\ (us\ @\ [v])) = snd\ v$
by *simp*
next
from B **and** C **and** D **and** E **show** $us\ @\ [v] \in A \sqcup B$
by (*cases* v , *cases* $snd\ (last\ us)$, *auto*)
qed
qed

lemma *ctying1-merge-aux-closed*:
assumes
 $A: \forall\ xs \in A. \forall\ ys \in A. \exists\ zs \in A.$
 $foldl\ (;\;) (\lambda x. None)\ zs = foldl\ (;\;) (\lambda x. None)\ (xs\ @\ ys)$ **and**
 $B: \forall\ xs \in B. \forall\ ys \in B. \exists\ zs \in B.$
 $foldl\ (;\;) (\lambda x. None)\ zs = foldl\ (;\;) (\lambda x. None)\ (xs\ @\ ys)$
shows $\llbracket us \in A \sqcup B; vs \in A \sqcup B \rrbracket \implies$
 $\exists\ ws \in A \sqcup B. foldl\ (;\;) (\lambda x. None)\ (concat\ (map\ fst\ ws)) =$
 $foldl\ (;\;) (\lambda x. None)\ (concat\ (map\ fst\ (us\ @\ vs))) \wedge$
 $length\ ws \leq length\ (us\ @\ vs) \wedge snd\ (last\ ws) = snd\ (last\ vs)$
(is $\llbracket -; - \rrbracket \implies \exists\ ws \in -. ?P\ ws\ us\ vs$ **)**
proof (*induction* $us\ @\ vs$ *arbitrary: us vs rule: length-induct*)
fix $us\ vs$
let $?f = foldl\ (;\;) (\lambda x. None)$
assume
 $C: \forall\ ts. length\ ts < length\ (us\ @\ vs) \longrightarrow$
 $(\forall\ ls\ rs. ts = ls\ @\ rs \longrightarrow ls \in A \sqcup B \longrightarrow rs \in A \sqcup B \longrightarrow$

```

    (∃ ws ∈ A ⊔ B. ?f (concat (map fst ws)) =
      ?f (concat (map fst (ls @ rs))) ∧
      length ws ≤ length (ls @ rs) ∧ snd (last ws) = snd (last rs)))
    (is ∀ -. - → (∀ ls rs. - → - → - → (∃ ws ∈ -. ?Q ws ls rs))) and
  D: us ∈ A ⊔ B and
  E: vs ∈ A ⊔ B
{
  fix vs' v
  assume F: vs = vs' @ [v]
  have ∃ ws ∈ A ⊔ B. ?f (concat (map fst ws)) =
    ?f (concat (map fst (us @ vs' @ [v]))) ∧
    length ws ≤ Suc (length us + length vs') ∧ snd (last ws) = snd v
  proof (cases vs', cases (¬ snd (last us)) = snd v)
    assume vs' = [] and (¬ snd (last us)) = snd v
    thus ?thesis
      using ctying1-merge-aux-closed-1 [OF - D] and
      ctying1-merge-aux-item [OF E] and C and F
      by (auto simp: less-Suc-eq-le)
  next
    have G: us ≠ []
      using D by (rule ctying1-merge-aux-nonempty)
    hence fst (last us) ∈ (if snd (last us) then A else B)
      using ctying1-merge-aux-item and D by auto
    moreover assume H: (¬ snd (last us)) ≠ snd v
    ultimately have fst (last us) ∈ (if snd v then A else B)
      by simp
    moreover have fst v ∈ (if snd v then A else B)
      using ctying1-merge-aux-item and E and F by auto
    ultimately have ∃ zs ∈ if snd v
      then A else B. ?f zs = ?f (concat (map fst [last us, v]))
      (is ∃ zs ∈ -. ?R zs)
      using A and B by auto
    then obtain zs where
      I: zs ∈ (if snd v then A else B) and J: ?R zs ..
    let ?w = (zs, snd v)
    assume K: vs' = []
    {
      fix us' u
      assume Cons: butlast us = u # us'
      hence L: snd v = (¬ snd (last (butlast us)))
        using D and H by (drule-tac ctying1-merge-aux-butlast, simp-all)
      let ?S = ?f (concat (map fst (butlast us)))
      have take (length (butlast us)) us ∈ A ⊔ B
        using Cons by (auto intro: ctying1-merge-aux-take [OF D])
      hence M: butlast us ∈ A ⊔ B
        by (subst (asm) (2) append-butlast-last-id [OF G, symmetric], simp)
      have N: ∀ ts. length ts < length (butlast us @ [last us, v]) →
        (∀ ls rs. ts = ls @ rs → ls ∈ A ⊔ B → rs ∈ A ⊔ B →
          (∃ ws ∈ A ⊔ B. ?Q ws ls rs))
    }
  }

```



```

    using  $C$  and  $F$  and  $K$  by (subst (asm) append-butlast-last-id
      [OF  $G$ , symmetric], simp)
  have  $\exists ws \in A \sqcup B. ?f (\text{concat } (\text{map fst } ws)) =$ 
     $?f (\text{concat } (\text{map fst } (\text{butlast } us @ [?w]))) \wedge$ 
     $\text{length } ws \leq \text{Suc } (\text{length } (\text{butlast } us)) \wedge \text{snd } (\text{last } ws) = \text{snd } ?w$ 
  proof (rule ctying1-merge-aux-closed-1)
    show  $\forall ts. \text{length } ts \leq \text{length } (\text{butlast } us) \longrightarrow$ 
       $(\forall ls \ rs. ts = ls @ rs \longrightarrow ls \in A \sqcup B \longrightarrow rs \in A \sqcup B \longrightarrow$ 
         $(\exists ws \in A \sqcup B. ?Q \ ws \ ls \ rs))$ 
    using  $N$  by force
  next
    from  $M$  show  $\text{butlast } us \in A \sqcup B$  .
  next
    show  $\text{fst } (zs, \text{snd } v) \in (\text{if } \text{snd } (zs, \text{snd } v) \text{ then } A \text{ else } B)$ 
    using  $I$  by simp
  next
    show  $\text{snd } (zs, \text{snd } v) = (\neg \text{snd } (\text{last } (\text{butlast } us)))$ 
    using  $L$  by simp
  qed
  moreover have  $\text{foldl } (;;) \ ?S \ zs =$ 
     $\text{foldl } (;;) \ ?S (\text{concat } (\text{map fst } [\text{last } us, v]))$ 
    using  $J$  by (rule ctying1-seq-eq)
  ultimately have  $\exists ws \in A \sqcup B. ?f (\text{concat } (\text{map fst } ws)) =$ 
     $?f (\text{concat } (\text{map fst } ((\text{butlast } us @ [\text{last } us]) @ [v]))) \wedge$ 
     $\text{length } ws \leq \text{Suc } (\text{length } us) \wedge \text{snd } (\text{last } ws) = \text{snd } v$ 
    by auto
}
with  $K$  and  $I$  and  $J$  show  $?thesis$ 
by (simp, subst append-butlast-last-id [OF  $G$ , symmetric],
  cases butlast us, (force split: if-split-asm)+)
next
case Cons
hence take  $(\text{length } vs') \ vs \in A \sqcup B$ 
by (auto intro: ctying1-merge-aux-take [OF  $E$ ])
hence  $vs' \in A \sqcup B$ 
using  $F$  by simp
then obtain  $ws$  where  $G: ws \in A \sqcup B$  and  $H: ?Q \ ws \ us \ vs'$ 
using  $C$  and  $D$  and  $F$  by force
have  $I: \forall ts. \text{length } ts \leq \text{length } ws \longrightarrow$ 
   $(\forall ls \ rs. ts = ls @ rs \longrightarrow ls \in A \sqcup B \longrightarrow rs \in A \sqcup B \longrightarrow$ 
     $(\exists ws \in A \sqcup B. ?Q \ ws \ ls \ rs))$ 
proof (rule allI, rule impI)
  fix  $ts :: (\text{state-upd list} \times \text{bool}) \text{ list}$ 
  assume  $J: \text{length } ts \leq \text{length } ws$ 
  show  $\forall ls \ rs. ts = ls @ rs \longrightarrow ls \in A \sqcup B \longrightarrow rs \in A \sqcup B \longrightarrow$ 
     $(\exists ws \in A \sqcup B. ?Q \ ws \ ls \ rs)$ 
  proof (rule spec [OF  $C$ , THEN mp])
    show  $\text{length } ts < \text{length } (us @ vs)$ 
    using  $F$  and  $H$  and  $J$  by simp
  end
end

```

```

    qed
  qed
  hence  $J$ :  $\text{snd } (\text{last } (\text{butlast } vs)) = (\neg \text{snd } (\text{last } vs))$ 
    by (metis  $E$   $F$   $\text{Cons}$   $\text{butlast-snoc}$   $\text{ctyping1-merge-aux-butlast}$ 
         $\text{list.distinct}(1)$ )
  have  $\exists ws' \in A \sqcup B$ .  $?f$  ( $\text{concat } (\text{map } \text{fst } ws')$ ) =
     $?f$  ( $\text{concat } (\text{map } \text{fst } (ws @ [v]))$ )  $\wedge$ 
     $\text{length } ws' \leq \text{Suc } (\text{length } ws) \wedge \text{snd } (\text{last } ws') = \text{snd } v$ 
  proof (rule  $\text{ctyping1-merge-aux-closed-1}$  [ $OF$   $I$   $G$ ])
    show  $\text{fst } v \in (\text{if } \text{snd } v \text{ then } A \text{ else } B)$ 
      by (rule  $\text{ctyping1-merge-aux-item}$  [ $OF$   $E$ ],  $\text{simp add: } F$ )
  next
    show  $\text{snd } v = (\neg \text{snd } (\text{last } ws))$ 
      using  $F$  and  $H$  and  $J$  by  $\text{simp}$ 
  qed
  thus  $?thesis$ 
    using  $H$  by  $\text{auto}$ 
  qed
}
note  $F = \text{this}$ 
show  $\exists ws \in A \sqcup B$ .  $?P$   $ws$   $us$   $vs$ 
proof (rule  $\text{rev-cases}$  [ $of$   $vs$ ])
  assume  $vs = []$ 
  thus  $?thesis$ 
    by ( $\text{simp add: ctyping1-merge-aux-nonempty}$  [ $OF$   $E$ ])
next
  fix  $vs' v$ 
  assume  $vs = vs' @ [v]$ 
  thus  $?thesis$ 
    using  $F$  by  $\text{simp}$ 
qed
qed

```

lemma $\text{ctyping1-merge-closed}$:

```

assumes
   $A$ :  $\forall xs \in A. \forall ys \in A. \exists zs \in A.$ 
     $\text{foldl } (;;) (\lambda x. \text{None}) zs = \text{foldl } (;;) (\lambda x. \text{None}) (xs @ ys)$  and
   $B$ :  $\forall xs \in B. \forall ys \in B. \exists zs \in B.$ 
     $\text{foldl } (;;) (\lambda x. \text{None}) zs = \text{foldl } (;;) (\lambda x. \text{None}) (xs @ ys)$  and
   $C$ :  $xs \in A \sqcup B$  and
   $D$ :  $ys \in A \sqcup B$ 
shows  $\exists zs \in A \sqcup B. \text{foldl } (;;) (\lambda x. \text{None}) zs =$ 
   $\text{foldl } (;;) (\lambda x. \text{None}) (xs @ ys)$ 
proof –
  let  $?f = \text{foldl } (;;) (\lambda x. \text{None})$ 
  obtain  $us$  where  $us \in A \sqcup B$  and
     $E$ :  $xs = \text{concat } (\text{map } \text{fst } us)$ 
  using  $C$  by ( $\text{auto simp: ctyping1-merge-def}$ )

```

moreover obtain vs **where** $vs \in A \sqcup B$ **and**
 $F: ys = \text{concat} (\text{map } \text{fst } vs)$
using D **by** (*auto simp: ctying1-merge-def*)
ultimately have $\exists ws \in A \sqcup B. ?f (\text{concat} (\text{map } \text{fst } ws)) =$
 $?f (\text{concat} (\text{map } \text{fst } (us @ vs))) \wedge$
 $\text{length } ws \leq \text{length } (us @ vs) \wedge \text{snd } (\text{last } ws) = \text{snd } (\text{last } vs)$
using A **and** B **by** (*blast intro: ctying1-merge-aux-closed*)
then obtain ws **where** $ws \in A \sqcup B$ **and**
 $?f (\text{concat} (\text{map } \text{fst } ws)) = ?f (xs @ ys)$
using E **and** F **by** *auto*
thus *?thesis*
by (*auto simp: ctying1-merge-def*)
qed

lemma *ctying1-merge-append-closed*:

assumes

$A: \forall xs \in A. \forall ys \in A. \exists zs \in A.$
 $\text{foldl } (;;) (\lambda x. \text{None}) zs = \text{foldl } (;;) (\lambda x. \text{None}) (xs @ ys)$ **and**
 $B: \forall xs \in B. \forall ys \in B. \exists zs \in B.$
 $\text{foldl } (;;) (\lambda x. \text{None}) zs = \text{foldl } (;;) (\lambda x. \text{None}) (xs @ ys)$ **and**
 $C: xs \in A \sqcup_{@} B$ **and**
 $D: ys \in A \sqcup_{@} B$

shows $\exists zs \in A \sqcup_{@} B. \text{foldl } (;;) (\lambda x. \text{None}) zs =$
 $\text{foldl } (;;) (\lambda x. \text{None}) (xs @ ys)$

proof –

let $?f = \text{foldl } (;;) (\lambda x. \text{None})$
{
assume $E: \text{card } B = \text{Suc } 0$
moreover from C **and this obtain** $as\ bs$ **where**
 $xs = as @ bs \wedge as \in A \wedge bs \in B$
by (*auto simp: ctying1-append-def ctying1-merge-append-def*)
moreover from D **and** E **obtain** $as'\ bs'$ **where**
 $ys = as' @ bs' \wedge as' \in A \wedge bs' \in B$
by (*auto simp: ctying1-append-def ctying1-merge-append-def*)
ultimately have $F: xs @ ys = as @ bs @ as' @ bs \wedge$
 $\{as, as'\} \subseteq A \wedge bs \in B$
by (*auto simp: card-1-singleton-iff*)
hence $?f (xs @ ys) = ?f (\text{remdups } (as @ \text{remdups } (bs @ as' @ bs)))$
by (*simp add: ctying1-seq-remdups*)
also have $\dots = ?f (\text{remdups } (as @ \text{remdups } (as' @ bs)))$
by (*simp add: remdups-append*)
finally have $G: ?f (xs @ ys) = ?f (as @ as' @ bs)$
by (*simp add: ctying1-seq-remdups*)
obtain as'' **where** $H: as'' \in A$ **and** $I: ?f as'' = ?f (as @ as')$
using A **and** F **by** *auto*
have $\exists zs \in A @ B. ?f zs = ?f (xs @ ys)$
proof (*rule bexI [of - as'' @ bs]*)
show $\text{foldl } (;;) (\lambda x. \text{None}) (as'' @ bs) =$
 $\text{foldl } (;;) (\lambda x. \text{None}) (xs @ ys)$

```

    using G and I by simp
next
  show  $as'' @ bs \in A @ B$ 
    using F and H by (auto simp: ctying1-append-def)
qed
}
moreover {
  fix n
  assume E:  $card\ B \neq Suc\ 0$ 
  moreover from C and this obtain  $ws\ bs$  where
     $xs = ws @ bs \wedge ws \in A \sqcup B \wedge bs \in B$ 
    by (auto simp: ctying1-append-def ctying1-merge-append-def)
  moreover from D and E obtain  $ws'\ bs'$  where
     $ys = ws' @ bs' \wedge ws' \in A \sqcup B \wedge bs' \in B$ 
    by (auto simp: ctying1-append-def ctying1-merge-append-def)
  ultimately have F:  $xs @ ys = ws @ bs @ ws' @ bs' \wedge$ 
     $\{ws, ws'\} \subseteq A \sqcup B \wedge \{bs, bs'\} \subseteq B$ 
    by simp
  hence  $[(bs, False)] \in A \sqcup B$ 
    by blast
  hence G:  $bs \in A \sqcup B$ 
    by (force simp: ctying1-merge-def)
  have  $\exists vs \in A \sqcup B. ?f\ vs = ?f\ (ws @ bs)$ 
    (is  $\exists vs \in \cdot. ?P\ vs\ ws\ bs$ )
  proof (rule ctying1-merge-closed)
    show  $\forall xs \in A. \forall ys \in A. \exists zs \in A. foldl\ (;;)\ (\lambda x. None)\ zs =$ 
       $foldl\ (;;)\ (\lambda x. None)\ (xs @ ys)$ 
    using A by simp
  next
    show  $\forall xs \in B. \forall ys \in B. \exists zs \in B. foldl\ (;;)\ (\lambda x. None)\ zs =$ 
       $foldl\ (;;)\ (\lambda x. None)\ (xs @ ys)$ 
    using B by simp
  next
    show  $ws \in A \sqcup B$ 
    using F by simp
  next
    from G show  $bs \in A \sqcup B$  .
  qed
  then obtain  $vs$  where H:  $vs \in A \sqcup B$  and I:  $?P\ vs\ ws\ bs$  ..
  have  $\exists vs' \in A \sqcup B. ?P\ vs'\ vs\ ws'$ 
  proof (rule ctying1-merge-closed)
    show  $\forall xs \in A. \forall ys \in A. \exists zs \in A. foldl\ (;;)\ (\lambda x. None)\ zs =$ 
       $foldl\ (;;)\ (\lambda x. None)\ (xs @ ys)$ 
    using A by simp
  next
    show  $\forall xs \in B. \forall ys \in B. \exists zs \in B. foldl\ (;;)\ (\lambda x. None)\ zs =$ 
       $foldl\ (;;)\ (\lambda x. None)\ (xs @ ys)$ 
    using B by simp
  next

```

```

    from H show  $vs \in A \sqcup B$  .
  next
    show  $ws' \in A \sqcup B$ 
    using F by simp
  qed
  then obtain  $vs'$  where  $J: vs' \in A \sqcup B$  and  $K: ?P\ vs'\ vs\ ws' ..$ 
  have  $\exists zs \in A \sqcup B @ B. ?f\ zs = ?f\ (xs @ ys)$ 
  proof (rule bexI [of -  $vs' @ bs'$ ])
    show  $foldl\ (;;)\ (\lambda x. None)\ (vs' @ bs') =$ 
       $foldl\ (;;)\ (\lambda x. None)\ (xs @ ys)$ 
    using F and I and K by simp
  next
    show  $vs' @ bs' \in A \sqcup B @ B$ 
    using F and J by (auto simp: ctyping1-append-def)
  qed
}
ultimately show ?thesis
using A and B and C and D by (auto simp: ctyping1-merge-append-def)
qed

```

lemma *ctyping1-aux-closed*:

```

 $\llbracket xs \in \vdash c; ys \in \vdash c \rrbracket \implies \exists zs \in \vdash c. foldl\ (;;)\ (\lambda x. None)\ zs =$ 
 $foldl\ (;;)\ (\lambda x. None)\ (xs @ ys)$ 
by (induction c arbitrary: xs ys, auto
intro: ctyping1-merge-closed ctyping1-merge-append-closed
simp: Let-def ctyping1-seq-def simp del: foldl-append)

```

lemma *ctyping1-idem-1*:

assumes

A: $s \in A$ and

B: $xs \in \vdash c$ and

C: $ys \in \vdash c$

shows $\exists f\ r.$

($\exists t.$

$(\lambda x. \text{case } foldl\ (;;)\ (\lambda x. None)\ ys\ x\ \text{of}$

$None \Rightarrow \text{case } foldl\ (;;)\ (\lambda x. None)\ xs\ x\ \text{of}$

$None \Rightarrow s\ x \mid \text{Some } None \Rightarrow t'\ x \mid \text{Some } (Some\ i) \Rightarrow i \mid$

$\text{Some } None \Rightarrow t''\ x \mid \text{Some } (Some\ i) \Rightarrow i) =$

$(\lambda x. \text{case } f\ x\ \text{of}$

$None \Rightarrow r\ x \mid \text{Some } None \Rightarrow t\ x \mid \text{Some } (Some\ i) \Rightarrow i)) \wedge$

$(\exists zs. f = foldl\ (;;)\ (\lambda x. None)\ zs \wedge zs \in \vdash c) \wedge$

$r \in A$

proof –

let $?f = foldl\ (;;)\ (\lambda x. None)$

let $?t = \lambda x. \text{case } ?f\ ys\ x\ \text{of}$

$None \Rightarrow \text{case } ?f\ xs\ x\ \text{of } \text{Some } None \Rightarrow t'\ x \mid - \Rightarrow (0 :: val) \mid$

$\text{Some } None \Rightarrow t''\ x \mid - \Rightarrow 0$

have $\exists zs \in \vdash c. ?f\ zs = ?f\ (xs @ ys)$

```

    using B and C by (rule ctying1-aux-closed)
  then obtain zs where zs ∈ ⊢ c and ?f zs = ?f (xs @ ys) ..
with A show ?thesis
  by (rule-tac exI [of - ?f zs], rule-tac exI [of - s],
      rule-tac conjI, rule-tac exI [of - ?t], fastforce dest: last-in-set
      simp: Let-def ctying1-seq-last split: option.split, blast)
qed

```

lemma *ctying1-idem-2*:

assumes

A: $s \in A$ **and**

B: $xs \in \vdash c$

shows $\exists f r.$

$(\exists t.$

$(\lambda x. \text{case foldl } (;;) (\lambda x. \text{None}) \text{ xs } x \text{ of}$

$\text{None} \Rightarrow s \ x \mid \text{Some None} \Rightarrow t' \ x \mid \text{Some (Some } i) \Rightarrow i) =$

$(\lambda x. \text{case } f \ x \text{ of}$

$\text{None} \Rightarrow r \ x \mid \text{Some None} \Rightarrow t \ x \mid \text{Some (Some } i) \Rightarrow i)) \wedge$

$(\exists xs. f = \text{foldl } (;;) (\lambda x. \text{None}) \text{ xs} \wedge xs \in \vdash c) \wedge$

$(\exists f s.$

$(\exists t. r = (\lambda x. \text{case } f \ x \text{ of}$

$\text{None} \Rightarrow s \ x \mid \text{Some None} \Rightarrow t \ x \mid \text{Some (Some } i) \Rightarrow i)) \wedge$

$(\exists xs. f = \text{foldl } (;;) (\lambda x. \text{None}) \text{ xs} \wedge xs \in \vdash c) \wedge$

$s \in A)$

proof –

let $?f = \text{foldl } (;;) (\lambda x. \text{None})$

let $?g = \lambda f s t x. \text{case } f \ x \text{ of}$

$\text{None} \Rightarrow s \ x \mid \text{Some None} \Rightarrow t \ x \mid \text{Some (Some } i) \Rightarrow i$

show ?thesis

by (rule exI [of - ?f xs], rule exI [of - ?g (?f xs) s t],

(fastforce simp: A B split: option.split)+)

qed

lemma *ctying1-idem*:

$\vdash c (\subseteq A, X) = (B, Y) \implies \vdash c (\subseteq B, Y) = (B, Y)$

by (cases A = {}, auto simp: ctying1-def

intro: ctying1-idem-1 ctying1-idem-2)

end

end

3 Overapproximation of program semantics by the type system

theory *Overapproximation*

imports *Idempotence*

begin

The purpose of this section is to prove that type system *ctyping2* overapproximates program semantics, namely that if (a) $(c, s) \Rightarrow t$, (b) the type system outputs a *state set* B and a *vname set* Y when it is input program c , *state set* A , and *vname set* X , and (c) state s agrees with a state in A on the value of every state variable in X , then t must agree with some state in B on the value of every state variable in Y (lemma *ctyping2-approx*).

This proof makes use of the lemma *ctyping1-idem* proven in the previous section.

3.1 Global context proofs

lemma *avars-aval*:

$s = t \ (\subseteq \text{avars } a) \implies \text{aval } a \ s = \text{aval } a \ t$
by (*induction a, simp-all*)

3.2 Local context proofs

context *noninterf*
begin

lemma *interf-set-mono*:

$\llbracket A' \subseteq A; X \subseteq X'; \forall (B', Y') \in U'. \exists (B, Y) \in U. B' \subseteq B \wedge Y' \subseteq Y; \forall (B, Y) \in \text{insert } (\text{Univ? } A \ X, Z) \ U. B: \text{dom } 'Y \rightsquigarrow W \rrbracket \implies$
 $\forall (B, Y) \in \text{insert } (\text{Univ? } A' \ X', Z) \ U'. B: \text{dom } 'Y \rightsquigarrow W$
by (*subgoal-tac Univ? A' X' \subseteq Univ? A X, fastforce,*
auto simp: univ-states-if-def)

lemma *btying1-btying2-aux-1* [*elim*]:

assumes

$A: \text{avars } a_1 = \{\}$ **and**

$B: \text{avars } a_2 = \{\}$ **and**

$C: \text{aval } a_1 \ (\lambda x. 0) < \text{aval } a_2 \ (\lambda x. 0)$

shows $\text{aval } a_1 \ s < \text{aval } a_2 \ s$

proof –

have $\text{aval } a_1 \ s = \text{aval } a_1 \ (\lambda x. 0) \wedge \text{aval } a_2 \ s = \text{aval } a_2 \ (\lambda x. 0)$

using A **and** B **by** (*blast intro: avars-aval*)

thus *?thesis*

using C **by** *simp*

qed

lemma *btying1-btying2-aux-2* [*elim*]:

assumes

$A: \text{avars } a_1 = \{\}$ **and**

$B: \text{avars } a_2 = \{\}$ **and**

$C: \neg \text{aval } a_1 \ (\lambda x. 0) < \text{aval } a_2 \ (\lambda x. 0)$ **and**

$D: \text{aval } a_1 \ s < \text{aval } a_2 \ s$
shows *False*
proof –
 $\text{have } \text{aval } a_1 \ s = \text{aval } a_1 \ (\lambda x. 0) \wedge \text{aval } a_2 \ s = \text{aval } a_2 \ (\lambda x. 0)$
 $\text{using } A \text{ and } B \text{ by } (\text{blast intro: avars-aval})$
 $\text{thus } ?thesis$
 $\text{using } C \text{ and } D \text{ by simp}$
qed

lemma *btyping1-btyping2-aux*:
 $\vdash b = \text{Some } v \implies \models b (\subseteq A, X) = \text{Some } (\text{if } v \text{ then } A \text{ else } \{\})$
by (*induction b arbitrary: v, auto split: if-split-asm option.split-asm*)

lemma *btyping1-btyping2*:
 $\vdash b = \text{Some } v \implies \models b (\subseteq A, X) = (\text{if } v \text{ then } (A, \{\}) \text{ else } (\{\}, A))$
by (*simp add: btyping2-def btyping1-btyping2-aux*)

lemma *btyping2-aux-subset*:
 $\models b (\subseteq A, X) = \text{Some } A' \implies A' = \{s. s \in A \wedge \text{bval } b \ s\}$
by (*induction b arbitrary: A', auto split: if-split-asm option.split-asm*)

lemma *btyping2-aux-diff*:
 $\models b (\subseteq A, X) = \text{Some } B; \models b (\subseteq A', X') = \text{Some } B'; A' \subseteq A; B' \subseteq B \implies$
 $A' - B' \subseteq A - B$
by (*blast dest: btyping2-aux-subset*)

lemma *btyping2-aux-mono*:
 $\models b (\subseteq A, X) = \text{Some } B; A' \subseteq A; X \subseteq X' \implies$
 $\exists B'. \models b (\subseteq A', X') = \text{Some } B' \wedge B' \subseteq B$
by (*induction b arbitrary: B, auto dest: btyping2-aux-diff split: if-split-asm option.split-asm*)

lemma *btyping2-mono*:
 $\models b (\subseteq A, X) = (B_1, B_2); \models b (\subseteq A', X') = (B_1', B_2'); A' \subseteq A; X \subseteq X' \implies$
 $B_1' \subseteq B_1 \wedge B_2' \subseteq B_2$
by (*simp add: btyping2-def split: option.split-asm, frule-tac [3-4] btyping2-aux-mono, auto dest: btyping2-aux-subset*)

lemma *btyping2-un-eq*:
 $\models b (\subseteq A, X) = (B_1, B_2) \implies B_1 \cup B_2 = A$
by (*auto simp: btyping2-def dest: btyping2-aux-subset split: option.split-asm*)

lemma *btyping2-fst-empty*:
 $\models b (\subseteq \{\}, X) = (\{\}, \{\})$
by (*auto simp: btyping2-def dest: btyping2-aux-subset split: option.split*)

lemma *btyping2-aux-eq*:
 $\models b (\subseteq A, X) = \text{Some } A'; s = t (\subseteq \text{state} \cap X) \implies \text{bval } b \ s = \text{bval } b \ t$
proof (*induction b arbitrary: A'*)


```

fix A' v
show
   $\llbracket Bc\ v\ (\subseteq A, X) = Some\ A';\ s = t\ (\subseteq state \cap X) \rrbracket \implies$ 
   $bval\ (Bc\ v)\ s = bval\ (Bc\ v)\ t$ 
  by simp
next
fix A' b
show
   $\llbracket \bigwedge A'.\ \models b\ (\subseteq A, X) = Some\ A' \implies s = t\ (\subseteq state \cap X) \implies$ 
   $bval\ b\ s = bval\ b\ t;$ 
   $\models Not\ b\ (\subseteq A, X) = Some\ A';\ s = t\ (\subseteq state \cap X) \rrbracket \implies$ 
   $bval\ (Not\ b)\ s = bval\ (Not\ b)\ t$ 
  by (simp split: option.split-asm)
next
fix A' b1 b2
show
   $\llbracket \bigwedge A'.\ \models b_1\ (\subseteq A, X) = Some\ A' \implies s = t\ (\subseteq state \cap X) \implies$ 
   $bval\ b_1\ s = bval\ b_1\ t;$ 
   $\bigwedge A'.\ \models b_2\ (\subseteq A, X) = Some\ A' \implies s = t\ (\subseteq state \cap X) \implies$ 
   $bval\ b_2\ s = bval\ b_2\ t;$ 
   $\models And\ b_1\ b_2\ (\subseteq A, X) = Some\ A';\ s = t\ (\subseteq state \cap X) \rrbracket \implies$ 
   $bval\ (And\ b_1\ b_2)\ s = bval\ (And\ b_1\ b_2)\ t$ 
  by (simp split: option.split-asm)
next
fix A' a1 a2
show
   $\llbracket \models Less\ a_1\ a_2\ (\subseteq A, X) = Some\ A';\ s = t\ (\subseteq state \cap X) \rrbracket \implies$ 
   $bval\ (Less\ a_1\ a_2)\ s = bval\ (Less\ a_1\ a_2)\ t$ 
  by (subgoal-tac aval a1 s = aval a1 t,
  subgoal-tac aval a2 s = aval a2 t,
  auto intro!: avars-aval split: if-split-asm)
qed

```

lemma *ctyping1-merge-in*:
 $xs \in A \cup B \implies xs \in A \sqcup B$
by (*force simp: ctyping1-merge-def*)

lemma *ctyping1-merge-append-in*:
 $\llbracket xs \in A;\ ys \in B \rrbracket \implies xs\ @\ ys \in A \sqcup_{@} B$
by (*force simp: ctyping1-merge-append-def ctyping1-append-def ctyping1-merge-in*)

lemma *ctyping1-aux-nonempty*:
 $\vdash c \neq \{\}$
by (*induction c, simp-all add: Let-def ctyping1-append-def*
ctyping1-merge-def ctyping1-merge-append-def, fastforce+)

lemma *ctyping1-mono*:
 $\llbracket (B, Y) = \vdash c\ (\subseteq A, X);\ (B', Y') = \vdash c\ (\subseteq A', X');\ A' \subseteq A;\ X \subseteq X' \rrbracket \implies$

$B' \subseteq B \wedge Y \subseteq Y'$
by (*auto simp: ctying1-def*)

lemma *ctying2-fst-empty*:

Some $(B, Y) = (U, v) \models c (\subseteq \{\}, X) \implies (B, Y) = (\{\}, UNIV)$

proof (*induction* $(U, v) \models c \{\} :: \text{state set } X \text{ arbitrary: } B \ Y \ U \ v$

rule: ctying2.induct)

fix $C \ X \ Y \ U \ v \ b \ c_1 \ c_2$

show

$\llbracket \bigwedge U' \ p \ B_2 \ C \ Y.$

$(U', p) = (\text{insert } (Univ? \ \{\} \ X, \text{bvars } b) \ U, \models b (\subseteq \{\}, X)) \implies$

$(\{\}, B_2) = p \implies \text{Some } (C, Y) = (U', v) \models c_1 (\subseteq \{\}, X) \implies$

$(C, Y) = (\{\}, UNIV);$

$\bigwedge U' \ p \ B_1 \ C \ Y.$

$(U', p) = (\text{insert } (Univ? \ \{\} \ X, \text{bvars } b) \ U, \models b (\subseteq \{\}, X)) \implies$

$(B_1, \{\}) = p \implies \text{Some } (C, Y) = (U', v) \models c_2 (\subseteq \{\}, X) \implies$

$(C, Y) = (\{\}, UNIV);$

$\text{Some } (C, Y) = (U, v) \models \text{IF } b \ \text{THEN } c_1 \ \text{ELSE } c_2 (\subseteq \{\}, X) \rrbracket \implies$

$(C, Y) = (\{\}, UNIV)$

by (*fastforce simp: btying2-fst-empty split: option.split-asm*)

next

fix $B \ X \ Z \ U \ v \ b \ c$

show

$\llbracket \bigwedge B_2 \ C \ Y \ B_1' \ B_2' \ B \ Z.$

$(\{\}, B_2) = \models b (\subseteq \{\}, X) \implies$

$(C, Y) = \vdash c (\subseteq \{\}, X) \implies$

$(B_1', B_2') = \models b (\subseteq C, Y) \implies$

$\forall (B, W) \in \text{insert } (Univ? \ \{\} \ X \cup Univ? \ C \ Y, \text{bvars } b) \ U.$

$B: \text{dom } 'W \rightsquigarrow UNIV \implies$

$\text{Some } (B, Z) = (\{\}, \text{False}) \models c (\subseteq \{\}, X) \implies$

$(B, Z) = (\{\}, UNIV);$

$\bigwedge B_1 \ B_2 \ C \ Y \ B_2' \ B \ Z.$

$(B_1, B_2) = \models b (\subseteq \{\}, X) \implies$

$(C, Y) = \vdash c (\subseteq B_1, X) \implies$

$(\{\}, B_2') = \models b (\subseteq C, Y) \implies$

$\forall (B, W) \in \text{insert } (Univ? \ \{\} \ X \cup Univ? \ C \ Y, \text{bvars } b) \ U.$

$B: \text{dom } 'W \rightsquigarrow UNIV \implies$

$\text{Some } (B, Z) = (\{\}, \text{False}) \models c (\subseteq \{\}, Y) \implies$

$(B, Z) = (\{\}, UNIV);$

$\text{Some } (B, Z) = (U, v) \models \text{WHILE } b \ \text{DO } c (\subseteq \{\}, X) \rrbracket \implies$

$(B, Z) = (\{\}, UNIV)$

by (*simp split: if-split-asm option.split-asm prod.split-asm,*

(fastforce simp: btying2-fst-empty ctying1-def)+)

qed (*simp-all split: if-split-asm option.split-asm prod.split-asm*)

lemma *ctying2-mono-assign* [*elim!*]:

$\llbracket (U, \text{False}) \models x ::= a (\subseteq A, X) = \text{Some } (C, Z); A' \subseteq A; X \subseteq X';$

$\forall (B', Y') \in U'. \exists (B, Y) \in U. B' \subseteq B \wedge Y' \subseteq Y \rrbracket \implies$

$\exists C' Z'. (U', False) \models x ::= a (\subseteq A', X') = Some (C', Z') \wedge$
 $C' \subseteq C \wedge Z \subseteq Z'$
by (*frule interf-set-mono [where $W = \{dom\ x\}$], auto split: if-split-asm*)

lemma *ctyping2-mono-seq*:

assumes

$A: \bigwedge A' B X' Y U'.$

$(U, False) \models c_1 (\subseteq A, X) = Some (B, Y) \implies A' \subseteq A \implies X \subseteq X' \implies$

$\forall (B', Y') \in U'. \exists (B, Y) \in U. B' \subseteq B \wedge Y' \subseteq Y \implies$

$\exists B' Y'. (U', False) \models c_1 (\subseteq A', X') = Some (B', Y') \wedge$

$B' \subseteq B \wedge Y \subseteq Y'$ **and**

$B: \bigwedge_p B Y B' C Y' Z U'.$

$(U, False) \models c_1 (\subseteq A, X) = Some\ p \implies (B, Y) = p \implies$

$(U, False) \models c_2 (\subseteq B, Y) = Some (C, Z) \implies B' \subseteq B \implies Y \subseteq Y' \implies$

$\forall (B', Y') \in U'. \exists (B, Y) \in U. B' \subseteq B \wedge Y' \subseteq Y \implies$

$\exists C' Z'. (U', False) \models c_2 (\subseteq B', Y') = Some (C', Z') \wedge$

$C' \subseteq C \wedge Z \subseteq Z'$ **and**

$C: (U, False) \models c_1;; c_2 (\subseteq A, X) = Some (C, Z)$ **and**

$D: A' \subseteq A$ **and**

$E: X \subseteq X'$ **and**

$F: \forall (B', Y') \in U'. \exists (B, Y) \in U. B' \subseteq B \wedge Y' \subseteq Y$

shows $\exists C' Z'. (U', False) \models c_1;; c_2 (\subseteq A', X') = Some (C', Z') \wedge$

$C' \subseteq C \wedge Z \subseteq Z'$

proof –

obtain $B\ Y$ **where** $(U, False) \models c_1 (\subseteq A, X) = Some (B, Y) \wedge$

$(U, False) \models c_2 (\subseteq B, Y) = Some (C, Z)$

using C **by** (*auto split: option.split-asm*)

moreover from this obtain $B'\ Y'$ **where**

$G: (U', False) \models c_1 (\subseteq A', X') = Some (B', Y') \wedge B' \subseteq B \wedge Y \subseteq Y'$

using A **and** D **and** E **and** F **by** *fastforce*

ultimately obtain $C'\ Z'$ **where**

$(U', False) \models c_2 (\subseteq B', Y') = Some (C', Z') \wedge C' \subseteq C \wedge Z \subseteq Z'$

using B **and** F **by** *fastforce*

thus *?thesis*

using G **by** *simp*

qed

lemma *ctyping2-mono-if*:

assumes

$A: \bigwedge W\ p\ B_1\ B_2\ B_1'\ C_1\ X'\ Y_1\ W'. (W, p) =$

$(insert\ (Univ?\ A\ X,\ bvars\ b)\ U, \models b (\subseteq A, X)) \implies (B_1, B_2) = p \implies$

$(W, False) \models c_1 (\subseteq B_1, X) = Some (C_1, Y_1) \implies B_1' \subseteq B_1 \implies$

$X \subseteq X' \implies \forall (B', Y') \in W'. \exists (B, Y) \in W. B' \subseteq B \wedge Y' \subseteq Y \implies$

$\exists C_1'\ Y_1'. (W', False) \models c_1 (\subseteq B_1', X') = Some (C_1', Y_1') \wedge$

$C_1' \subseteq C_1 \wedge Y_1 \subseteq Y_1'$ **and**

$B: \bigwedge W\ p\ B_1\ B_2\ B_2'\ C_2\ X'\ Y_2\ W'. (W, p) =$

$(insert\ (Univ?\ A\ X,\ bvars\ b)\ U, \models b (\subseteq A, X)) \implies (B_1, B_2) = p \implies$

$(W, False) \models c_2 (\subseteq B_2, X) = Some (C_2, Y_2) \implies B_2' \subseteq B_2 \implies$

$X \subseteq X' \implies \forall (B', Y') \in W'. \exists (B, Y) \in W. B' \subseteq B \wedge Y' \subseteq Y \implies$

$\exists C_2' Y_2'. (W', False) \models c_2 (\subseteq B_2', X') = Some (C_2', Y_2') \wedge$
 $C_2' \subseteq C_2 \wedge Y_2 \subseteq Y_2'$ **and**
 $C: (U, False) \models IF\ b\ THEN\ c_1\ ELSE\ c_2 (\subseteq A, X) = Some (C, Y)$ **and**
 $D: A' \subseteq A$ **and**
 $E: X \subseteq X'$ **and**
 $F: \forall (B', Y') \in U'. \exists (B, Y) \in U. B' \subseteq B \wedge Y' \subseteq Y$
shows $\exists C' Y'. (U', False) \models IF\ b\ THEN\ c_1\ ELSE\ c_2 (\subseteq A', X') =$
 $Some (C', Y') \wedge C' \subseteq C \wedge Y \subseteq Y'$
proof –
let $?W = insert\ (Univ?\ A\ X,\ bvars\ b)\ U$
let $?W' = insert\ (Univ?\ A'\ X',\ bvars\ b)\ U'$
obtain $B_1\ B_2\ C_1\ C_2\ Y_1\ Y_2$ **where**
 $G: (C, Y) = (C_1 \cup C_2, Y_1 \cap Y_2) \wedge (B_1, B_2) = \models b (\subseteq A, X) \wedge$
 $Some (C_1, Y_1) = (?W, False) \models c_1 (\subseteq B_1, X) \wedge$
 $Some (C_2, Y_2) = (?W, False) \models c_2 (\subseteq B_2, X)$
using C **by** (*simp split: option.split-asm prod.split-asm*)
moreover obtain $B_1'\ B_2'$ **where** $H: (B_1', B_2') = \models b (\subseteq A', X')$
by (*cases* $\models b (\subseteq A', X')$, *simp*)
ultimately have $I: B_1' \subseteq B_1 \wedge B_2' \subseteq B_2$
by (*metis btyping2-mono D E*)
moreover have $J: \forall (B', Y') \in ?W'. \exists (B, Y) \in ?W. B' \subseteq B \wedge Y' \subseteq Y$
using D **and** E **and** F **by** (*auto simp: univ-states-if-def*)
ultimately have $\exists C_1' Y_1'$.
 $(?W', False) \models c_1 (\subseteq B_1', X') = Some (C_1', Y_1') \wedge C_1' \subseteq C_1 \wedge Y_1 \subseteq Y_1'$
using A **and** E **and** G **by force**
moreover have $\exists C_2' Y_2'$.
 $(?W', False) \models c_2 (\subseteq B_2', X') = Some (C_2', Y_2') \wedge C_2' \subseteq C_2 \wedge Y_2 \subseteq Y_2'$
using B **and** E **and** G **and** I **and** J **by force**
ultimately show *?thesis*
using G **and** H **by** (*auto split: prod.split*)
qed

lemma *ctyping2-mono-while*:

assumes

$A: \bigwedge B_1\ B_2\ C\ Y\ B_1'\ B_2'\ D_1\ E\ X'\ V\ U'. (B_1, B_2) = \models b (\subseteq A, X) \implies$
 $(C, Y) = \vdash c (\subseteq B_1, X) \implies (B_1', B_2') = \models b (\subseteq C, Y) \implies$
 $\forall (B, W) \in insert\ (Univ?\ A\ X \cup Univ?\ C\ Y,\ bvars\ b)\ U.$
 $B: dom\ 'W \rightsquigarrow UNIV \implies$
 $(\{\}, False) \models c (\subseteq B_1, X) = Some (E, V) \implies D_1 \subseteq B_1 \implies$
 $X \subseteq X' \implies \forall (B', Y') \in U'. \exists (B, Y) \in \{\}. B' \subseteq B \wedge Y' \subseteq Y \implies$
 $\exists E'\ V'. (U', False) \models c (\subseteq D_1, X') = Some (E', V') \wedge$
 $E' \subseteq E \wedge V \subseteq V'$ **and**
 $B: \bigwedge B_1\ B_2\ C\ Y\ B_1'\ B_2'\ D_1'\ F\ Y'\ W\ U'. (B_1, B_2) = \models b (\subseteq A, X) \implies$
 $(C, Y) = \vdash c (\subseteq B_1, X) \implies (B_1', B_2') = \models b (\subseteq C, Y) \implies$
 $\forall (B, W) \in insert\ (Univ?\ A\ X \cup Univ?\ C\ Y,\ bvars\ b)\ U.$
 $B: dom\ 'W \rightsquigarrow UNIV \implies$
 $(\{\}, False) \models c (\subseteq B_1', Y) = Some (F, W) \implies D_1' \subseteq B_1' \implies$
 $Y \subseteq Y' \implies \forall (B', Y') \in U'. \exists (B, Y) \in \{\}. B' \subseteq B \wedge Y' \subseteq Y \implies$
 $\exists F'\ W'. (U', False) \models c (\subseteq D_1', Y') = Some (F', W') \wedge$

$F' \subseteq F \wedge W \subseteq W'$ **and**
 $C: (U, \text{False}) \models \text{WHILE } b \text{ DO } c (\subseteq A, X) = \text{Some } (B, Z)$ **and**
 $D: A' \subseteq A$ **and**
 $E: X \subseteq X'$ **and**
 $F: \forall (B', Y') \in U'. \exists (B, Y) \in U. B' \subseteq B \wedge Y' \subseteq Y$
shows $\exists B' Z'. (U', \text{False}) \models \text{WHILE } b \text{ DO } c (\subseteq A', X') = \text{Some } (B', Z') \wedge$
 $B' \subseteq B \wedge Z \subseteq Z'$
proof –
obtain $B_1 B_1' B_2 B_2' C E F V W Y$ **where** $G: (B_1, B_2) = \models b (\subseteq A, X) \wedge$
 $(C, Y) = \vdash c (\subseteq B_1, X) \wedge (B_1', B_2') = \models b (\subseteq C, Y) \wedge$
 $(\forall (B, W) \in \text{insert } (\text{Univ? } A \ X \cup \text{Univ? } C \ Y, \text{bvars } b) \ U).$
 $B: \text{dom } ' W \rightsquigarrow \text{UNIV}) \wedge$
 $\text{Some } (E, V) = (\{\}, \text{False}) \models c (\subseteq B_1, X) \wedge$
 $\text{Some } (F, W) = (\{\}, \text{False}) \models c (\subseteq B_1', Y) \wedge$
 $(B, Z) = (B_2 \cup B_2', \text{Univ?? } B_2 \ X \cap Y)$
using C **by** (*force split: if-split-asm option.split-asm prod.split-asm*)
moreover obtain $D_1 D_2$ **where** $H: \models b (\subseteq A', X') = (D_1, D_2)$
by (*cases* $\models b (\subseteq A', X')$, *simp*)
ultimately have $I: D_1 \subseteq B_1 \wedge D_2 \subseteq B_2$
by (*smt (verit) btyping2-mono D E*)
moreover obtain $C' Y'$ **where** $J: (C', Y') = \vdash c (\subseteq D_1, X')$
by (*cases* $\vdash c (\subseteq D_1, X')$, *simp*)
ultimately have $K: C' \subseteq C \wedge Y \subseteq Y'$
by (*meson ctyping1-mono E G*)
moreover obtain $D_1' D_2'$ **where** $L: \models b (\subseteq C', Y') = (D_1', D_2')$
by (*cases* $\models b (\subseteq C', Y')$, *simp*)
ultimately have $M: D_1' \subseteq B_1' \wedge D_2' \subseteq B_2'$
by (*smt (verit) btyping2-mono G*)
then obtain $F' W'$ **where**
 $(\{\}, \text{False}) \models c (\subseteq D_1', Y') = \text{Some } (F', W') \wedge F' \subseteq F \wedge W \subseteq W'$
using B **and** F **and** G **and** K **by** *force*
moreover obtain $E' V'$ **where**
 $(\{\}, \text{False}) \models c (\subseteq D_1, X') = \text{Some } (E', V') \wedge E' \subseteq E \wedge V \subseteq V'$
using A **and** E **and** F **and** G **and** I **by** *force*
moreover have $\text{Univ? } A' \ X' \subseteq \text{Univ? } A \ X$
using D **and** E **by** (*auto simp: univ-states-if-def*)
moreover have $\text{Univ? } C' \ Y' \subseteq \text{Univ? } C \ Y$
using K **by** (*auto simp: univ-states-if-def*)
ultimately have $(U', \text{False}) \models \text{WHILE } b \text{ DO } c (\subseteq A', X') =$
 $\text{Some } (D_2 \cup D_2', \text{Univ?? } D_2 \ X' \cap Y')$
using F **and** G **and** H **and** J [*symmetric*] **and** L **by** *force*
moreover have $D_2 \cup D_2' \subseteq B$
using G **and** I **and** M **by** *auto*
moreover have $Z \subseteq \text{Univ?? } D_2 \ X' \cap Y'$
using E **and** G **and** I **and** K **by** *auto*
ultimately show *?thesis*
by *simp*
qed

lemma *ctyping2-mono*:

$\llbracket (U, \text{False}) \models c \ (\subseteq A, X) = \text{Some } (C, Z); A' \subseteq A; X \subseteq X';$
 $\forall (B', Y') \in U'. \exists (B, Y) \in U. B' \subseteq B \wedge Y' \subseteq Y \rrbracket \implies$
 $\exists C' Z'. (U', \text{False}) \models c \ (\subseteq A', X') = \text{Some } (C', Z') \wedge C' \subseteq C \wedge Z \subseteq Z'$
proof (*induction* $(U, \text{False}) \models c \ A \ X$ *arbitrary*: $A' \ C \ X' \ Z \ U \ U'$)

rule: *ctyping2.induct*)

fix $A \ A' \ X \ X' \ U \ U' \ C \ Z \ c_1 \ c_2$

show

$\llbracket \bigwedge A' \ B \ X' \ Y \ U'.$

$(U, \text{False}) \models c_1 \ (\subseteq A, X) = \text{Some } (B, Y) \implies$

$A' \subseteq A \implies X \subseteq X' \implies$

$\forall (B', Y') \in U'. \exists (B, Y) \in U. B' \subseteq B \wedge Y' \subseteq Y \implies$

$\exists B' Y'. (U', \text{False}) \models c_1 \ (\subseteq A', X') = \text{Some } (B', Y') \wedge$

$B' \subseteq B \wedge Y' \subseteq Y;$

$\bigwedge p \ B \ Y \ A' \ C \ X' \ Z \ U'. (U, \text{False}) \models c_1 \ (\subseteq A, X) = \text{Some } p \implies$

$(B, Y) = p \implies (U, \text{False}) \models c_2 \ (\subseteq B, Y) = \text{Some } (C, Z) \implies$

$A' \subseteq B \implies Y \subseteq X' \implies$

$\forall (B', Y') \in U'. \exists (B, Y) \in U. B' \subseteq B \wedge Y' \subseteq Y \implies$

$\exists C' Z'. (U', \text{False}) \models c_2 \ (\subseteq A', X') = \text{Some } (C', Z') \wedge$

$C' \subseteq C \wedge Z \subseteq Z';$

$(U, \text{False}) \models c_1;; c_2 \ (\subseteq A, X) = \text{Some } (C, Z);$

$A' \subseteq A; X \subseteq X';$

$\forall (B', Y') \in U'. \exists (B, Y) \in U. B' \subseteq B \wedge Y' \subseteq Y \rrbracket \implies$

$\exists C' Z'. (U', \text{False}) \models c_1;; c_2 \ (\subseteq A', X') = \text{Some } (C', Z') \wedge$

$C' \subseteq C \wedge Z \subseteq Z'$

by (*rule ctyping2-mono-seq*)

next

fix $A \ A' \ X \ X' \ U \ U' \ C \ Z \ b \ c_1 \ c_2$

show

$\llbracket \bigwedge U'' \ p \ B_1 \ B_2 \ A' \ C \ X' \ Z \ U'.$

$(U'', p) = (\text{insert } (\text{Univ? } A \ X, \text{bvars } b) \ U, \models b \ (\subseteq A, X)) \implies$

$(B_1, B_2) = p \implies (U'', \text{False}) \models c_1 \ (\subseteq B_1, X) = \text{Some } (C, Z) \implies$

$A' \subseteq B_1 \implies X \subseteq X' \implies$

$\forall (B', Y') \in U'. \exists (B, Y) \in U''. B' \subseteq B \wedge Y' \subseteq Y \implies$

$\exists C' Z'. (U', \text{False}) \models c_1 \ (\subseteq A', X') = \text{Some } (C', Z') \wedge$

$C' \subseteq C \wedge Z \subseteq Z';$

$\bigwedge U'' \ p \ B_1 \ B_2 \ A' \ C \ X' \ Z \ U'.$

$(U'', p) = (\text{insert } (\text{Univ? } A \ X, \text{bvars } b) \ U, \models b \ (\subseteq A, X)) \implies$

$(B_1, B_2) = p \implies (U'', \text{False}) \models c_2 \ (\subseteq B_2, X) = \text{Some } (C, Z) \implies$

$A' \subseteq B_2 \implies X \subseteq X' \implies$

$\forall (B', Y') \in U'. \exists (B, Y) \in U''. B' \subseteq B \wedge Y' \subseteq Y \implies$

$\exists C' Z'. (U', \text{False}) \models c_2 \ (\subseteq A', X') = \text{Some } (C', Z') \wedge$

$C' \subseteq C \wedge Z \subseteq Z';$

$(U, \text{False}) \models \text{IF } b \ \text{THEN } c_1 \ \text{ELSE } c_2 \ (\subseteq A, X) = \text{Some } (C, Z);$

$A' \subseteq A; X \subseteq X';$

$\forall (B', Y') \in U'. \exists (B, Y) \in U. B' \subseteq B \wedge Y' \subseteq Y \rrbracket \implies$

$\exists C' Z'. (U', \text{False}) \models \text{IF } b \ \text{THEN } c_1 \ \text{ELSE } c_2 \ (\subseteq A', X') =$

$\text{Some } (C', Z') \wedge C' \subseteq C \wedge Z \subseteq Z'$

by (*rule ctyping2-mono-if*)

```

next
fix A A' X X' U U' B Z b c
show
   $\llbracket \bigwedge B_1 B_2 C Y B_1' B_2' A' B X' Z U' .$ 
     $(B_1, B_2) = \models b (\subseteq A, X) \implies$ 
     $(C, Y) = \vdash c (\subseteq B_1, X) \implies$ 
     $(B_1', B_2') = \models b (\subseteq C, Y) \implies$ 
     $\forall (B, W) \in \text{insert } (\text{Univ? } A X \cup \text{Univ? } C Y, \text{bvars } b) U.$ 
       $B: \text{dom } ' W \rightsquigarrow \text{UNIV} \implies$ 
       $(\{\}, \text{False}) \models c (\subseteq B_1, X) = \text{Some } (B, Z) \implies$ 
       $A' \subseteq B_1 \implies X \subseteq X' \implies$ 
       $\forall (B', Y') \in U'. \exists (B, Y) \in \{\}. B' \subseteq B \wedge Y' \subseteq Y \implies$ 
       $\exists B' Z'. (U', \text{False}) \models c (\subseteq A', X') = \text{Some } (B', Z') \wedge$ 
       $B' \subseteq B \wedge Z \subseteq Z';$ 
     $\bigwedge B_1 B_2 C Y B_1' B_2' A' B X' Z U' .$ 
       $(B_1, B_2) = \models b (\subseteq A, X) \implies$ 
       $(C, Y) = \vdash c (\subseteq B_1, X) \implies$ 
       $(B_1', B_2') = \models b (\subseteq C, Y) \implies$ 
       $\forall (B, W) \in \text{insert } (\text{Univ? } A X \cup \text{Univ? } C Y, \text{bvars } b) U.$ 
         $B: \text{dom } ' W \rightsquigarrow \text{UNIV} \implies$ 
         $(\{\}, \text{False}) \models c (\subseteq B_1', Y) = \text{Some } (B, Z) \implies$ 
         $A' \subseteq B_1' \implies Y \subseteq X' \implies$ 
         $\forall (B', Y') \in U'. \exists (B, Y) \in \{\}. B' \subseteq B \wedge Y' \subseteq Y \implies$ 
         $\exists B' Z'. (U', \text{False}) \models c (\subseteq A', X') = \text{Some } (B', Z') \wedge$ 
         $B' \subseteq B \wedge Z \subseteq Z';$ 
       $(U, \text{False}) \models \text{WHILE } b \text{ DO } c (\subseteq A, X) = \text{Some } (B, Z);$ 
       $A' \subseteq A; X \subseteq X';$ 
       $\forall (B', Y') \in U'. \exists (B, Y) \in U. B' \subseteq B \wedge Y' \subseteq Y \implies$ 
       $\exists B' Z'. (U', \text{False}) \models \text{WHILE } b \text{ DO } c (\subseteq A', X') =$ 
       $\text{Some } (B', Z') \wedge B' \subseteq B \wedge Z \subseteq Z'$ 
    by (rule ctyping2-mono-while)
qed fastforce+

```

```

lemma ctyping1-ctyping2-fst-assign [elim!]:
assumes
  A:  $(C, Z) = \vdash x ::= a (\subseteq A, X)$  and
  B:  $\text{Some } (C', Z') = (U, \text{False}) \models x ::= a (\subseteq A, X)$ 
shows  $C' \subseteq C$ 
proof -
{
  fix s
  assume  $s \in A$ 
  moreover assume  $\text{avars } a = \{\}$ 
  hence  $\text{aval } a \ s = \text{aval } a \ (\lambda x. 0)$ 
  by (blast intro: avars-aval)
  ultimately have  $\exists s'. (\exists t. s(x ::= \text{aval } a \ s) = (\lambda x'. \text{case case}$ 
    if  $x' = x$  then  $\text{Some } (\text{Some } (\text{aval } a \ (\lambda x. 0)))$  else  $\text{None of}$ 
     $\text{None} \Rightarrow \text{None} \mid \text{Some } v \Rightarrow \text{Some } v$  of

```

```

      None  $\Rightarrow$   $s' x' \mid$  Some None  $\Rightarrow$   $t x' \mid$  Some (Some  $i \Rightarrow i$ )  $\wedge s' \in A$ 
    by fastforce
  }
  note  $C = \text{this}$ 
  from  $A$  and  $B$  show ?thesis
    by (clarsimp simp: ctyping1-def ctyping1-seq-def split: if-split-asm,
        erule-tac  $C$ , simp, fastforce)
qed

```

lemma *ctyping1-ctyping2-fst-seq*:

assumes

$A: \bigwedge B B' Y Y'. (B, Y) = \vdash c_1 (\subseteq A, X) \Longrightarrow$
 Some $(B', Y') = (U, \text{False}) \models c_1 (\subseteq A, X) \Longrightarrow B' \subseteq B$ **and**
 $B: \bigwedge p B Y C C' Z Z'. (U, \text{False}) \models c_1 (\subseteq A, X) = \text{Some } p \Longrightarrow$
 $(B, Y) = p \Longrightarrow (C, Z) = \vdash c_2 (\subseteq B, Y) \Longrightarrow$
 Some $(C', Z') = (U, \text{False}) \models c_2 (\subseteq B, Y) \Longrightarrow C' \subseteq C$ **and**
 $C: (C, Z) = \vdash c_1;; c_2 (\subseteq A, X)$ **and**
 $D: \text{Some } (C', Z') = (U, \text{False}) \models c_1;; c_2 (\subseteq A, X)$

shows $C' \subseteq C$

proof –

```

let ?f = foldl (;;) ( $\lambda x. \text{None}$ )
let ?P =  $\lambda r A S. \exists f s. (\exists t. r = (\lambda x. \text{case } f x \text{ of}$ 
    None  $\Rightarrow s x \mid$  Some None  $\Rightarrow t x \mid$  Some (Some  $i \Rightarrow i$ ))  $\wedge$ 
    ( $\exists ys. f = ?f ys \wedge ys \in S$ )  $\wedge s \in A$ )
let ?F =  $\lambda A S. \{r. ?P r A S\}$ 
{
  fix  $s_3 B' Y'$ 
  assume
     $E: \bigwedge B'' B C C' Z'. B' = B'' \Longrightarrow B = B'' \Longrightarrow C = ?F B'' (\vdash c_2) \Longrightarrow$ 
    Some  $(C', Z') = (U, \text{False}) \models c_2 (\subseteq B'', Y') \Longrightarrow$ 
     $C' \subseteq ?F B'' (\vdash c_2)$  and
     $F: \bigwedge B B''. B = ?F A (\vdash c_1) \Longrightarrow B'' = B' \Longrightarrow B' \subseteq ?F A (\vdash c_1)$  and
     $G: \text{Some } (C', Z') = (U, \text{False}) \models c_2 (\subseteq B', Y')$  and
     $H: s_3 \in C'$ 
  have ?P  $s_3 A (\vdash c_1 \sqcup_{\text{@}} \vdash c_2)$ 

```

proof –

obtain s_2 **and** t_2 **and** ys_2 **where**

```

 $I: s_3 = (\lambda x. \text{case } ?f ys_2 x \text{ of}$ 
    None  $\Rightarrow s_2 x \mid$  Some None  $\Rightarrow t_2 x \mid$  Some (Some  $i \Rightarrow i$ )  $\wedge$ 
     $s_2 \in B' \wedge ys_2 \in \vdash c_2$ 

```

using E **and** G **and** H **by** fastforce

from this obtain s_1 **and** t_1 **and** ys_1 **where**

```

 $J: s_2 = (\lambda x. \text{case } ?f ys_1 x \text{ of}$ 
    None  $\Rightarrow s_1 x \mid$  Some None  $\Rightarrow t_1 x \mid$  Some (Some  $i \Rightarrow i$ )  $\wedge$ 
     $s_1 \in A \wedge ys_1 \in \vdash c_1$ 

```

using F **by** fastforce

let $?t = \lambda x. \text{case } ?f ys_2 x \text{ of}$

```

    None  $\Rightarrow \text{case } ?f ys_1 x \text{ of Some None } \Rightarrow t_1 x \mid - \Rightarrow 0 \mid$ 
    Some None  $\Rightarrow t_2 x \mid - \Rightarrow 0$ 

```



```

from  $I$  and  $J$  have  $s_3 = (\lambda x. \text{case } ?f \ (ys_1 \ @ \ ys_2) \ x \text{ of}$ 
   $\text{None} \Rightarrow s_1 \ x \mid \text{Some } \text{None} \Rightarrow ?t \ x \mid \text{Some } (\text{Some } i) \Rightarrow i)$ 
  by (fastforce dest: last-in-set simp: Let-def ctying1-seq-last
    split: option.split)
moreover have  $ys_1 \ @ \ ys_2 \in \vdash \ c_1 \sqcup_{@} \vdash \ c_2$ 
  by (simp add: ctying1-merge-append-in I J)
ultimately show  $?thesis$ 
  using  $J$  by fastforce
qed
}
note  $E = \text{this}$ 
from  $A$  and  $B$  and  $C$  and  $D$  show  $?thesis$ 
  by (auto simp: ctying1-def split: option.split-asm, erule-tac E)
qed

```

lemma *ctying1-ctying2-fst-if*:

assumes

$A: \bigwedge U' \ p \ B_1 \ B_2 \ C_1 \ C_1' \ Y_1 \ Y_1'.$
 $(U', p) = (\text{insert } (\text{Univ? } A \ X, \text{bvars } b) \ U, \models b \ (\subseteq A, X)) \Rightarrow$
 $(B_1, B_2) = p \Rightarrow (C_1, Y_1) = \vdash \ c_1 \ (\subseteq B_1, X) \Rightarrow$
 $\text{Some } (C_1', Y_1') = (U', \text{False}) \models c_1 \ (\subseteq B_1, X) \Rightarrow C_1' \subseteq C_1$ **and**
 $B: \bigwedge U' \ p \ B_1 \ B_2 \ C_2 \ C_2' \ Y_2 \ Y_2'.$
 $(U', p) = (\text{insert } (\text{Univ? } A \ X, \text{bvars } b) \ U, \models b \ (\subseteq A, X)) \Rightarrow$
 $(B_1, B_2) = p \Rightarrow (C_2, Y_2) = \vdash \ c_2 \ (\subseteq B_2, X) \Rightarrow$
 $\text{Some } (C_2', Y_2') = (U', \text{False}) \models c_2 \ (\subseteq B_2, X) \Rightarrow C_2' \subseteq C_2$ **and**
 $C: (C, Y) = \vdash \text{IF } b \text{ THEN } c_1 \text{ ELSE } c_2 \ (\subseteq A, X)$ **and**
 $D: \text{Some } (C', Y') = (U, \text{False}) \models \text{IF } b \text{ THEN } c_1 \text{ ELSE } c_2 \ (\subseteq A, X)$

shows $C' \subseteq C$

proof –

let $?f = \text{foldl } (,;) \ (\lambda x. \text{None})$
let $?P = \lambda r \ A \ S. \exists f \ s. (\exists t. r = (\lambda x. \text{case } f \ x \text{ of}$
 $\text{None} \Rightarrow s \ x \mid \text{Some } \text{None} \Rightarrow t \ x \mid \text{Some } (\text{Some } i) \Rightarrow i)) \wedge$
 $(\exists ys. f = ?f \ ys \wedge ys \in S) \wedge s \in A$
let $?F = \lambda A \ S. \{r. ?P \ r \ A \ S\}$
let $?S_1 = \lambda f. \text{if } f = \text{Some } \text{True} \vee f = \text{None} \text{ then } \vdash \ c_1 \text{ else } \{\}$
let $?S_2 = \lambda f. \text{if } f = \text{Some } \text{False} \vee f = \text{None} \text{ then } \vdash \ c_2 \text{ else } \{\}$
{
fix $s' \ B_1 \ B_2 \ C_1$
assume
 $E: \bigwedge U' \ B_1' \ C_1' \ C_1''. U' = \text{insert } (\text{Univ? } A \ X, \text{bvars } b) \ U \Rightarrow$
 $B_1' = B_1 \Rightarrow C_1' = ?F \ B_1 \ (\vdash \ c_1) \Rightarrow C_1'' = C_1 \Rightarrow$
 $C_1 \subseteq ?F \ B_1 \ (\vdash \ c_1)$ **and**
 $F: \models b \ (\subseteq A, X) = (B_1, B_2)$ **and**
 $G: s' \in C_1$

have $?P \ s' \ A \ (\text{let } f = \vdash \ b \text{ in } ?S_1 \ f \sqcup ?S_2 \ f)$

proof –

obtain s **and** t **and** ys **where**

$H: s' = (\lambda x. \text{case } ?f \ ys \ x \text{ of}$
 $\text{None} \Rightarrow s \ x \mid \text{Some } \text{None} \Rightarrow t \ x \mid \text{Some } (\text{Some } i) \Rightarrow i) \wedge$

```

      s ∈ B1 ∧ ys ∈ ⊢ c1
    using E and G by fastforce
  moreover from F and this have s ∈ A
    by (blast dest: btyping2-un-eq)
  moreover from F and H have ⊢ b ≠ Some False
    by (auto dest: btyping1-btyping2 [where A = A and X = X])
  hence ys ∈ (let f = ⊢ b in ?S1 f ∪ ?S2 f)
    using H by (auto simp: Let-def)
  hence ys ∈ (let f = ⊢ b in ?S1 f ⊔ ?S2 f)
    by (auto simp: Let-def intro: ctyping1-merge-in)
  ultimately show ?thesis
    by blast
qed
}
note E = this
{
  fix s' B1 B2 C2
  assume
    F: ∧ U' B2' C2' C2''. U' = insert (Univ? A X, bvars b) U ⇒
      B2' = B1 ⇒ C2' = ?F B2 (⊢ c2) ⇒ C2'' = C2 ⇒
      C2 ⊆ ?F B2 (⊢ c2) and
    G: ⊢ b (⊆ A, X) = (B1, B2) and
    H: s' ∈ C2
  have ?P s' A (let f = ⊢ b in ?S1 f ⊔ ?S2 f)
  proof -
    obtain s and t and ys where
      I: s' = (λx. case ?f ys x of
        None ⇒ s x | Some None ⇒ t x | Some (Some i) ⇒ i) ∧
      s ∈ B2 ∧ ys ∈ ⊢ c2
    using F and H by fastforce
  moreover from G and this have s ∈ A
    by (blast dest: btyping2-un-eq)
  moreover from G and I have ⊢ b ≠ Some True
    by (auto dest: btyping1-btyping2 [where A = A and X = X])
  hence ys ∈ (let f = ⊢ b in ?S1 f ∪ ?S2 f)
    using I by (auto simp: Let-def)
  hence ys ∈ (let f = ⊢ b in ?S1 f ⊔ ?S2 f)
    by (auto simp: Let-def intro: ctyping1-merge-in)
  ultimately show ?thesis
    by blast
qed
}
note F = this
from A and B and C and D show ?thesis
  by (auto simp: ctyping1-def split: option.split-asm prod.split-asm,
    erule-tac [2] F, erule-tac E)
qed

lemma ctyping1-ctyping2-fst-while:

```

assumes

$A: (C, Y) = \vdash \text{WHILE } b \text{ DO } c (\subseteq A, X) \text{ and}$

$B: \text{Some } (C', Y') = (U, \text{False}) \models \text{WHILE } b \text{ DO } c (\subseteq A, X)$

shows $C' \subseteq C$

proof –

let $?f = \text{foldl } (:) (\lambda x. \text{None})$

let $?P = \lambda r A S. \exists f s. (\exists t. r = (\lambda x. \text{case } f x \text{ of}$

$\text{None} \Rightarrow s x \mid \text{Some } \text{None} \Rightarrow t x \mid \text{Some } (\text{Some } i) \Rightarrow i)) \wedge$

$(\exists ys. f = ?f ys \wedge ys \in S) \wedge s \in A$

let $?F = \lambda A S. \{r. ?P r A S\}$

let $?S_1 = \lambda f. \text{if } f = \text{Some False} \vee f = \text{None} \text{ then } \{\} \text{ else } \{ \}$

let $?S_2 = \lambda f. \text{if } f = \text{Some True} \vee f = \text{None} \text{ then } \vdash c \text{ else } \{ \}$

{

fix $s' B_1 B_2 B_1' B_2'$

assume

$C: \models b (\subseteq A, X) = (B_1, B_2) \text{ and}$

$D: \models b (\subseteq ?F B_1 (\vdash c), \text{Univ}?? B_1 \{x. \forall f \in \{?f ys \mid ys. ys \in \vdash c\}.$

$f x \neq \text{Some None} \wedge (f x = \text{None} \longrightarrow x \in X)) = (B_1', B_2')$

$(\text{is} \models - (\subseteq ?C, ?Y) = -)$

assume $s' \in C'$ **and** $\text{Some } (C', Y') = (\text{if } (\forall s \in \text{Univ}?? A X \cup$

$\text{Univ}?? ?C ?Y. \forall x \in \text{bvars } b. \text{All } (\text{interf } s (\text{dom } x))) \wedge$

$(\forall p \in U. \forall B W. p = (B, W) \longrightarrow (\forall s \in B. \forall x \in W. \text{All } (\text{interf } s (\text{dom } x))))$

$\text{then } \text{Some } (B_2 \cup B_2', \text{Univ}?? B_2 X \cap ?Y)$

$\text{else None})$

hence $s' \in B_2 \cup B_2'$

by $(\text{simp split: if-split-asm})$

hence $?P s' A (\text{let } f = \vdash b \text{ in } ?S_1 f \cup ?S_2 f)$

proof

assume $E: s' \in B_2$

hence $s' \in A$

using C **by** $(\text{blast dest: btyping2-un-eq})$

moreover from C **and** E **have** $\vdash b \neq \text{Some True}$

by $(\text{auto dest: btyping1-btyping2 } [\text{where } A = A \text{ and } X = X])$

hence $\square \in (\text{let } f = \vdash b \text{ in } ?S_1 f \cup ?S_2 f)$

by $(\text{auto simp: Let-def})$

ultimately show $?thesis$

by force

next

assume $s' \in B_2'$

then obtain s **and** t **and** ys **where**

$E: s' = (\lambda x. \text{case } ?f ys x \text{ of}$

$\text{None} \Rightarrow s x \mid \text{Some } \text{None} \Rightarrow t x \mid \text{Some } (\text{Some } i) \Rightarrow i) \wedge$

$s \in B_1 \wedge ys \in \vdash c$

using D **by** $(\text{blast dest: btyping2-un-eq})$

moreover from C **and this have** $s \in A$

by $(\text{blast dest: btyping2-un-eq})$

moreover from C **and** E **have** $\vdash b \neq \text{Some False}$

by $(\text{auto dest: btyping1-btyping2 } [\text{where } A = A \text{ and } X = X])$

hence $ys \in (\text{let } f = \vdash b \text{ in } ?S_1 f \cup ?S_2 f)$

```

    using E by (auto simp: Let-def)
    ultimately show ?thesis
    by blast
qed
}
note C = this
from A and B show ?thesis
by (auto intro: C simp: ctyping1-def
    split: option.split-asm prod.split-asm)
qed

lemma ctyping1-ctyping2-fst:
  
$$\llbracket (C, Z) = \vdash c \ (\subseteq A, X); \text{Some } (C', Z') = (U, \text{False}) \models c \ (\subseteq A, X) \rrbracket \implies C' \subseteq C$$

proof (induction (U, False) c A X arbitrary: C C' Z Z' U
  rule: ctyping2.induct)
  fix A X C C' Z Z' U c1 c2
  show
    
$$\llbracket \bigwedge C C' Z Z'. (C, Z) = \vdash c_1 \ (\subseteq A, X) \implies \text{Some } (C', Z') = (U, \text{False}) \models c_1 \ (\subseteq A, X) \implies C' \subseteq C; \\ \bigwedge p B Y C C' Z Z'. (U, \text{False}) \models c_1 \ (\subseteq A, X) = \text{Some } p \implies (B, Y) = p \implies (C, Z) = \vdash c_2 \ (\subseteq B, Y) \implies \text{Some } (C', Z') = (U, \text{False}) \models c_2 \ (\subseteq B, Y) \implies C' \subseteq C; \\ (C, Z) = \vdash c_1;; c_2 \ (\subseteq A, X); \text{Some } (C', Z') = (U, \text{False}) \models c_1;; c_2 \ (\subseteq A, X) \rrbracket \implies C' \subseteq C$$

    by (rule ctyping1-ctyping2-fst-seq)
next
  fix A X C C' Z Z' U b c1 c2
  show
    
$$\llbracket \bigwedge U' p B_1 B_2 C C' Z Z'. (U', p) = (\text{insert } (\text{Univ? } A X, \text{bvars } b) U, \models b \ (\subseteq A, X)) \implies (B_1, B_2) = p \implies (C, Z) = \vdash c_1 \ (\subseteq B_1, X) \implies \text{Some } (C', Z') = (U', \text{False}) \models c_1 \ (\subseteq B_1, X) \implies C' \subseteq C; \\ \bigwedge U' p B_1 B_2 C C' Z Z'. (U', p) = (\text{insert } (\text{Univ? } A X, \text{bvars } b) U, \models b \ (\subseteq A, X)) \implies (B_1, B_2) = p \implies (C, Z) = \vdash c_2 \ (\subseteq B_2, X) \implies \text{Some } (C', Z') = (U', \text{False}) \models c_2 \ (\subseteq B_2, X) \implies C' \subseteq C; \\ (C, Z) = \vdash \text{IF } b \text{ THEN } c_1 \text{ ELSE } c_2 \ (\subseteq A, X); \text{Some } (C', Z') = (U, \text{False}) \models \text{IF } b \text{ THEN } c_1 \text{ ELSE } c_2 \ (\subseteq A, X) \rrbracket \implies C' \subseteq C$$

    by (rule ctyping1-ctyping2-fst-if)
next
  fix A X B B' Z Z' U b c

```

show

$$\llbracket \bigwedge B_1 B_2 C Y B_1' B_2' B B' Z Z'. \quad \begin{aligned} & (B_1, B_2) = \models b (\subseteq A, X) \implies \\ & (C, Y) = \vdash c (\subseteq B_1, X) \implies \\ & (B_1', B_2') = \models b (\subseteq C, Y) \implies \\ & \forall (B, W) \in \text{insert } (\text{Univ? } A X \cup \text{Univ? } C Y, \text{bvars } b) U. \\ & \quad B: \text{dom } ' W \rightsquigarrow \text{UNIV} \implies \\ & (B, Z) = \vdash c (\subseteq B_1, X) \implies \\ & \text{Some } (B', Z') = (\{\}, \text{False}) \models c (\subseteq B_1, X) \implies \\ & \quad B' \subseteq B; \\ & \bigwedge B_1 B_2 C Y B_1' B_2' B B' Z Z'. \\ & (B_1, B_2) = \models b (\subseteq A, X) \implies \\ & (C, Y) = \vdash c (\subseteq B_1, X) \implies \\ & (B_1', B_2') = \models b (\subseteq C, Y) \implies \\ & \forall (B, W) \in \text{insert } (\text{Univ? } A X \cup \text{Univ? } C Y, \text{bvars } b) U. \\ & \quad B: \text{dom } ' W \rightsquigarrow \text{UNIV} \implies \\ & (B, Z) = \vdash c (\subseteq B_1', Y) \implies \\ & \text{Some } (B', Z') = (\{\}, \text{False}) \models c (\subseteq B_1', Y) \implies \\ & \quad B' \subseteq B; \\ & (B, Z) = \vdash \text{WHILE } b \text{ DO } c (\subseteq A, X); \\ & \text{Some } (B', Z') = (U, \text{False}) \models \text{WHILE } b \text{ DO } c (\subseteq A, X) \rrbracket \implies \\ & \quad B' \subseteq B \end{aligned}$$

by (*rule ctying1-ctying2-fst-while*)
qed (*simp add: ctying1-def, auto*)

lemma *ctying1-ctying2-snd-assign* [*elim!*]:

$$\llbracket (C, Z) = \vdash x ::= a (\subseteq A, X); \quad \text{Some } (C', Z') = (U, \text{False}) \models x ::= a (\subseteq A, X) \rrbracket \implies Z \subseteq Z'$$

by (*auto simp: ctying1-def ctying1-seq-def split: if-split-asm*)

lemma *ctying1-ctying2-snd-seq*:
assumes

$$\begin{aligned} & A: \bigwedge B B' Y Y'. (B, Y) = \vdash c_1 (\subseteq A, X) \implies \\ & \quad \text{Some } (B', Y') = (U, \text{False}) \models c_1 (\subseteq A, X) \implies Y \subseteq Y' \text{ and} \\ & B: \bigwedge p B Y C C' Z Z'. (U, \text{False}) \models c_1 (\subseteq A, X) = \text{Some } p \implies \\ & \quad (B, Y) = p \implies (C, Z) = \vdash c_2 (\subseteq B, Y) \implies \\ & \quad \text{Some } (C', Z') = (U, \text{False}) \models c_2 (\subseteq B, Y) \implies Z \subseteq Z' \text{ and} \\ & C: (C, Z) = \vdash c_1;; c_2 (\subseteq A, X) \text{ and} \\ & D: \text{Some } (C', Z') = (U, \text{False}) \models c_1;; c_2 (\subseteq A, X) \end{aligned}$$

shows $Z \subseteq Z'$
proof –
let $?f = \text{foldl } (,;) (\lambda x. \text{None})$
let $?F = \lambda A S. \{r. \exists f s. (\exists t. r = (\lambda x. \text{case } f x \text{ of } \text{None} \Rightarrow s x \mid \text{Some } \text{None} \Rightarrow t x \mid \text{Some } (\text{Some } i) \Rightarrow i)) \wedge$

$$(\exists ys. f = ?f ys \wedge ys \in S) \wedge s \in A\}$$

let $?G = \lambda X S. \{x. \forall f \in \{?f ys \mid ys. ys \in S\}.$

$$f x \neq \text{Some } \text{None} \wedge (f x = \text{None} \longrightarrow x \in X)\}$$

$$\{$$

```

fix  $x \ B \ Y$ 
assume  $\bigwedge B' \ B'' \ C \ C' \ Z'. \ B = B' \implies B'' = B' \implies C = ?F \ B' \ (\vdash \ c_2) \implies$ 
   $\text{Some } (C', Z') = (U, \text{False}) \models c_2 \ (\subseteq B', Y) \implies$ 
   $\text{Univ}?? \ B' \ (?G \ Y \ (\vdash \ c_2)) \subseteq Z' \text{ and}$ 
   $\text{Some } (C', Z') = (U, \text{False}) \models c_2 \ (\subseteq B, Y)$ 
hence  $E: \text{Univ}?? \ B \ (?G \ Y \ (\vdash \ c_2)) \subseteq Z'$ 
  by simp
assume  $\bigwedge C \ B'. \ C = ?F \ A \ (\vdash \ c_1) \implies B' = B \implies$ 
   $\text{Univ}?? \ A \ (?G \ X \ (\vdash \ c_1)) \subseteq Y$ 
hence  $F: \text{Univ}?? \ A \ (?G \ X \ (\vdash \ c_1)) \subseteq Y$ 
  by simp
assume  $G: \forall f. (\exists zs. f = ?f \ zs \wedge zs \in \vdash \ c_1 \sqcup_{@} \vdash \ c_2) \longrightarrow$ 
   $f \ x \neq \text{Some } \text{None} \wedge (f \ x = \text{None} \longrightarrow x \in X)$ 
{
  fix  $ys$ 
  have  $\vdash \ c_1 \neq \{\}$ 
    by (rule ctying1-aux-nonempty)
  then obtain  $xs$  where  $xs \in \vdash \ c_1$ 
    by blast
  moreover assume  $ys \in \vdash \ c_2$ 
  ultimately have  $xs \ @ \ ys \in \vdash \ c_1 \sqcup_{@} \vdash \ c_2$ 
    by (rule ctying1-merge-append-in)
  moreover assume  $?f \ ys \ x = \text{Some } \text{None}$ 
  hence  $?f \ (xs \ @ \ ys) \ x = \text{Some } \text{None}$ 
    by (simp add: Let-def ctying1-seq-last split: if-split-asm)
  ultimately have False
    using  $G$  by blast
}
hence  $H: \forall ys \in \vdash \ c_2. ?f \ ys \ x \neq \text{Some } \text{None}$ 
  by blast
{
  fix  $xs \ ys$ 
  assume  $xs \in \vdash \ c_1$  and  $ys \in \vdash \ c_2$ 
  hence  $xs \ @ \ ys \in \vdash \ c_1 \sqcup_{@} \vdash \ c_2$ 
    by (rule ctying1-merge-append-in)
  moreover assume  $?f \ xs \ x = \text{Some } \text{None}$  and  $?f \ ys \ x = \text{None}$ 
  hence  $?f \ (xs \ @ \ ys) \ x = \text{Some } \text{None}$ 
    by (auto dest: last-in-set simp: Let-def ctying1-seq-last split: if-split-asm)
  ultimately have  $(\exists ys \in \vdash \ c_2. ?f \ ys \ x = \text{None}) \longrightarrow$ 
     $(\forall xs \in \vdash \ c_1. ?f \ xs \ x \neq \text{Some } \text{None})$ 
    using  $G$  by blast
}
hence  $I: (\exists ys \in \vdash \ c_2. ?f \ ys \ x = \text{None}) \longrightarrow$ 
   $(\forall xs \in \vdash \ c_1. ?f \ xs \ x \neq \text{Some } \text{None})$ 
  by blast
{
  fix  $xs \ ys$ 
  assume  $xs \in \vdash \ c_1$  and  $J: ys \in \vdash \ c_2$ 

```

```

hence  $xs @ ys \in \vdash c_1 \sqcup @ \vdash c_2$ 
  by (rule ctying1-merge-append-in)
moreover assume  $?f xs x = None$  and  $K: ?f ys x = None$ 
hence  $?f (xs @ ys) x = None$ 
  by (simp add: Let-def ctying1-seq-last split: if-split-asm)
ultimately have  $x \in X$ 
  using  $G$  by blast
moreover have  $\forall xs \in \vdash c_1. ?f xs x \neq Some None$ 
  using  $I$  and  $J$  and  $K$  by blast
ultimately have  $x \in Z'$ 
  using  $E$  and  $F$  and  $H$  by fastforce
}
moreover {
  fix  $ys$ 
  assume  $ys \in \vdash c_2$  and  $?f ys x = None$ 
  hence  $\forall xs \in \vdash c_1. ?f xs x \neq Some None$ 
    using  $I$  by blast
  moreover assume  $\forall xs \in \vdash c_1. \exists v. ?f xs x = Some v$ 
  ultimately have  $x \in Z'$ 
    using  $E$  and  $F$  and  $H$  by fastforce
}
moreover {
  assume  $\forall ys \in \vdash c_2. \exists v. ?f ys x = Some v$ 
  hence  $x \in Z'$ 
    using  $E$  and  $H$  by fastforce
}
ultimately have  $x \in Z'$ 
  by (cases  $\exists ys \in \vdash c_2. ?f ys x = None,$ 
    cases  $\exists xs \in \vdash c_1. ?f xs x = None, auto)
moreover assume  $x \notin Z'$ 
ultimately have False
  by contradiction
}
note  $E = this$ 
from  $A$  and  $B$  and  $C$  and  $D$  show ?thesis
  by (auto dest: ctying2-fst-empty ctying2-fst-empty [OF sym]
    simp: ctying1-def split: option.split-asm, erule-tac E)
qed$ 
```

lemma *ctying1-ctying2-snd-if:*

assumes

```

 $A: \bigwedge U' p B_1 B_2 C_1 C_1' Y_1 Y_1'.$ 
   $(U', p) = (insert (Univ? A X, bvars b) U, \models b (\subseteq A, X)) \implies$ 
   $(B_1, B_2) = p \implies (C_1, Y_1) = \vdash c_1 (\subseteq B_1, X) \implies$ 
   $Some (C_1', Y_1') = (U', False) \models c_1 (\subseteq B_1, X) \implies Y_1 \subseteq Y_1' \text{ and}$ 
 $B: \bigwedge U' p B_1 B_2 C_2 C_2' Y_2 Y_2'.$ 
   $(U', p) = (insert (Univ? A X, bvars b) U, \models b (\subseteq A, X)) \implies$ 
   $(B_1, B_2) = p \implies (C_2, Y_2) = \vdash c_2 (\subseteq B_2, X) \implies$ 
   $Some (C_2', Y_2') = (U', False) \models c_2 (\subseteq B_2, X) \implies Y_2 \subseteq Y_2' \text{ and}$ 

```

$C: (C, Y) = \vdash \text{IF } b \text{ THEN } c_1 \text{ ELSE } c_2 (\subseteq A, X) \text{ and}$
 $D: \text{Some } (C', Y') = (U, \text{False}) \models \text{IF } b \text{ THEN } c_1 \text{ ELSE } c_2 (\subseteq A, X)$
shows $Y \subseteq Y'$
proof –
let $?f = \text{foldl } (;\;) (\lambda x. \text{None})$
let $?F = \lambda A \ S. \{r. \exists f \ s. (\exists t. r = (\lambda x. \text{case } f \ x \text{ of}$
 $\text{None} \Rightarrow s \ x \mid \text{Some } \text{None} \Rightarrow t \ x \mid \text{Some } (\text{Some } i) \Rightarrow i)) \wedge$
 $(\exists ys. f = ?f \ ys \wedge ys \in S) \wedge s \in A\}$
let $?G = \lambda X \ S. \{x. \forall f \in \{?f \ ys \mid ys. ys \in S\}.$
 $f \ x \neq \text{Some } \text{None} \wedge (f \ x = \text{None} \longrightarrow x \in X)\}$
let $?S_1 = \lambda f. \text{if } f = \text{Some } \text{True} \vee f = \text{None} \text{ then } \vdash c_1 \text{ else } \{\}$
let $?S_2 = \lambda f. \text{if } f = \text{Some } \text{False} \vee f = \text{None} \text{ then } \vdash c_2 \text{ else } \{\}$
let $?P = \lambda x. \forall f. (\exists ys. f = ?f \ ys \wedge ys \in (\text{let } f = \vdash b \text{ in } ?S_1 \ f \sqcup ?S_2 \ f)) \longrightarrow$
 $f \ x \neq \text{Some } \text{None} \wedge (f \ x = \text{None} \longrightarrow x \in X)$
let $?U = \text{insert } (\text{Univ? } A \ X, \text{bvars } b) \ U$
{
fix $B_1 \ B_2 \ Y_1' \ Y_2' \text{ and } C_1' :: \text{state set and } C_2' :: \text{state set}$
assume $\bigwedge U' \ B_1' \ C_1 \ C_1''. U' = ?U \Longrightarrow B_1' = B_1 \Longrightarrow$
 $C_1 = ?F \ B_1 (\vdash c_1) \Longrightarrow C_1'' = C_1' \Longrightarrow \text{Univ?? } B_1 (?G \ X (\vdash c_1)) \subseteq Y_1'$
hence $E: \text{Univ?? } B_1 (?G \ X (\vdash c_1)) \subseteq Y_1'$
by simp
moreover assume $\bigwedge U' \ B_1' \ C_2 \ C_2''. U' = ?U \Longrightarrow B_1' = B_1 \Longrightarrow$
 $C_2 = ?F \ B_2 (\vdash c_2) \Longrightarrow C_2'' = C_2' \Longrightarrow \text{Univ?? } B_2 (?G \ X (\vdash c_2)) \subseteq Y_2'$
hence $F: \text{Univ?? } B_2 (?G \ X (\vdash c_2)) \subseteq Y_2'$
by simp
moreover assume $G: \models b (\subseteq A, X) = (B_1, B_2)$
moreover {
fix x
assume $?P \ x$
have $x \in Y_1'$
proof $(\text{cases } \vdash b = \text{Some } \text{False})$
case True
with E **and** G **show** $?thesis$
by $(\text{drule-tac btyping1-btyping2 [where } A = A \text{ and } X = X], \text{auto})$
next
case False
{
fix xs
assume $xs \in \vdash c_1$
with False **have** $xs \in (\text{let } f = \vdash b \text{ in } ?S_1 \ f \sqcup ?S_2 \ f)$
by $(\text{auto intro: ctyping1-merge-in simp: Let-def})$
hence $?f \ xs \ x \neq \text{Some } \text{None} \wedge (?f \ xs \ x = \text{None} \longrightarrow x \in X)$
using $\langle ?P \ x \rangle$ **by auto**
}
hence $x \in \text{Univ?? } B_1 (?G \ X (\vdash c_1))$
by auto
thus $?thesis$
using $E \ ..$
qed


```

}
moreover {
  fix x
  assume ?P x
  have x ∈ Y2'
  proof (cases ⊢ b = Some True)
    case True
    with F and G show ?thesis
      by (drule-tac btyping1-btyping2 [where A = A and X = X], auto)
  next
    case False
    {
      fix ys
      assume ys ∈ ⊢ c2
      with False have ys ∈ (let f = ⊢ b in ?S1 f ⊔ ?S2 f)
        by (auto intro: ctyping1-merge-in simp: Let-def)
      hence ?f ys x ≠ Some None ∧ (?f ys x = None ⟶ x ∈ X)
        using ⟨?P x⟩ by auto
    }
    hence x ∈ Univ?? B2 (?G X (⊢ c2))
      by auto
    thus ?thesis
      using F ..
  qed
}
ultimately have (A = {} ⟶ UNIV ⊆ Y1' ∧ UNIV ⊆ Y2') ∧
  (A ≠ {} ⟶ {x. ?P x} ⊆ Y1' ∧ {x. ?P x} ⊆ Y2')
  by (auto simp: btyping2-fst-empty)
}
note E = this
from A and B and C and D show ?thesis
  by (clarsimp simp: ctyping1-def split: option.split-asm prod.split-asm,
      erule-tac E)
qed

lemma ctyping1-ctyping2-snd-while:
  assumes
    A: (C, Y) = ⊢ WHILE b DO c (⊆ A, X) and
    B: Some (C', Y') = (U, False) ⊢ WHILE b DO c (⊆ A, X)
  shows Y ⊆ Y'
proof -
  let ?f = foldl (·;) (λx. None)
  let ?F = λA S. {r. ∃ f s. (∃ t. r = (λx. case f x of
    None ⇒ s x | Some None ⇒ t x | Some (Some i) ⇒ i)) ∧
    (∃ ys. f = ?f ys ∧ ys ∈ S) ∧ s ∈ A}
  let ?S1 = λf. if f = Some False ∨ f = None then {} else {}
  let ?S2 = λf. if f = Some True ∨ f = None then ⊢ c else {}
  let ?P = λx. ∀ f. (∃ ys. f = ?f ys ∧ ys ∈ (let f = ⊢ b in ?S1 f ⊔ ?S2 f)) ⟶
    f x ≠ Some None ∧ (f x = None ⟶ x ∈ X)

```

```

let ?Y = λA. Univ?? A {x. ∀f ∈ {?f ys | ys. ys ∈ ⊢ c}.
  f x ≠ Some None ∧ (f x = None ⟶ x ∈ X)}
{
  fix B1 B2 B1' B2'
  assume C: ⊢ b (⊆ A, X) = (B1, B2)
  assume Some (C', Y') = (if (∀s ∈ Univ? A X ∪
    Univ? (?F B1 (⊢ c)) (?Y B1). ∀x ∈ bvars b. All (interf s (dom x))) ∧
    (∀p ∈ U. ∀B W. p = (B, W) ⟶ (∀s ∈ B. ∀x ∈ W. All (interf s (dom x))))
    then Some (B2 ∪ B2', Univ?? B2 X ∩ ?Y B1)
    else None)
  hence D: Y' = Univ?? B2 X ∩ ?Y B1
  by (simp split: if-split-asm)
  {
    fix x
    assume A = {}
    hence x ∈ Y'
    using C and D by (simp add: btyping2-fst-empty)
  }
  moreover {
    fix x
    assume ?P x
    {
      assume ⊢ b ≠ Some True
      hence [] ∈ (let f = ⊢ b in ?S1 f ∪ ?S2 f)
      by (auto simp: Let-def)
      hence x ∈ X
      using ⟨?P x⟩ by auto
    }
    hence E: ⊢ b ≠ Some True ⟶ x ∈ Univ?? B2 X
    by auto
    {
      fix ys
      assume ⊢ b ≠ Some False and ys ∈ ⊢ c
      hence ys ∈ (let f = ⊢ b in ?S1 f ∪ ?S2 f)
      by (auto simp: Let-def)
      hence ?f ys x ≠ Some None ∧ (?f ys x = None ⟶ x ∈ X)
      using ⟨?P x⟩ by auto
    }
    hence F: ⊢ b ≠ Some False ⟶ x ∈ ?Y B1
    by auto
    have x ∈ Y'
    proof (cases ⊢ b)
    case None
    thus ?thesis
    using D and E and F by simp
  next
    case (Some v)
    show ?thesis
    proof (cases v)

```

```

    case True
    with C and D and F and Some show ?thesis
    by (drule-tac btyping1-btyping2 [where A = A and X = X], simp)
  next
  case False
  with C and D and E and Some show ?thesis
  by (drule-tac btyping1-btyping2 [where A = A and X = X], simp)
qed
qed
}
ultimately have (A = {}  $\longrightarrow$  UNIV  $\subseteq$  Y')  $\wedge$  (A  $\neq$  {}  $\longrightarrow$  {x. ?P x}  $\subseteq$  Y')
by auto
}
note C = this
from A and B show ?thesis
by (auto intro!: C simp: ctyping1-def
    split: option.split-asm prod.split-asm)
qed

lemma ctyping1-ctyping2-snd:
 $\llbracket (C, Z) = \vdash c (\subseteq A, X); \text{Some } (C', Z') = (U, \text{False}) \models c (\subseteq A, X) \rrbracket \Longrightarrow$ 
 $Z \subseteq Z'$ 
proof (induction (U, False) c A X arbitrary: C C' Z Z' U
  rule: ctyping2.induct)
  fix A X C C' Z Z' U c1 c2
  show
 $\llbracket \bigwedge B B' Y Y'. (B, Y) = \vdash c_1 (\subseteq A, X) \Longrightarrow$ 
 $\text{Some } (B', Y') = (U, \text{False}) \models c_1 (\subseteq A, X) \Longrightarrow$ 
 $Y \subseteq Y';$ 
 $\bigwedge p B Y C C' Z Z'. (U, \text{False}) \models c_1 (\subseteq A, X) = \text{Some } p \Longrightarrow$ 
 $(B, Y) = p \Longrightarrow (C, Z) = \vdash c_2 (\subseteq B, Y) \Longrightarrow$ 
 $\text{Some } (C', Z') = (U, \text{False}) \models c_2 (\subseteq B, Y) \Longrightarrow$ 
 $Z \subseteq Z';$ 
 $(C, Z) = \vdash c_1;; c_2 (\subseteq A, X);$ 
 $\text{Some } (C', Z') = (U, \text{False}) \models c_1;; c_2 (\subseteq A, X) \rrbracket \Longrightarrow$ 
 $Z \subseteq Z'$ 
  by (rule ctyping1-ctyping2-snd-seq)
next
  fix A X C C' Z Z' U b c1 c2
  show
 $\llbracket \bigwedge U' p B_1 B_2 C C' Z Z'. (U', p) = (\text{insert } (\text{Univ? } A X, \text{bvars } b) U, \models b (\subseteq A, X)) \Longrightarrow$ 
 $(B_1, B_2) = p \Longrightarrow (C, Z) = \vdash c_1 (\subseteq B_1, X) \Longrightarrow$ 
 $\text{Some } (C', Z') = (U', \text{False}) \models c_1 (\subseteq B_1, X) \Longrightarrow$ 
 $Z \subseteq Z';$ 
 $\bigwedge U' p B_1 B_2 C C' Z Z'. (U', p) = (\text{insert } (\text{Univ? } A X, \text{bvars } b) U, \models b (\subseteq A, X)) \Longrightarrow$ 
 $(B_1, B_2) = p \Longrightarrow (C, Z) = \vdash c_2 (\subseteq B_2, X) \Longrightarrow$ 

```

$Some (C', Z') = (U', False) \models c_2 (\subseteq B_2, X) \implies$
 $Z \subseteq Z';$
 $(C, Z) = \vdash IF\ b\ THEN\ c_1\ ELSE\ c_2 (\subseteq A, X);$
 $Some (C', Z') = (U, False) \models IF\ b\ THEN\ c_1\ ELSE\ c_2 (\subseteq A, X) \implies$
 $Z \subseteq Z'$
by (rule *ctyping1-ctyping2-snd-if*)
next
fix $A\ X\ B\ B'\ Z\ Z'\ U\ b\ c$
show
 $\llbracket \bigwedge B_1\ B_2\ C\ Y\ B_1'\ B_2'\ B\ B'\ Z\ Z'.$
 $(B_1, B_2) = \models b (\subseteq A, X) \implies$
 $(C, Y) = \vdash c (\subseteq B_1, X) \implies$
 $(B_1', B_2') = \models b (\subseteq C, Y) \implies$
 $\forall (B, W) \in insert\ (Univ?\ A\ X \cup Univ?\ C\ Y, bvars\ b)\ U.$
 $B: dom\ 'W \rightsquigarrow UNIV \implies$
 $(B, Z) = \vdash c (\subseteq B_1, X) \implies$
 $Some (B', Z') = (\{\}, False) \models c (\subseteq B_1, X) \implies$
 $Z \subseteq Z';$
 $\bigwedge B_1\ B_2\ C\ Y\ B_1'\ B_2'\ B\ B'\ Z\ Z'.$
 $(B_1, B_2) = \models b (\subseteq A, X) \implies$
 $(C, Y) = \vdash c (\subseteq B_1, X) \implies$
 $(B_1', B_2') = \models b (\subseteq C, Y) \implies$
 $\forall (B, W) \in insert\ (Univ?\ A\ X \cup Univ?\ C\ Y, bvars\ b)\ U.$
 $B: dom\ 'W \rightsquigarrow UNIV \implies$
 $(B, Z) = \vdash c (\subseteq B_1', Y) \implies$
 $Some (B', Z') = (\{\}, False) \models c (\subseteq B_1', Y) \implies$
 $Z \subseteq Z';$
 $(B, Z) = \vdash WHILE\ b\ DO\ c (\subseteq A, X);$
 $Some (B', Z') = (U, False) \models WHILE\ b\ DO\ c (\subseteq A, X) \implies$
 $Z \subseteq Z'$
by (rule *ctyping1-ctyping2-snd-while*)
qed (simp add: *ctyping1-def*, auto)

lemma *ctyping1-ctyping2*:
 $\llbracket \vdash c (\subseteq A, X) = (C, Z); (U, False) \models c (\subseteq A, X) = Some (C', Z') \rrbracket \implies$
 $C' \subseteq C \wedge Z \subseteq Z'$
by (rule *conjI*, ((rule *ctyping1-ctyping2-fst* [OF *sym sym*] |
rule ctyping1-ctyping2-snd [OF *sym sym*]), *assumption+*)+)

lemma *btyping2-aux-approx-1* [elim]:
assumes
 $A: \models b_1 (\subseteq A, X) = Some\ B_1$ **and**
 $B: \models b_2 (\subseteq A, X) = Some\ B_2$ **and**
 $C: bval\ b_1\ s$ **and**
 $D: bval\ b_2\ s$ **and**
 $E: r \in A$ **and**
 $F: s = r (\subseteq state \cap X)$

shows $\exists r' \in B_1 \cap B_2. r = r' (\subseteq \text{state} \cap X)$
proof –
 from *A and C and E and F have* $r \in B_1$
 by (*frule-tac btyping2-aux-subset, drule-tac btyping2-aux-eq, auto*)
 moreover from *B and D and E and F have* $r \in B_2$
 by (*frule-tac btyping2-aux-subset, drule-tac btyping2-aux-eq, auto*)
 ultimately show *?thesis*
 by *blast*
qed

lemma *btyping2-aux-approx-2* [*elim*]:

assumes
A: avars $a_1 \subseteq \text{state}$ **and**
B: avars $a_2 \subseteq \text{state}$ **and**
C: avars $a_1 \subseteq X$ **and**
D: avars $a_2 \subseteq X$ **and**
E: aval $a_1 s < \text{aval } a_2 s$ **and**
F: r $\in A$ **and**
G: s $= r (\subseteq \text{state} \cap X)$
shows $\exists r'. r' \in A \wedge \text{aval } a_1 r' < \text{aval } a_2 r' \wedge r = r' (\subseteq \text{state} \cap X)$
proof –
 have $\text{aval } a_1 s = \text{aval } a_1 r \wedge \text{aval } a_2 s = \text{aval } a_2 r$
 using *A and B and C and D and G* by (*blast intro: avars-aval*)
 thus *?thesis*
 using *E and F* by *auto*
qed

lemma *btyping2-aux-approx-3* [*elim*]:

assumes
A: avars $a_1 \subseteq \text{state}$ **and**
B: avars $a_2 \subseteq \text{state}$ **and**
C: avars $a_1 \subseteq X$ **and**
D: avars $a_2 \subseteq X$ **and**
E: $\neg \text{aval } a_1 s < \text{aval } a_2 s$ **and**
F: r $\in A$ **and**
G: s $= r (\subseteq \text{state} \cap X)$
shows $\exists r' \in A - \{s \in A. \text{aval } a_1 s < \text{aval } a_2 s\}. r = r' (\subseteq \text{state} \cap X)$
proof –
 have $\text{aval } a_1 s = \text{aval } a_1 r \wedge \text{aval } a_2 s = \text{aval } a_2 r$
 using *A and B and C and D and G* by (*blast intro: avars-aval*)
 thus *?thesis*
 using *E and F* by *auto*
qed

lemma *btyping2-aux-approx*:

$\llbracket b (\subseteq A, X) = \text{Some } A'; s \in \text{Univ } A (\subseteq \text{state} \cap X) \rrbracket \implies$
 $s \in \text{Univ } (\text{if } \text{bval } b \text{ then } A' \text{ else } A - A') (\subseteq \text{state} \cap X)$
by (*induction b arbitrary: A', auto dest: btyping2-aux-subset*
split: if-split-asm option.split-asm)

lemma *btyping2-approx*:

$\llbracket \models b (\subseteq A, X) = (B_1, B_2); s \in \text{Univ } A (\subseteq \text{state} \cap X) \rrbracket \implies$
 $s \in \text{Univ} \text{ (if } \text{bval } b \text{ s then } B_1 \text{ else } B_2) (\subseteq \text{state} \cap X)$
by (*drule sym, simp add: btyping2-def split: option.split-asm,*
drule btyping2-aux-approx, auto)

lemma *ctyping2-approx-assign* [*elim!*]:

$\llbracket \forall t'. \text{aval } a \text{ s} = t' x \longrightarrow (\forall s. t' = s(x := \text{aval } a \text{ s}) \longrightarrow s \notin A) \vee$
 $(\exists y \in \text{state} \cap X. y \neq x \wedge t y \neq t' y);$
 $v \models a (\subseteq X); t \in A; s = t (\subseteq \text{state} \cap X) \rrbracket \implies \text{False}$
by (*drule spec [of - t(x := aval a t)], cases a,*
(fastforce simp del: aval.simps(3) intro: avars-aval)+)

lemma *ctyping2-approx-if-1*:

$\llbracket \text{bval } b \text{ s}; \models b (\subseteq A, X) = (B_1, B_2); r \in A; s = r (\subseteq \text{state} \cap X);$
 $(\text{insert } (\text{Univ? } A \text{ X, bvars } b) \text{ U, v}) \models c_1 (\subseteq B_1, X) = \text{Some } (C_1, Y_1);$
 $\bigwedge A B X Y U v. (U, v) \models c_1 (\subseteq A, X) = \text{Some } (B, Y) \implies$
 $\exists r \in A. s = r (\subseteq \text{state} \cap X) \implies \exists r' \in B. t = r' (\subseteq \text{state} \cap Y) \rrbracket \implies$
 $\exists r' \in C_1 \cup C_2. t = r' (\subseteq \text{state} \cap (Y_1 \cap Y_2))$
by (*drule btyping2-approx, blast, fastforce*)

lemma *ctyping2-approx-if-2*:

$\llbracket \neg \text{bval } b \text{ s}; \models b (\subseteq A, X) = (B_1, B_2); r \in A; s = r (\subseteq \text{state} \cap X);$
 $(\text{insert } (\text{Univ? } A \text{ X, bvars } b) \text{ U, v}) \models c_2 (\subseteq B_2, X) = \text{Some } (C_2, Y_2);$
 $\bigwedge A B X Y U v. (U, v) \models c_2 (\subseteq A, X) = \text{Some } (B, Y) \implies$
 $\exists r \in A. s = r (\subseteq \text{state} \cap X) \implies \exists r' \in B. t = r' (\subseteq \text{state} \cap Y) \rrbracket \implies$
 $\exists r' \in C_1 \cup C_2. t = r' (\subseteq \text{state} \cap (Y_1 \cap Y_2))$
by (*drule btyping2-approx, blast, fastforce*)

lemma *ctyping2-approx-while-1* [*elim*]:

$\llbracket \neg \text{bval } b \text{ s}; r \in A; s = r (\subseteq \text{state} \cap X); \models b (\subseteq A, X) = (B, \{\}) \rrbracket \implies$
 $\exists t \in C. s = t (\subseteq \text{state} \cap Y)$
by (*drule btyping2-approx, blast, simp*)

lemma *ctyping2-approx-while-2* [*elim*]:

$\llbracket \forall t \in B_2 \cup B_2'. \exists x \in \text{state} \cap (X \cap Y). r x \neq t x; \neg \text{bval } b \text{ s};$
 $r \in A; s = r (\subseteq \text{state} \cap X); \models b (\subseteq A, X) = (B_1, B_2) \rrbracket \implies \text{False}$
by (*drule btyping2-approx, blast, auto*)

lemma *ctyping2-approx-while-aux*:

assumes

$A: \models b (\subseteq A, X) = (B_1, B_2) \text{ and}$
 $B: \vdash c (\subseteq B_1, X) = (C, Y) \text{ and}$
 $C: \models b (\subseteq C, Y) = (B_1', B_2') \text{ and}$
 $D: (\{\}, \text{False}) \models c (\subseteq B_1, X) = \text{Some } (D, Z) \text{ and}$
 $E: (\{\}, \text{False}) \models c (\subseteq B_1', Y) = \text{Some } (D', Z') \text{ and}$
 $F: r_1 \in A \text{ and}$

$G: s_1 = r_1 (\subseteq \text{state} \cap X)$ **and**
 $H: \text{bval } b \ s_1$ **and**
 $I: \bigwedge C \ B \ Y \ W \ U. (\text{case} \models b (\subseteq C, Y) \text{ of } (B_1', B_2') \Rightarrow$
 $\text{case} \vdash c (\subseteq B_1', Y) \text{ of } (C', Y') \Rightarrow$
 $\text{case} \models b (\subseteq C', Y') \text{ of } (B_1'', B_2'') \Rightarrow$
 $\text{if } (\forall s \in \text{Univ? } C \ Y \cup \text{Univ? } C' \ Y'. \forall x \in \text{bvars } b. \text{All } (\text{interf } s (\text{dom } x))) \wedge$
 $(\forall p \in U. \text{case } p \text{ of } (B, W) \Rightarrow \forall s \in B. \forall x \in W. \text{All } (\text{interf } s (\text{dom } x)))$
 $\text{then case } (\{\}, \text{False}) \models c (\subseteq B_1', Y) \text{ of}$
 $\text{None} \Rightarrow \text{None} \mid \text{Some } - \Rightarrow \text{case } (\{\}, \text{False}) \models c (\subseteq B_1'', Y') \text{ of}$
 $\text{None} \Rightarrow \text{None} \mid \text{Some } - \Rightarrow \text{Some } (B_2' \cup B_2'', \text{Univ?? } B_2' \ Y \cap Y')$
 $\text{else None}) = \text{Some } (B, W) \Rightarrow$
 $\exists r \in C. s_2 = r (\subseteq \text{state} \cap Y) \Rightarrow \exists r \in B. s_3 = r (\subseteq \text{state} \cap W)$
 $(\text{is } \bigwedge C \ B \ Y \ W \ U. ?P \ C \ B \ Y \ W \ U \Rightarrow - \Rightarrow -)$ **and**
 $J: \bigwedge A \ B \ X \ Y \ U \ v. (U, v) \models c (\subseteq A, X) = \text{Some } (B, Y) \Rightarrow$
 $\exists r \in A. s_1 = r (\subseteq \text{state} \cap X) \Rightarrow \exists r \in B. s_2 = r (\subseteq \text{state} \cap Y)$ **and**
 $K: \forall s \in \text{Univ? } A \ X \cup \text{Univ? } C \ Y. \forall x \in \text{bvars } b. \text{All } (\text{interf } s (\text{dom } x))$ **and**
 $L: \forall p \in U. \forall B \ W. p = (B, W) \rightarrow$
 $(\forall s \in B. \forall x \in W. \text{All } (\text{interf } s (\text{dom } x)))$
shows $\exists r \in B_2 \cup B_2'. s_3 = r (\subseteq \text{state} \cap \text{Univ?? } B_2 \ X \cap Y)$
proof –
obtain $C' \ Y'$ **where** $M: (C', Y') = \vdash c (\subseteq B_1', Y)$
by $(\text{cases} \vdash c (\subseteq B_1', Y), \text{simp})$
obtain $B_1'' \ B_2''$ **where** $N: (B_1'', B_2'') = \models b (\subseteq C', Y')$
by $(\text{cases} \models b (\subseteq C', Y'), \text{simp})$
let $?B = B_2' \cup B_2''$
let $?W = \text{Univ?? } B_2' \ Y \cap Y'$
have $(C, Y) = \vdash c (\subseteq C, Y)$
using ctyping1-idem **and** B **by** auto
moreover have $B_1' \subseteq C$
using C **by** $(\text{blast dest: btyping2-un-eq})$
ultimately have $O: C' \subseteq C \wedge Y \subseteq Y'$
by $(\text{rule ctyping1-mono } [OF - M], \text{simp})$
hence $\text{Univ? } C' \ Y' \subseteq \text{Univ? } C \ Y$
by $(\text{auto simp: univ-states-if-def})$
moreover from I **have** $?P \ C \ ?B \ Y \ ?W \ U \Rightarrow$
 $\exists r \in C. s_2 = r (\subseteq \text{state} \cap Y) \Rightarrow \exists r \in ?B. s_3 = r (\subseteq \text{state} \cap ?W)$.
ultimately have $(\text{case } (\{\}, \text{False}) \models c (\subseteq B_1'', Y') \text{ of}$
 $\text{None} \Rightarrow \text{None} \mid \text{Some } - \Rightarrow \text{Some } (?B, ?W)) = \text{Some } (?B, ?W) \Rightarrow$
 $\exists r \in C. s_2 = r (\subseteq \text{state} \cap Y) \Rightarrow \exists r \in ?B. s_3 = r (\subseteq \text{state} \cap ?W)$
using C **and** E **and** K **and** L **and** M **and** N
by $(\text{fastforce split: if-split-asm prod.split-asm})$
moreover have $P: B_1'' \subseteq B_1' \wedge B_2'' \subseteq B_2'$
by $(\text{metis btyping2-mono } C \ N \ O)$
hence $\exists D'' \ Z''. (\{\}, \text{False}) \models c (\subseteq B_1'', Y') =$
 $\text{Some } (D'', Z'') \wedge D'' \subseteq D' \wedge Z' \subseteq Z''$
using E **and** O **by** $(\text{auto intro: ctyping2-mono})$
ultimately have
 $\exists r \in C. s_2 = r (\subseteq \text{state} \cap Y) \Rightarrow \exists r \in ?B. s_3 = r (\subseteq \text{state} \cap ?W)$
by fastforce

moreover from A and D and F and G and H and J obtain r_2 where
 $r_2 \in D$ and $s_2 = r_2$ ($\subseteq \text{state} \cap Z$)
 by (*drule-tac btyping2-approx, blast, force*)
 moreover have $D \subseteq C \wedge Y \subseteq Z$
 using B and D by (*rule ctyping1-ctyping2*)
 ultimately obtain r_3 where $Q: r_3 \in ?B$ and $R: s_3 = r_3$ ($\subseteq \text{state} \cap ?W$)
 by *blast*
 show *?thesis*
 proof (*rule bezI [of - r3]*)
 show $s_3 = r_3$ ($\subseteq \text{state} \cap \text{Univ}?? B_2 X \cap Y$)
 using O and R by *auto*
 next
 show $r_3 \in B_2 \cup B_2'$
 using P and Q by *blast*
 qed
 qed

lemmas *ctyping2-approx-while-3* =
ctyping2-approx-while-aux [**where** $B_2 = \{\}$, *simplified*]

lemma *ctyping2-approx-while-4*:

$\models b$ ($\subseteq A, X$) = (B_1, B_2) ;
 $\vdash c$ ($\subseteq B_1, X$) = (C, Y) ;
 $\models b$ ($\subseteq C, Y$) = (B_1', B_2') ;
 $(\{\}, \text{False}) \models c$ ($\subseteq B_1, X$) = *Some* (D, Z) ;
 $(\{\}, \text{False}) \models c$ ($\subseteq B_1', Y$) = *Some* (D', Z') ;
 $r_1 \in A; s_1 = r_1$ ($\subseteq \text{state} \cap X$); *bval* b s_1 ;
 $\bigwedge C B Y W U. (\text{case } \models b (\subseteq C, Y) \text{ of } (B_1', B_2') \Rightarrow$
 $\text{case } \vdash c (\subseteq B_1', Y) \text{ of } (C', Y') \Rightarrow$
 $\text{case } \models b (\subseteq C', Y') \text{ of } (B_1'', B_2'') \Rightarrow$
 $\text{if } (\forall s \in \text{Univ}?? C Y \cup \text{Univ}?? C' Y'. \forall x \in \text{bvars } b. \text{All } (\text{interf } s (\text{dom } x))) \wedge$
 $(\forall p \in U. \text{case } p \text{ of } (B, W) \Rightarrow \forall s \in B. \forall x \in W. \text{All } (\text{interf } s (\text{dom } x)))$
 $\text{then case } (\{\}, \text{False}) \models c (\subseteq B_1', Y) \text{ of}$
 $\text{None} \Rightarrow \text{None} \mid \text{Some} - \Rightarrow \text{case } (\{\}, \text{False}) \models c (\subseteq B_1'', Y') \text{ of}$
 $\text{None} \Rightarrow \text{None} \mid \text{Some} - \Rightarrow \text{Some } (B_2' \cup B_2'', \text{Univ}?? B_2' Y \cap Y')$
 $\text{else None}) = \text{Some } (B, W) \Rightarrow$
 $\exists r \in C. s_2 = r$ ($\subseteq \text{state} \cap Y$) $\Rightarrow \exists r \in B. s_3 = r$ ($\subseteq \text{state} \cap W$);
 $\bigwedge A B X Y U v. (U, v) \models c (\subseteq A, X) = \text{Some } (B, Y) \Rightarrow$
 $\exists r \in A. s_1 = r$ ($\subseteq \text{state} \cap X$) $\Rightarrow \exists r \in B. s_2 = r$ ($\subseteq \text{state} \cap Y$);
 $\forall s \in \text{Univ}?? A X \cup \text{Univ}?? C Y. \forall x \in \text{bvars } b. \text{All } (\text{interf } s (\text{dom } x));$
 $\forall p \in U. \forall B W. p = (B, W) \longrightarrow (\forall s \in B. \forall x \in W. \text{All } (\text{interf } s (\text{dom } x)));$
 $\forall r \in B_2 \cup B_2'. \exists x \in \text{state} \cap (X \cap Y). s_3 x \neq r x \Rightarrow$
False

by (*drule ctyping2-approx-while-aux, assumption+, auto*)

lemma *ctyping2-approx*:

$\models (c, s) \Rightarrow t; (U, v) \models c (\subseteq A, X) = \text{Some } (B, Y);$
 $s \in \text{Univ } A$ ($\subseteq \text{state} \cap X$) $\Rightarrow t \in \text{Univ } B$ ($\subseteq \text{state} \cap Y$)
 proof (*induction arbitrary: A B X Y U v rule: big-step-induct*)


```

fix A B X Y U v b c1 c2 s t
show
   $\llbracket \text{bval } b \text{ s}; (c_1, s) \Rightarrow t; \wedge A C X Y U v. (U, v) \models c_1 (\subseteq A, X) = \text{Some } (C, Y) \Rightarrow$ 
 $s \in \text{Univ } A (\subseteq \text{state} \cap X) \Rightarrow$ 
 $t \in \text{Univ } C (\subseteq \text{state} \cap Y);$ 
 $(U, v) \models \text{IF } b \text{ THEN } c_1 \text{ ELSE } c_2 (\subseteq A, X) = \text{Some } (B, Y);$ 
 $s \in \text{Univ } A (\subseteq \text{state} \cap X) \rrbracket \Rightarrow$ 
 $t \in \text{Univ } B (\subseteq \text{state} \cap Y)$ 
  by (auto split: option.split-asm prod.split-asm,
    rule ctyping2-approx-if-1)
next
  fix A B X Y U v b c1 c2 s t
  show
     $\llbracket \neg \text{bval } b \text{ s}; (c_2, s) \Rightarrow t; \wedge A C X Y U v. (U, v) \models c_2 (\subseteq A, X) = \text{Some } (C, Y) \Rightarrow$ 
 $s \in \text{Univ } A (\subseteq \text{state} \cap X) \Rightarrow$ 
 $t \in \text{Univ } C (\subseteq \text{state} \cap Y);$ 
 $(U, v) \models \text{IF } b \text{ THEN } c_1 \text{ ELSE } c_2 (\subseteq A, X) = \text{Some } (B, Y);$ 
 $s \in \text{Univ } A (\subseteq \text{state} \cap X) \rrbracket \Rightarrow$ 
 $t \in \text{Univ } B (\subseteq \text{state} \cap Y)$ 
    by (auto split: option.split-asm prod.split-asm,
      rule ctyping2-approx-if-2)
  next
    fix A B X Y U v b c s1 s2 s3
    show
       $\llbracket \text{bval } b \text{ s}_1; (c, s_1) \Rightarrow s_2; \wedge A B X Y U v. (U, v) \models c (\subseteq A, X) = \text{Some } (B, Y) \Rightarrow$ 
 $s_1 \in \text{Univ } A (\subseteq \text{state} \cap X) \Rightarrow$ 
 $s_2 \in \text{Univ } B (\subseteq \text{state} \cap Y);$ 
 $(\text{WHILE } b \text{ DO } c, s_2) \Rightarrow s_3;$ 
 $\wedge A B X Y U v. (U, v) \models \text{WHILE } b \text{ DO } c (\subseteq A, X) = \text{Some } (B, Y) \Rightarrow$ 
 $s_2 \in \text{Univ } A (\subseteq \text{state} \cap X) \Rightarrow$ 
 $s_3 \in \text{Univ } B (\subseteq \text{state} \cap Y);$ 
 $(U, v) \models \text{WHILE } b \text{ DO } c (\subseteq A, X) = \text{Some } (B, Y);$ 
 $s_1 \in \text{Univ } A (\subseteq \text{state} \cap X) \rrbracket \Rightarrow$ 
 $s_3 \in \text{Univ } B (\subseteq \text{state} \cap Y)$ 
      by (auto split: if-split-asm option.split-asm prod.split-asm,
        erule-tac [2] ctyping2-approx-while-4,
        erule ctyping2-approx-while-3)
    qed (auto split: if-split-asm option.split-asm prod.split-asm)

end

end

```

4 Sufficiency of well-typedness for information flow correctness

```

theory Correctness
  imports Overapproximation
begin

```

The purpose of this section is to prove that type system *ctyping2* is correct in that it guarantees that well-typed programs satisfy the information flow correctness criterion expressed by predicate *correct*, namely that if the type system outputs a value other than *None* (that is, a *pass* verdict) when it is input program *c*, state set *A*, and *vname* set *X*, then *correct c A X* (theorem *ctyping2-correct*).

This proof makes use of the lemmas *ctyping1-idem* and *ctyping2-approx* proven in the previous sections.

4.1 Global context proofs

lemma *flow-append-1*:

```

assumes A:  $\bigwedge cfs' :: (com \times state) \text{ list.}$ 
   $c \# \text{map fst } (cfs :: (com \times state) \text{ list}) = \text{map fst } cfs' \implies$ 
   $\text{flow-aux } (\text{map fst } cfs' @ \text{map fst } cfs'') =$ 
   $\text{flow-aux } (\text{map fst } cfs') @ \text{flow-aux } (\text{map fst } cfs'')$ 
shows  $\text{flow-aux } (c \# \text{map fst } cfs @ \text{map fst } cfs'') =$ 
   $\text{flow-aux } (c \# \text{map fst } cfs) @ \text{flow-aux } (\text{map fst } cfs'')$ 
using A [of (c,  $\lambda x. 0$ ) # cfs] by simp

```

lemma *flow-append*:

```

 $\text{flow } (cfs @ cfs') = \text{flow } cfs @ \text{flow } cfs'$ 
by (simp add: flow-def, induction map fst cfs arbitrary: cfs
  rule: flow-aux.induct, auto, rule flow-append-1)

```

lemma *flow-cons*:

```

 $\text{flow } (cf \# cfs) = \text{flow-aux } (\text{fst } cf \# []) @ \text{flow } cfs$ 
by (subgoal-tac cf # cfs = [cf] @ cfs, simp only: flow-append,
  simp-all add: flow-def)

```

lemma *small-steps-l-append*:

```

 $\llbracket (c, s) \rightarrow^* \{cfs\} (c', s'); (c', s') \rightarrow^* \{cfs'\} (c'', s'') \rrbracket \implies$ 
 $(c, s) \rightarrow^* \{cfs @ cfs'\} (c'', s'')$ 
by (induction c' s' cfs' c'' s'' rule: small-steps-l-induct,
  simp, simp only: append-assoc [symmetric] small-steps-l.simps)

```

lemma *small-steps-l-cons-1*:

```

 $(c, s) \rightarrow^* \{[cf]\} (c'', s'') \implies$ 
 $cf = (c, s) \wedge$ 

```

$(\exists c' s'. (c, s) \rightarrow (c', s') \wedge (c', s') \rightarrow^* \{\square\} (c'', s''))$
by (*subst* (*asm*) *append-Nil* [*symmetric*],
simp only: small-stepspl.simps, simp)

lemma *small-stepspl-cons-2*:
 $\llbracket (c, s) \rightarrow^* \{cf \# cfs\} (c'', s'') \implies$
 $cf = (c, s) \wedge$
 $(\exists c' s'. (c, s) \rightarrow (c', s') \wedge (c', s') \rightarrow^* \{cfs\} (c'', s''));$
 $(c, s) \rightarrow^* \{cf \# cfs @ [(c'', s'')]\} (c''', s''') \rrbracket \implies$
 $cf = (c, s) \wedge$
 $(\exists c' s'. (c, s) \rightarrow (c', s') \wedge$
 $(c', s') \rightarrow^* \{cfs @ [(c'', s'')]\} (c''', s'''))$
by (*simp only: append-Cons* [*symmetric*],
simp only: small-stepspl.simps, simp)

lemma *small-stepspl-cons*:
 $(c, s) \rightarrow^* \{cf \# cfs\} (c'', s'') \implies$
 $cf = (c, s) \wedge$
 $(\exists c' s'. (c, s) \rightarrow (c', s') \wedge (c', s') \rightarrow^* \{cfs\} (c'', s''))$
by (*induction c s cfs c'' s'' rule: small-stepspl-induct,*
erule small-stepspl-cons-1, rule small-stepspl-cons-2)

lemma *small-steps-stepspl-1*:
 $\exists cfs. (c, s) \rightarrow^* \{cfs\} (c, s)$
by (*rule exI* [*of* - \square], *simp*)

lemma *small-steps-stepspl-2*:
 $\llbracket (c, s) \rightarrow (c', s'); (c', s') \rightarrow^* \{cfs\} (c'', s'') \rrbracket \implies$
 $\exists cfs'. (c, s) \rightarrow^* \{cfs'\} (c'', s'')$
by (*rule exI* [*of* - $\llbracket (c, s) \rrbracket @ cfs$], *rule small-stepspl-append*
 $\llbracket \text{where } c' = c' \text{ and } s' = s' \rrbracket$, *subst append-Nil* [*symmetric*],
simp only: small-stepspl.simps)

lemma *small-steps-stepspl*:
 $(c, s) \rightarrow^* (c', s') \implies \exists cfs. (c, s) \rightarrow^* \{cfs\} (c', s')$
by (*induction c s c' s' rule: star-induct,*
rule small-steps-stepspl-1, blast intro: small-steps-stepspl-2)

lemma *small-stepspl-steps*:
 $(c, s) \rightarrow^* \{cfs\} (c', s') \implies (c, s) \rightarrow^* (c', s')$
by (*induction c s cfs c' s' rule: small-stepspl-induct,*
auto intro: star-trans)

lemma *small-stepspl-skip*:
 $(SKIP, s) \rightarrow^* \{cfs\} (c, t) \implies$
 $(c, t) = (SKIP, s) \wedge \text{flow } cfs = \square$
by (*induction SKIP s cfs c t rule: small-stepspl-induct,*
auto simp: flow-def)

lemma *small-stepsl-assign-1*:

$(x ::= a, s) \rightarrow^* \{\Box\} (c', s') \implies$
 $(c', s') = (x ::= a, s) \wedge \text{flow } \Box = \Box \vee$
 $(c', s') = (\text{SKIP}, s(x := \text{aval } a \ s)) \wedge \text{flow } \Box = [x ::= a]$
by (*simp add: flow-def*)

lemma *small-stepsl-assign-2*:

$\llbracket (x ::= a, s) \rightarrow^* \{cfs\} (c', s') \implies$
 $(c', s') = (x ::= a, s) \wedge \text{flow } cfs = \Box \vee$
 $(c', s') = (\text{SKIP}, s(x := \text{aval } a \ s)) \wedge \text{flow } cfs = [x ::= a];$
 $(x ::= a, s) \rightarrow^* \{cfs @ [(c', s')]\} (c'', s'') \implies$
 $(c'', s'') = (x ::= a, s) \wedge$
 $\text{flow } (cfs @ [(c', s')]) = \Box \vee$
 $(c'', s'') = (\text{SKIP}, s(x := \text{aval } a \ s)) \wedge$
 $\text{flow } (cfs @ [(c', s')]) = [x ::= a]$
by (*auto, (simp add: flow-append, simp add: flow-def)+*)

lemma *small-stepsl-assign*:

$(x ::= a, s) \rightarrow^* \{cfs\} (c, t) \implies$
 $(c, t) = (x ::= a, s) \wedge \text{flow } cfs = \Box \vee$
 $(c, t) = (\text{SKIP}, s(x := \text{aval } a \ s)) \wedge \text{flow } cfs = [x ::= a]$
by (*induction x ::= a :: com s cfs c t rule: small-stepsl-induct,*
erule small-stepsl-assign-1, rule small-stepsl-assign-2)

lemma *small-stepsl-seq-1*:

$(c_1;; c_2, s) \rightarrow^* \{\Box\} (c', s') \implies$
 $(\exists c'' cfs'. c' = c'';; c_2 \wedge$
 $(c_1, s) \rightarrow^* \{cfs'\} (c'', s') \wedge$
 $\text{flow } \Box = \text{flow } cfs') \vee$
 $(\exists s'' cfs' cfs''. \text{length } cfs'' < \text{length } \Box \wedge$
 $(c_1, s) \rightarrow^* \{cfs'\} (\text{SKIP}, s'') \wedge$
 $(c_2, s'') \rightarrow^* \{cfs''\} (c', s') \wedge$
 $\text{flow } \Box = \text{flow } cfs' @ \text{flow } cfs''))$
by *force*

lemma *small-stepsl-seq-2*:

assumes

$A: (c_1;; c_2, s) \rightarrow^* \{cfs\} (c', s') \implies$
 $(\exists c'' cfs'. c' = c'';; c_2 \wedge$
 $(c_1, s) \rightarrow^* \{cfs'\} (c'', s') \wedge$
 $\text{flow } cfs = \text{flow } cfs') \vee$
 $(\exists s'' cfs' cfs''. \text{length } cfs'' < \text{length } cfs \wedge$
 $(c_1, s) \rightarrow^* \{cfs'\} (\text{SKIP}, s'') \wedge$
 $(c_2, s'') \rightarrow^* \{cfs''\} (c', s') \wedge$
 $\text{flow } cfs = \text{flow } cfs' @ \text{flow } cfs''))$ **and**
 $B: (c_1;; c_2, s) \rightarrow^* \{cfs @ [(c', s')]\} (c'', s'')$

shows

$(\exists d \text{ cfs}'. c'' = d;; c_2 \wedge$
 $(c_1, s) \rightarrow^* \{cfs'\} (d, s'') \wedge$
 $flow(cfs @ [(c', s')]) = flow cfs') \vee$
 $(\exists t \text{ cfs}' \text{ cfs}''. length \text{ cfs}'' < length(cfs @ [(c', s')]) \wedge$
 $(c_1, s) \rightarrow^* \{cfs'\} (SKIP, t) \wedge$
 $(c_2, t) \rightarrow^* \{cfs''\} (c'', s'') \wedge$
 $flow(cfs @ [(c', s')]) = flow cfs' @ flow cfs'')$
(is ?P \vee ?Q)

proof –

{
assume $C: (c', s') \rightarrow (c'', s'')$
assume
 $(\exists d. c' = d;; c_2 \wedge (\exists \text{ cfs}'.$
 $(c_1, s) \rightarrow^* \{cfs'\} (d, s') \wedge$
 $flow \text{ cfs} = flow \text{ cfs}') \vee$
 $(\exists t \text{ cfs}' \text{ cfs}''. length \text{ cfs}'' < length \text{ cfs} \wedge$
 $(c_1, s) \rightarrow^* \{cfs'\} (SKIP, t) \wedge$
 $(c_2, t) \rightarrow^* \{cfs''\} (c', s') \wedge$
 $flow \text{ cfs} = flow \text{ cfs}' @ flow \text{ cfs}'')$
(is $(\exists d. ?R \text{ d} \wedge (\exists \text{ cfs}'. ?S \text{ d cfs}')) \vee$
 $(\exists t \text{ cfs}' \text{ cfs}''. ?T \text{ t cfs}' \text{ cfs}''))$
hence ?thesis

proof

assume $\exists c''. ?R \text{ c}'' \wedge (\exists \text{ cfs}'. ?S \text{ c}'' \text{ cfs}')$

then obtain d **and** cfs' **where**

$D: c' = d;; c_2$ **and**

$E: (c_1, s) \rightarrow^* \{cfs'\} (d, s')$ **and**

$F: flow \text{ cfs} = flow \text{ cfs}'$

by blast

hence $(d;; c_2, s') \rightarrow (c'', s'')$

using C **by simp**

moreover {

assume

$G: d = SKIP$ **and**

$H: (c'', s'') = (c_2, s')$

have $?Q$

proof ($rule \text{ exI } [of - s']$, $rule \text{ exI } [of - cfs']$,

$rule \text{ exI } [of - []]$)

from D **and** E **and** F **and** G **and** H **show**

$length [] < length(cfs @ [(c', s')]) \wedge$

$(c_1, s) \rightarrow^* \{cfs'\} (SKIP, s') \wedge$

$(c_2, s') \rightarrow^* \{[]\} (c'', s'') \wedge$

$flow(cfs @ [(c', s')]) = flow \text{ cfs}' @ flow []$

by ($simp \text{ add: flow-append, simp add: flow-def}$)

qed

}

moreover {

fix $d' \text{ t}'$

```

assume
   $G: (d, s') \rightarrow (d', t')$  and
   $H: (c'', s'') = (d';; c_2, t')$ 
have  $?P$ 
proof (rule  $exI$  [of -  $d'$ ], rule  $exI$  [of -  $cfs' @ [(d, s')]$ ])
  from  $D$  and  $E$  and  $F$  and  $G$  and  $H$  show
     $c'' = d';; c_2 \wedge$ 
     $(c_1, s) \rightarrow^* \{cfs' @ [(d, s')]\} (d', s') \wedge$ 
     $flow (cfs @ [(c', s')]) = flow (cfs' @ [(d, s')])$ 
    by (simp add: flow-append, simp add: flow-def)
  qed
}
ultimately show  $?thesis$ 
by blast
next
assume  $\exists t \ cfs' \ cfs''. \ ?T \ t \ cfs' \ cfs''$ 
then obtain  $t$  and  $cfs'$  and  $cfs''$  where
   $D: length \ cfs'' < length \ cfs$  and
   $E: (c_1, s) \rightarrow^* \{cfs'\} (SKIP, t)$  and
   $F: (c_2, t) \rightarrow^* \{cfs''\} (c', s')$  and
   $G: flow \ cfs = flow \ cfs' @ flow \ cfs''$ 
by blast
show  $?thesis$ 
proof (rule  $disjI2$ , rule  $exI$  [of -  $t$ ], rule  $exI$  [of -  $cfs'$ ],
  rule  $exI$  [of -  $cfs'' @ [(c', s')]$ ])
  from  $C$  and  $D$  and  $E$  and  $F$  and  $G$  show
     $length (cfs'' @ [(c', s')]) < length (cfs @ [(c', s')]) \wedge$ 
     $(c_1, s) \rightarrow^* \{cfs'\} (SKIP, t) \wedge$ 
     $(c_2, t) \rightarrow^* \{cfs'' @ [(c', s')]\} (c'', s'') \wedge$ 
     $flow (cfs @ [(c', s')]) =$ 
     $flow \ cfs' @ flow (cfs'' @ [(c', s')])$ 
    by (simp add: flow-append)
  qed
qed
}
with  $A$  and  $B$  show  $?thesis$ 
by simp
qed

```

lemma *small-stepsl-seq*:

```

 $(c_1;; c_2, s) \rightarrow^* \{cfs\} (c, t) \implies$ 
 $(\exists c' \ cfs'. \ c = c';; c_2 \wedge$ 
 $(c_1, s) \rightarrow^* \{cfs'\} (c', t) \wedge$ 
 $flow \ cfs = flow \ cfs') \vee$ 
 $(\exists s' \ cfs' \ cfs''. \ length \ cfs'' < length \ cfs \wedge$ 
 $(c_1, s) \rightarrow^* \{cfs'\} (SKIP, s') \wedge (c_2, s') \rightarrow^* \{cfs''\} (c, t) \wedge$ 
 $flow \ cfs = flow \ cfs' @ flow \ cfs'')$ 
by (induction  $c_1;; c_2 \ s \ cfs \ c \ t$  arbitrary:  $c_1 \ c_2$ 
rule: small-stepsl-induct, erule small-stepsl-seq-1,

```

rule *small-stepsl-seq-2*)

lemma *small-stepsl-if-1*:

$(IF\ b\ THEN\ c_1\ ELSE\ c_2,\ s) \rightarrow^*\{\Box\} (c', s') \implies$
 $(c', s') = (IF\ b\ THEN\ c_1\ ELSE\ c_2,\ s) \wedge$
 $flow\ \Box = \Box \vee$
 $bval\ b\ s \wedge (c_1,\ s) \rightarrow^*\{tl\ \Box\} (c', s') \wedge$
 $flow\ \Box = \langle bvars\ b \rangle \# flow\ (tl\ \Box) \vee$
 $\neg bval\ b\ s \wedge (c_2,\ s) \rightarrow^*\{tl\ \Box\} (c', s') \wedge$
 $flow\ \Box = \langle bvars\ b \rangle \# flow\ (tl\ \Box)$
by (*simp add: flow-def*)

lemma *small-stepsl-if-2*:

assumes

$A: (IF\ b\ THEN\ c_1\ ELSE\ c_2,\ s) \rightarrow^*\{cfs\} (c', s') \implies$
 $(c', s') = (IF\ b\ THEN\ c_1\ ELSE\ c_2,\ s) \wedge$
 $flow\ cfs = \Box \vee$
 $bval\ b\ s \wedge (c_1,\ s) \rightarrow^*\{tl\ cfs\} (c', s') \wedge$
 $flow\ cfs = \langle bvars\ b \rangle \# flow\ (tl\ cfs) \vee$
 $\neg bval\ b\ s \wedge (c_2,\ s) \rightarrow^*\{tl\ cfs\} (c', s') \wedge$
 $flow\ cfs = \langle bvars\ b \rangle \# flow\ (tl\ cfs)$ **and**
 $B: (IF\ b\ THEN\ c_1\ ELSE\ c_2,\ s) \rightarrow^*\{cfs\ @\ [(c', s')]\} (c'', s'')$

shows

$(c'', s'') = (IF\ b\ THEN\ c_1\ ELSE\ c_2,\ s) \wedge$
 $flow\ (cfs\ @\ [(c', s')]) = \Box \vee$
 $bval\ b\ s \wedge (c_1,\ s) \rightarrow^*\{tl\ (cfs\ @\ [(c', s')])\} (c'', s'') \wedge$
 $flow\ (cfs\ @\ [(c', s')]) = \langle bvars\ b \rangle \# flow\ (tl\ (cfs\ @\ [(c', s')])) \vee$
 $\neg bval\ b\ s \wedge (c_2,\ s) \rightarrow^*\{tl\ (cfs\ @\ [(c', s')])\} (c'', s'') \wedge$
 $flow\ (cfs\ @\ [(c', s')]) = \langle bvars\ b \rangle \# flow\ (tl\ (cfs\ @\ [(c', s')]))$
 $(is\ -\ \vee\ ?P)$

proof –

{

assume

$C: (IF\ b\ THEN\ c_1\ ELSE\ c_2,\ s) \rightarrow^*\{cfs\} (c', s')$ **and**
 $D: (c', s') \rightarrow (c'', s'')$

assume

$c' = IF\ b\ THEN\ c_1\ ELSE\ c_2 \wedge s' = s \wedge$
 $flow\ cfs = \Box \vee$
 $bval\ b\ s \wedge (c_1,\ s) \rightarrow^*\{tl\ cfs\} (c', s') \wedge$
 $flow\ cfs = \langle bvars\ b \rangle \# flow\ (tl\ cfs) \vee$
 $\neg bval\ b\ s \wedge (c_2,\ s) \rightarrow^*\{tl\ cfs\} (c', s') \wedge$
 $flow\ cfs = \langle bvars\ b \rangle \# flow\ (tl\ cfs)$
 $(is\ ?Q \vee ?R \vee ?S)$

hence $?P$

proof (*rule disjE, erule-tac [2] disjE*)

assume $?Q$

moreover from this have $(IF\ b\ THEN\ c_1\ ELSE\ c_2,\ s) \rightarrow (c'', s'')$

using D **by** *simp*

```

ultimately show ?thesis
  using C by (erule-tac IfE, auto dest: small-steps-l-cons
    simp: tl-append flow-cons split: list.split)
next
  assume ?R
  with C and D show ?thesis
    by (auto simp: tl-append flow-cons split: list.split)
next
  assume ?S
  with C and D show ?thesis
    by (auto simp: tl-append flow-cons split: list.split)
qed
}
with A and B show ?thesis
  by simp
qed

```

lemma *small-steps-l-if*:

$$\begin{aligned}
& (IF\ b\ THEN\ c_1\ ELSE\ c_2,\ s) \rightarrow^*\{cfs\}\ (c,\ t) \implies \\
& (c,\ t) = (IF\ b\ THEN\ c_1\ ELSE\ c_2,\ s) \wedge \\
& \quad flow\ cfs = [] \vee \\
& \quad bval\ b\ s \wedge (c_1,\ s) \rightarrow^*\{tl\ cfs\}\ (c,\ t) \wedge \\
& \quad \quad flow\ cfs = \langle bvars\ b \rangle \# flow\ (tl\ cfs) \vee \\
& \quad \neg bval\ b\ s \wedge (c_2,\ s) \rightarrow^*\{tl\ cfs\}\ (c,\ t) \wedge \\
& \quad \quad flow\ cfs = \langle bvars\ b \rangle \# flow\ (tl\ cfs)
\end{aligned}$$

by (*induction IF b THEN c₁ ELSE c₂ s cfs c t arbitrary: b c₁ c₂*
rule: small-steps-l-induct, erule small-steps-l-if-1,
rule small-steps-l-if-2)

lemma *small-steps-l-while-1*:

$$\begin{aligned}
& (WHILE\ b\ DO\ c,\ s) \rightarrow^*\{[]\}\ (c',\ s') \implies \\
& (c',\ s') = (WHILE\ b\ DO\ c,\ s) \wedge flow\ [] = [] \vee \\
& (IF\ b\ THEN\ c;;\ WHILE\ b\ DO\ c\ ELSE\ SKIP,\ s) \rightarrow^*\{tl\ []\}\ (c',\ s') \wedge \\
& \quad flow\ [] = flow\ (tl\ [])
\end{aligned}$$

by (*simp add: flow-def*)

lemma *small-steps-l-while-2*:

assumes

$$\begin{aligned}
& A: (WHILE\ b\ DO\ c,\ s) \rightarrow^*\{cfs\}\ (c',\ s') \implies \\
& (c',\ s') = (WHILE\ b\ DO\ c,\ s) \wedge \\
& \quad flow\ cfs = [] \vee \\
& (IF\ b\ THEN\ c;;\ WHILE\ b\ DO\ c\ ELSE\ SKIP,\ s) \rightarrow^*\{tl\ cfs\}\ (c',\ s') \wedge \\
& \quad flow\ cfs = flow\ (tl\ cfs) \textbf{ and} \\
& B: (WHILE\ b\ DO\ c,\ s) \rightarrow^*\{cfs\ @\ [(c',\ s')]\}\ (c'',\ s'')
\end{aligned}$$

shows

$$\begin{aligned}
& (c'',\ s'') = (WHILE\ b\ DO\ c,\ s) \wedge \\
& \quad flow\ (cfs\ @\ [(c',\ s')]) = [] \vee \\
& (IF\ b\ THEN\ c;;\ WHILE\ b\ DO\ c\ ELSE\ SKIP,\ s)
\end{aligned}$$

$\rightarrow^*\{tl\ (cfs\ @\ [(c',\ s')])\}\ (c'',\ s'') \wedge$
 $flow\ (cfs\ @\ [(c',\ s')]) = flow\ (tl\ (cfs\ @\ [(c',\ s')]))$
 $(is\ -\ \vee\ ?P)$
proof –
 {
 assume
 $C: (WHILE\ b\ DO\ c,\ s) \rightarrow^*\{cfs\}\ (c',\ s')$ **and**
 $D: (c',\ s') \rightarrow (c'',\ s'')$
 assume
 $c' = WHILE\ b\ DO\ c \wedge s' = s \wedge$
 $flow\ cfs = [] \vee$
 $(IF\ b\ THEN\ c;;\ WHILE\ b\ DO\ c\ ELSE\ SKIP,\ s) \rightarrow^*\{tl\ cfs\}\ (c',\ s') \wedge$
 $flow\ cfs = flow\ (tl\ cfs)$
 $(is\ ?Q \vee ?R)$
 hence $?P$
 proof
 assume $?Q$
 moreover from this have $(WHILE\ b\ DO\ c,\ s) \rightarrow (c'',\ s'')$
 using D **by** *simp*
 ultimately show $?thesis$
 using C **by** (*erule-tac WhileE, auto dest: small-steps-l-cons*
 simp: tl-append flow-cons split: list.split)
 next
 assume $?R$
 with C **and** D **show** $?thesis$
 by (*auto simp: tl-append flow-cons split: list.split*)
 qed
 }
with A **and** B **show** $?thesis$
 by *simp*
qed

lemma *small-steps-l-while*:
 $(WHILE\ b\ DO\ c,\ s) \rightarrow^*\{cfs\}\ (c',\ s') \implies$
 $(c',\ s') = (WHILE\ b\ DO\ c,\ s) \wedge$
 $flow\ cfs = [] \vee$
 $(IF\ b\ THEN\ c;;\ WHILE\ b\ DO\ c\ ELSE\ SKIP,\ s) \rightarrow^*\{tl\ cfs\}\ (c',\ s') \wedge$
 $flow\ cfs = flow\ (tl\ cfs)$
by (*induction WHILE b DO c s cfs c' s' arbitrary: b c*
rule: small-steps-l-induct, erule small-steps-l-while-1,
rule small-steps-l-while-2)

lemma *bvars-bval*:
 $s = t (\subseteq\ bvars\ b) \implies bval\ b\ s = bval\ b\ t$
by (*induction b, simp-all, rule arg-cong2, auto intro: avars-aval*)

lemma *run-flow-append*:
 $run-flow\ (cs\ @\ cs')\ s = run-flow\ cs'\ (run-flow\ cs\ s)$

by (*induction cs s rule: run-flow.induct, simp-all (no-asm)*)

lemma *no-upd-append*:

$no_upd\ (cs\ @\ cs')\ x = (no_upd\ cs\ x \wedge no_upd\ cs'\ x)$

by (*induction cs, simp-all*)

lemma *no-upd-run-flow*:

$no_upd\ cs\ x \implies run_flow\ cs\ s\ x = s\ x$

by (*induction cs s rule: run-flow.induct, auto*)

lemma *small-steps-l-run-flow-1*:

$(c, s) \rightarrow^*\{\square\}\ (c', s') \implies s' = run_flow\ (flow\ \square)\ s$

by (*simp add: flow-def*)

lemma *small-steps-l-run-flow-2*:

$(c, s) \rightarrow (c', s') \implies s' = run_flow\ (flow_aux\ [c])\ s$

by (*induction [c] arbitrary: c c' rule: flow-aux.induct, auto*)

lemma *small-steps-l-run-flow-3*:

$\llbracket (c, s) \rightarrow^*\{cfs\}\ (c', s') \implies s' = run_flow\ (flow\ cfs)\ s;$

$(c, s) \rightarrow^*\{cfs\ @\ [(c', s')]\}\ (c'', s'') \implies$

$s'' = run_flow\ (flow\ (cfs\ @\ [(c', s')]))\ s$

by (*simp add: flow-append run-flow-append,*

auto intro: small-steps-l-run-flow-2 simp: flow-def)

lemma *small-steps-l-run-flow*:

$(c, s) \rightarrow^*\{cfs\}\ (c', s') \implies s' = run_flow\ (flow\ cfs)\ s$

by (*induction c s cfs c' s' rule: small-steps-l-induct,*
erule small-steps-l-run-flow-1, rule small-steps-l-run-flow-3)

4.2 Local context proofs

context *noninterf*

begin

lemma *no-upd-sources*:

$no_upd\ cs\ x \implies x \in sources\ cs\ s\ x$

by (*induction cs rule: rev-induct, auto simp: no-upd-append*
split: com-flow.split)

lemma *sources-aux-sources*:

$sources_aux\ cs\ s\ x \subseteq sources\ cs\ s\ x$

by (*induction cs rule: rev-induct, auto split: com-flow.split*)

lemma *sources-aux-append*:

$sources_aux\ cs\ s\ x \subseteq sources_aux\ (cs\ @\ cs')\ s\ x$

by (*induction cs' rule: rev-induct, simp, subst append-assoc [symmetric],*
auto simp del: append-assoc split: com-flow.split)

lemma *sources-aux-observe-hd-1*:

$\forall y \in X. s: \text{dom } y \rightsquigarrow \text{dom } x \implies X \subseteq \text{sources-aux } [\langle X \rangle] s x$
by (*subst append-Nil* [*symmetric*], *subst sources-aux.simps*, *auto*)

lemma *sources-aux-observe-hd-2*:

$(\forall y \in X. s: \text{dom } y \rightsquigarrow \text{dom } x \implies X \subseteq \text{sources-aux } (\langle X \rangle \# xs) s x) \implies$
 $\forall y \in X. s: \text{dom } y \rightsquigarrow \text{dom } x \implies X \subseteq \text{sources-aux } (\langle X \rangle \# xs @ [x']) s x$
by (*subst append-Cons* [*symmetric*], *subst sources-aux.simps*,
auto split: com-flow.split)

lemma *sources-aux-observe-hd*:

$\forall y \in X. s: \text{dom } y \rightsquigarrow \text{dom } x \implies X \subseteq \text{sources-aux } (\langle X \rangle \# cs) s x$
by (*induction cs rule: rev-induct*,
erule sources-aux-observe-hd-1, *rule sources-aux-observe-hd-2*)

lemma *sources-observe-tl-1*:

assumes

A: $\bigwedge z a. c = (x ::= a :: \text{com-flow}) \implies z = x \implies$
 $\text{sources-aux } cs s x \subseteq \text{sources-aux } (\langle X \rangle \# cs) s x$ **and**
B: $\bigwedge z a y. c = (x ::= a :: \text{com-flow}) \implies z = x \implies$
 $\text{sources } cs s y \subseteq \text{sources } (\langle X \rangle \# cs) s y$ **and**
C: $\bigwedge z a. c = (z ::= a :: \text{com-flow}) \implies z \neq x \implies$
 $\text{sources } cs s x \subseteq \text{sources } (\langle X \rangle \# cs) s x$ **and**
D: $\bigwedge Y y. c = \langle Y \rangle \implies$
 $\text{sources } cs s y \subseteq \text{sources } (\langle X \rangle \# cs) s y$ **and**
E: $z \in (\text{case } c \text{ of}$
 $z ::= a \Rightarrow \text{if } z = x$
 $\text{then sources-aux } cs s x \cup \bigcup \{\text{sources } cs s y \mid y.$
 $\text{run-flow } cs s: \text{dom } y \rightsquigarrow \text{dom } x \wedge y \in \text{avars } a\}$
 $\text{else sources } cs s x \mid$
 $\langle X \rangle \Rightarrow$
 $\text{sources } cs s x \cup \bigcup \{\text{sources } cs s y \mid y.$
 $\text{run-flow } cs s: \text{dom } y \rightsquigarrow \text{dom } x \wedge y \in X\})$

shows $z \in \text{sources } (\langle X \rangle \# cs @ [c]) s x$

proof –

{

fix *a*

assume

F: $\forall A. (\forall y. \text{run-flow } cs s: \text{dom } y \rightsquigarrow \text{dom } x \longrightarrow$
 $A = \text{sources } (\langle X \rangle \# cs) s y \longrightarrow y \notin \text{avars } a) \vee z \notin A$ **and**
G: $c = x ::= a$

have $z \in \text{sources-aux } cs s x \cup \bigcup \{\text{sources } cs s y \mid y.$
 $\text{run-flow } cs s: \text{dom } y \rightsquigarrow \text{dom } x \wedge y \in \text{avars } a\}$

using *E* **and** *G* **by** *simp*

hence $z \in \text{sources-aux } (\langle X \rangle \# cs) s x$

using *A* **and** *G* **proof** (*erule-tac UnE*, *blast*)

assume $z \in \bigcup \{\text{sources } cs s y \mid y.$

```

    run-flow cs s: dom y  $\rightsquigarrow$  dom x  $\wedge$  y  $\in$  avars a}
  then obtain y where
    H: z  $\in$  sources cs s y and
    I: run-flow cs s: dom y  $\rightsquigarrow$  dom x and
    J: y  $\in$  avars a
    by blast
  have z  $\in$  sources ( $\langle X \rangle \#$  cs) s y
    using B and G and H by blast
  hence y  $\notin$  avars a
    using F and I by blast
  thus ?thesis
    using J by contradiction
qed
}
moreover {
  fix y a
  assume c = y ::= a and y  $\neq$  x
  moreover from this have z  $\in$  sources cs s x
    using E by simp
  ultimately have z  $\in$  sources ( $\langle X \rangle \#$  cs) s x
    using C by blast
}
moreover {
  fix Y
  assume
    F:  $\forall A. (\forall y. \text{run-flow cs s: dom y} \rightsquigarrow \text{dom x} \longrightarrow$ 
      A = sources ( $\langle X \rangle \#$  cs) s y  $\longrightarrow$  y  $\notin$  Y)  $\vee$  z  $\notin$  A and
    G: c =  $\langle Y \rangle$ 
  have z  $\in$  sources cs s x  $\cup \bigcup \{ \text{sources cs s y} \mid y. \text{run-flow cs s: dom y} \rightsquigarrow \text{dom x} \wedge y \in Y \}$ 
    using E and G by simp
  hence z  $\in$  sources ( $\langle X \rangle \#$  cs) s x
  using D and G proof (erule-tac UnE, blast)
  assume z  $\in \bigcup \{ \text{sources cs s y} \mid y. \text{run-flow cs s: dom y} \rightsquigarrow \text{dom x} \wedge y \in Y \}$ 
  then obtain y where
    H: z  $\in$  sources cs s y and
    I: run-flow cs s: dom y  $\rightsquigarrow$  dom x and
    J: y  $\in$  Y
    by blast
  have z  $\in$  sources ( $\langle X \rangle \#$  cs) s y
    using D and G and H by blast
  hence y  $\notin$  Y
    using F and I by blast
  thus ?thesis
    using J by contradiction
qed
}
ultimately show ?thesis

```

by (*simp only: append-Cons [symmetric] sources.simps,*
auto split: com-flow.split)
qed

lemma *sources-observe-tl-2:*

assumes

$A: \bigwedge z a. c = (z ::= a :: \text{com-flow}) \implies$
 $\text{sources-aux } cs \ s \ x \subseteq \text{sources-aux } (\langle X \rangle \# cs) \ s \ x$ **and**

$B: \bigwedge Y. c = \langle Y \rangle \implies$
 $\text{sources-aux } cs \ s \ x \subseteq \text{sources-aux } (\langle X \rangle \# cs) \ s \ x$ **and**

$C: \bigwedge Y y. c = \langle Y \rangle \implies$
 $\text{sources } cs \ s \ y \subseteq \text{sources } (\langle X \rangle \# cs) \ s \ y$ **and**

$D: z \in (\text{case } c \text{ of}$
 $z ::= a \Rightarrow$
 $\text{sources-aux } cs \ s \ x \mid$
 $\langle X \rangle \Rightarrow$
 $\text{sources-aux } cs \ s \ x \cup \bigcup \{ \text{sources } cs \ s \ y \mid y.$
 $\text{run-flow } cs \ s: \text{dom } y \rightsquigarrow \text{dom } x \wedge y \in X \})$

shows $z \in \text{sources-aux } (\langle X \rangle \# cs @ [c]) \ s \ x$

proof –

{
 fix $y \ a$
 assume $c = y ::= a$
 moreover from this have $z \in \text{sources-aux } cs \ s \ x$
 using D **by** *simp*
 ultimately have $z \in \text{sources-aux } (\langle X \rangle \# cs) \ s \ x$
 using A **by** *blast*
}
moreover {
 fix Y
 assume
 $E: \forall A. (\forall y. \text{run-flow } cs \ s: \text{dom } y \rightsquigarrow \text{dom } x \longrightarrow$
 $A = \text{sources } (\langle X \rangle \# cs) \ s \ y \longrightarrow y \notin Y) \vee z \notin A$ **and**
 $F: c = \langle Y \rangle$
 have $z \in \text{sources-aux } cs \ s \ x \cup \bigcup \{ \text{sources } cs \ s \ y \mid y.$
 $\text{run-flow } cs \ s: \text{dom } y \rightsquigarrow \text{dom } x \wedge y \in Y \}$
 using D **and** F **by** *simp*
 hence $z \in \text{sources-aux } (\langle X \rangle \# cs) \ s \ x$
 using B **and** F **proof** (*erule-tac UnE, blast*)
 assume $z \in \bigcup \{ \text{sources } cs \ s \ y \mid y.$
 $\text{run-flow } cs \ s: \text{dom } y \rightsquigarrow \text{dom } x \wedge y \in Y \}$
 then obtain y **where**
 $H: z \in \text{sources } cs \ s \ y$ **and**
 $I: \text{run-flow } cs \ s: \text{dom } y \rightsquigarrow \text{dom } x$ **and**
 $J: y \in Y$
 by *blast*
 have $z \in \text{sources } (\langle X \rangle \# cs) \ s \ y$
 using C **and** F **and** H **by** *blast*
 hence $y \notin Y$

```

    using E and I by blast
  thus ?thesis
    using J by contradiction
qed
}
ultimately show ?thesis
  by (simp only: append-Cons [symmetric] sources-aux.simps,
      auto split: com-flow.split)
qed

```

```

lemma sources-observe-tl:
  sources cs s x  $\subseteq$  sources ( $\langle X \rangle \# cs$ ) s x
and sources-aux-observe-tl:
  sources-aux cs s x  $\subseteq$  sources-aux ( $\langle X \rangle \# cs$ ) s x
proof (induction cs s x and cs s x rule: sources-induct)
  fix cs c s x
  show
     $\llbracket \bigwedge z a. c = z ::= a \implies z = x \implies$ 
      sources-aux cs s x  $\subseteq$  sources-aux ( $\langle X \rangle \# cs$ ) s x;
     $\bigwedge z a b y. c = z ::= a \implies z = x \implies$ 
      sources cs s y  $\subseteq$  sources ( $\langle X \rangle \# cs$ ) s y;
     $\bigwedge z a. c = z ::= a \implies z \neq x \implies$ 
      sources cs s x  $\subseteq$  sources ( $\langle X \rangle \# cs$ ) s x;
     $\bigwedge Y. c = \langle Y \rangle \implies$ 
      sources cs s x  $\subseteq$  sources ( $\langle X \rangle \# cs$ ) s x;
     $\bigwedge Y a y. c = \langle Y \rangle \implies$ 
      sources cs s y  $\subseteq$  sources ( $\langle X \rangle \# cs$ ) s y  $\rrbracket \implies$ 
      sources (cs @ [c]) s x  $\subseteq$  sources ( $\langle X \rangle \# cs @ [c]$ ) s x
    by (auto, rule sources-observe-tl-1)
  next
    fix s x
    show sources [] s x  $\subseteq$  sources [ $\langle X \rangle$ ] s x
      by (subst (3) append-Nil [symmetric],
          simp only: sources.simps, simp)
  next
    fix cs c s x
    show
       $\llbracket \bigwedge z a. c = z ::= a \implies$ 
        sources-aux cs s x  $\subseteq$  sources-aux ( $\langle X \rangle \# cs$ ) s x;
       $\bigwedge Y. c = \langle Y \rangle \implies$ 
        sources-aux cs s x  $\subseteq$  sources-aux ( $\langle X \rangle \# cs$ ) s x;
       $\bigwedge Y a y. c = \langle Y \rangle \implies$ 
        sources cs s y  $\subseteq$  sources ( $\langle X \rangle \# cs$ ) s y  $\rrbracket \implies$ 
        sources-aux (cs @ [c]) s x  $\subseteq$  sources-aux ( $\langle X \rangle \# cs @ [c]$ ) s x
      by (auto, rule sources-observe-tl-2)
    qed simp
qed simp

```

```

lemma sources-member-1:

```

assumes

A: $\bigwedge z a. c = (x ::= a :: \text{com-flow}) \implies z = x \implies$
 $y \in \text{sources-aux } cs' (\text{run-flow } cs \ s) \ x \implies$
 $\text{sources } cs \ s \ y \subseteq \text{sources-aux } (cs @ cs') \ s \ x$ **and**
B: $\bigwedge z a w. c = (x ::= a :: \text{com-flow}) \implies z = x \implies$
 $y \in \text{sources } cs' (\text{run-flow } cs \ s) \ w \implies$
 $\text{sources } cs \ s \ y \subseteq \text{sources } (cs @ cs') \ s \ w$ **and**
C: $\bigwedge z a. c = (z ::= a :: \text{com-flow}) \implies z \neq x \implies$
 $y \in \text{sources } cs' (\text{run-flow } cs \ s) \ x \implies$
 $\text{sources } cs \ s \ y \subseteq \text{sources } (cs @ cs') \ s \ x$ **and**
D: $\bigwedge Y w. c = \langle Y \rangle \implies$
 $y \in \text{sources } cs' (\text{run-flow } cs \ s) \ w \implies$
 $\text{sources } cs \ s \ y \subseteq \text{sources } (cs @ cs') \ s \ w$ **and**
E: $y \in (\text{case } c \text{ of}$
 $z ::= a \Rightarrow \text{if } z = x$
 $\text{then sources-aux } cs' (\text{run-flow } cs \ s) \ x \cup$
 $\bigcup \{ \text{sources } cs' (\text{run-flow } cs \ s) \ y \mid y.$
 $\text{run-flow } cs' (\text{run-flow } cs \ s): \text{dom } y \rightsquigarrow \text{dom } x \wedge y \in \text{avars } a \}$
 $\text{else sources } cs' (\text{run-flow } cs \ s) \ x \mid$
 $\langle X \rangle \Rightarrow$
 $\text{sources } cs' (\text{run-flow } cs \ s) \ x \cup$
 $\bigcup \{ \text{sources } cs' (\text{run-flow } cs \ s) \ y \mid y.$
 $\text{run-flow } cs' (\text{run-flow } cs \ s): \text{dom } y \rightsquigarrow \text{dom } x \wedge y \in X \})$ **and**
F: $z \in \text{sources } cs \ s \ y$

shows $z \in \text{sources } (cs @ cs' @ [c]) \ s \ x$

proof –

{
fix a
assume
G: $\forall A. (\forall y. \text{run-flow } cs' (\text{run-flow } cs \ s): \text{dom } y \rightsquigarrow \text{dom } x \longrightarrow$
 $A = \text{sources } (cs @ cs') \ s \ y \longrightarrow y \notin \text{avars } a) \vee z \notin A$ **and**
H: $c = x ::= a$
have $y \in \text{sources-aux } cs' (\text{run-flow } cs \ s) \ x \cup$
 $\bigcup \{ \text{sources } cs' (\text{run-flow } cs \ s) \ y \mid y.$
 $\text{run-flow } cs' (\text{run-flow } cs \ s): \text{dom } y \rightsquigarrow \text{dom } x \wedge y \in \text{avars } a \}$
using E **and** H **by** *simp*
hence $z \in \text{sources-aux } (cs @ cs') \ s \ x$
using A **and** F **and** H **proof** (*erule-tac UnE, blast*)
assume $y \in \bigcup \{ \text{sources } cs' (\text{run-flow } cs \ s) \ y \mid y.$
 $\text{run-flow } cs' (\text{run-flow } cs \ s): \text{dom } y \rightsquigarrow \text{dom } x \wedge y \in \text{avars } a \}$
then obtain w **where**
I: $y \in \text{sources } cs' (\text{run-flow } cs \ s) \ w$ **and**
J: $\text{run-flow } cs' (\text{run-flow } cs \ s): \text{dom } w \rightsquigarrow \text{dom } x$ **and**
K: $w \in \text{avars } a$
by *blast*
have $z \in \text{sources } (cs @ cs') \ s \ w$
using B **and** F **and** H **and** I **by** *blast*
hence $w \notin \text{avars } a$
using G **and** J **by** *blast*

```

    thus ?thesis
    using K by contradiction
  qed
}
moreover {
  fix w a
  assume c = w ::= a and w ≠ x
  moreover from this have y ∈ sources cs' (run-flow cs s) x
    using E by simp
  ultimately have z ∈ sources (cs @ cs') s x
    using C and F by blast
}
moreover {
  fix Y
  assume
    G: ∀ A. (∀ y. run-flow cs' (run-flow cs s): dom y ∼ dom x ⟶
      A = sources (cs @ cs') s y ⟶ y ∉ Y) ∨ z ∉ A and
    H: c = ⟨Y⟩
  have y ∈ sources cs' (run-flow cs s) x ∪
    ∪ {sources cs' (run-flow cs s) y | y.
      run-flow cs' (run-flow cs s): dom y ∼ dom x ∧ y ∈ Y}
    using E and H by simp
  hence z ∈ sources (cs @ cs') s x
  using D and F and H proof (erule-tac UnE, blast)
    assume y ∈ ∪ {sources cs' (run-flow cs s) y | y.
      run-flow cs' (run-flow cs s): dom y ∼ dom x ∧ y ∈ Y}
    then obtain w where
      I: y ∈ sources cs' (run-flow cs s) w and
      J: run-flow cs' (run-flow cs s): dom w ∼ dom x and
      K: w ∈ Y
    by blast
    have z ∈ sources (cs @ cs') s w
      using D and F and H and I by blast
    hence w ∉ Y
      using G and J by blast
    thus ?thesis
      using K by contradiction
  qed
}
ultimately show ?thesis
  by (simp only: append-assoc [symmetric] sources.simps,
    auto simp: run-flow-append split: com-flow.split)
qed

```

lemma *sources-member-2*:

assumes

$A: \bigwedge z a. c = (z ::= a :: \text{com-flow}) \implies$
 $y \in \text{sources-aux } cs' (\text{run-flow } cs \ s) \ x \implies$
 $\text{sources } cs \ s \ y \subseteq \text{sources-aux } (cs @ cs') \ s \ x$ **and**

$B: \bigwedge Y. c = \langle Y \rangle \implies$
 $y \in \text{sources-aux } cs' (\text{run-flow } cs \ s) \ x \implies$
 $\text{sources } cs \ s \ y \subseteq \text{sources-aux } (cs \ @ \ cs') \ s \ x \text{ and}$
 $C: \bigwedge Y \ w. c = \langle Y \rangle \implies$
 $y \in \text{sources } cs' (\text{run-flow } cs \ s) \ w \implies$
 $\text{sources } cs \ s \ y \subseteq \text{sources } (cs \ @ \ cs') \ s \ w \text{ and}$
 $D: y \in (\text{case } c \text{ of}$
 $z ::= a \implies$
 $\text{sources-aux } cs' (\text{run-flow } cs \ s) \ x \mid$
 $\langle X \rangle \implies$
 $\text{sources-aux } cs' (\text{run-flow } cs \ s) \ x \cup$
 $\bigcup \{ \text{sources } cs' (\text{run-flow } cs \ s) \ y \mid y.$
 $\text{run-flow } cs' (\text{run-flow } cs \ s): \text{dom } y \rightsquigarrow \text{dom } x \wedge y \in X \} \text{ and}$
 $E: z \in \text{sources } cs \ s \ y$
shows $z \in \text{sources-aux } (cs \ @ \ cs' \ @ \ [c]) \ s \ x$
proof –
 $\{$
 $\text{fix } w \ a$
 $\text{assume } c = w ::= a$
 $\text{moreover from this have } y \in \text{sources-aux } cs' (\text{run-flow } cs \ s) \ x$
 $\text{using } D \text{ by simp}$
 $\text{ultimately have } z \in \text{sources-aux } (cs \ @ \ cs') \ s \ x$
 $\text{using } A \text{ and } E \text{ by blast}$
 $\}$
moreover $\{$
 $\text{fix } Y$
 assume
 $G: \forall A. (\forall y. \text{run-flow } cs' (\text{run-flow } cs \ s): \text{dom } y \rightsquigarrow \text{dom } x \longrightarrow$
 $A = \text{sources } (cs \ @ \ cs') \ s \ y \longrightarrow y \notin Y) \vee z \notin A \text{ and}$
 $H: c = \langle Y \rangle$
 $\text{have } y \in \text{sources-aux } cs' (\text{run-flow } cs \ s) \ x \cup$
 $\bigcup \{ \text{sources } cs' (\text{run-flow } cs \ s) \ y \mid y.$
 $\text{run-flow } cs' (\text{run-flow } cs \ s): \text{dom } y \rightsquigarrow \text{dom } x \wedge y \in Y \}$
 $\text{using } D \text{ and } H \text{ by simp}$
 $\text{hence } z \in \text{sources-aux } (cs \ @ \ cs') \ s \ x$
 $\text{using } B \text{ and } E \text{ and } H \text{ proof (erule-tac UnE, blast)}$
 $\text{assume } y \in \bigcup \{ \text{sources } cs' (\text{run-flow } cs \ s) \ y \mid y.$
 $\text{run-flow } cs' (\text{run-flow } cs \ s): \text{dom } y \rightsquigarrow \text{dom } x \wedge y \in Y \}$
 $\text{then obtain } w \text{ where}$
 $I: y \in \text{sources } cs' (\text{run-flow } cs \ s) \ w \text{ and}$
 $J: \text{run-flow } cs' (\text{run-flow } cs \ s): \text{dom } w \rightsquigarrow \text{dom } x \text{ and}$
 $K: w \in Y$
 by blast
 $\text{have } z \in \text{sources } (cs \ @ \ cs') \ s \ w$
 $\text{using } C \text{ and } E \text{ and } H \text{ and } I \text{ by blast}$
 $\text{hence } w \notin Y$
 $\text{using } G \text{ and } J \text{ by blast}$
 thus ?thesis
 $\text{using } K \text{ by contradiction}$

qed
 }
 ultimately show ?thesis
 by (simp only: append-assoc [symmetric] sources-aux.simps,
 auto simp: run-flow-append split: com-flow.split)
 qed

lemma sources-member:

$y \in \text{sources } cs' (\text{run-flow } cs \ s) \ x \implies$
 $\text{sources } cs \ s \ y \subseteq \text{sources } (cs \ @ \ cs') \ s \ x$

and sources-aux-member:

$y \in \text{sources-aux } cs' (\text{run-flow } cs \ s) \ x \implies$
 $\text{sources } cs \ s \ y \subseteq \text{sources-aux } (cs \ @ \ cs') \ s \ x$

proof (induction $cs' \ s \ x$ **and** $cs' \ s \ x$ rule: sources-induct)

fix $cs' \ c \ s \ x$

show

$\llbracket \bigwedge z \ a. \ c = z ::= a \implies z = x \implies$
 $y \in \text{sources-aux } cs' (\text{run-flow } cs \ s) \ x \implies$
 $\text{sources } cs \ s \ y \subseteq \text{sources-aux } (cs \ @ \ cs') \ s \ x;$
 $\bigwedge z \ a \ b \ w. \ c = z ::= a \implies z = x \implies$
 $y \in \text{sources } cs' (\text{run-flow } cs \ s) \ w \implies$
 $\text{sources } cs \ s \ y \subseteq \text{sources } (cs \ @ \ cs') \ s \ w;$
 $\bigwedge z \ a. \ c = z ::= a \implies z \neq x \implies$
 $y \in \text{sources } cs' (\text{run-flow } cs \ s) \ x \implies$
 $\text{sources } cs \ s \ y \subseteq \text{sources } (cs \ @ \ cs') \ s \ x;$
 $\bigwedge Y. \ c = \langle Y \rangle \implies$
 $y \in \text{sources } cs' (\text{run-flow } cs \ s) \ x \implies$
 $\text{sources } cs \ s \ y \subseteq \text{sources } (cs \ @ \ cs') \ s \ x;$
 $\bigwedge Y \ a \ w. \ c = \langle Y \rangle \implies$
 $y \in \text{sources } cs' (\text{run-flow } cs \ s) \ w \implies$
 $\text{sources } cs \ s \ y \subseteq \text{sources } (cs \ @ \ cs') \ s \ w;$
 $y \in \text{sources } (cs' \ @ \ [c]) (\text{run-flow } cs \ s) \ x \implies$
 $\text{sources } cs \ s \ y \subseteq \text{sources } (cs \ @ \ cs' \ @ \ [c]) \ s \ x$
by (auto, rule sources-member-1)

next

fix $cs' \ c \ s \ x$

show

$\llbracket \bigwedge z \ a. \ c = z ::= a \implies$
 $y \in \text{sources-aux } cs' (\text{run-flow } cs \ s) \ x \implies$
 $\text{sources } cs \ s \ y \subseteq \text{sources-aux } (cs \ @ \ cs') \ s \ x;$
 $\bigwedge Y. \ c = \langle Y \rangle \implies$
 $y \in \text{sources-aux } cs' (\text{run-flow } cs \ s) \ x \implies$
 $\text{sources } cs \ s \ y \subseteq \text{sources-aux } (cs \ @ \ cs') \ s \ x;$
 $\bigwedge Y \ a \ w. \ c = \langle Y \rangle \implies$
 $y \in \text{sources } cs' (\text{run-flow } cs \ s) \ w \implies$
 $\text{sources } cs \ s \ y \subseteq \text{sources } (cs \ @ \ cs') \ s \ w;$
 $y \in \text{sources-aux } (cs' \ @ \ [c]) (\text{run-flow } cs \ s) \ x \implies$
 $\text{sources } cs \ s \ y \subseteq \text{sources-aux } (cs \ @ \ cs' \ @ \ [c]) \ s \ x$
by (auto, rule sources-member-2)

qed *simp-all*

lemma *ctyping2-confine*:

$\llbracket (c, s) \Rightarrow s'; (U, v) \models c (\subseteq A, X) = \text{Some } (B, Y);$
 $\exists (C, Z) \in U. \neg C: \text{dom } 'Z \rightsquigarrow \{\text{dom } x\} \rrbracket \Longrightarrow s' x = s x$
by (*induction arbitrary: A B X Y U v rule: big-step-induct,*
auto split: if-split-asm option.split-asm prod.split-asm, fastforce+)

lemma *ctyping2-term-if*:

$\llbracket \bigwedge x' y' z'' s. x' = x \Longrightarrow y' = y \Longrightarrow z = z'' \Longrightarrow \exists s'. (c_1, s) \Rightarrow s';$
 $\bigwedge x' y' z'' s. x' = x \Longrightarrow y' = y \Longrightarrow z' = z'' \Longrightarrow \exists s'. (c_2, s) \Rightarrow s'' \rrbracket \Longrightarrow$
 $\exists s'. (\text{IF } b \text{ THEN } c_1 \text{ ELSE } c_2, s) \Rightarrow s'$
by (*cases bval b s, fastforce+*)

lemma *ctyping2-term*:

$\llbracket (U, v) \models c (\subseteq A, X) = \text{Some } (B, Y);$
 $\exists (C, Z) \in U. \neg C: \text{dom } 'Z \rightsquigarrow \text{UNIV} \rrbracket \Longrightarrow \exists s'. (c, s) \Rightarrow s'$
by (*induction (U, v) c A X arbitrary: B Y U v s rule: ctyping2.induct,*
auto split: if-split-asm option.split-asm prod.split-asm, fastforce,
erule ctyping2-term-if)

lemma *ctyping2-correct-aux-skip* [elim]:

$\llbracket (\text{SKIP}, s) \rightarrow^* \{cfs_1\} (c_1, s_1); (c_1, s_1) \rightarrow^* \{cfs_2\} (c_2, s_2) \rrbracket \Longrightarrow$
 $(\forall t_1. \exists c_2' t_2. \forall x.$
 $(s_1 = t_1 (\subseteq \text{sources-aux } (\text{flow } cfs_2) s_1 x) \longrightarrow$
 $(c_1, t_1) \rightarrow^* (c_2', t_2) \wedge (c_2 = \text{SKIP}) = (c_2' = \text{SKIP})) \wedge$
 $(s_1 = t_1 (\subseteq \text{sources } (\text{flow } cfs_2) s_1 x) \longrightarrow s_2 x = t_2 x)) \wedge$
 $(\forall x. (\exists p \in U. \text{case } p \text{ of } (B, W) \Rightarrow$
 $\exists s \in B. \exists y \in W. \neg s: \text{dom } y \rightsquigarrow \text{dom } x) \longrightarrow \text{no-upd } (\text{flow } cfs_2) x)$
by (*fastforce dest: small-steps-skip*)

lemma *ctyping2-correct-aux-assign* [elim]:

assumes

A: (if ($\forall s \in \text{Univ? } A X. \forall y \in \text{avars } a. s: \text{dom } y \rightsquigarrow \text{dom } x$) \wedge
 $(\forall p \in U. \forall B Y. p = (B, Y) \longrightarrow$
 $(\forall s \in B. \forall y \in Y. s: \text{dom } y \rightsquigarrow \text{dom } x))$
then $\text{Some } (\text{if } x \in \text{state} \wedge A \neq \{\})$
then $\text{if } v \models a (\subseteq X)$
then $(\{s(x := \text{aval } a s) \mid s. s \in A\}, \text{insert } x X)$
else $(A, X - \{x\})$
else $(A, \text{Univ?? } A X)$
else $\text{None}) = \text{Some } (B, Y)$
(is ($\text{if } ?P \text{ then } - \text{ else } -$) $= -$) **and**
B: (x ::= a, s) → {cfs₁} (c₁, s₁) and*
C: (c₁, s₁) → {cfs₂} (c₂, s₂) and*
D: r ∈ A and
E: s = r (⊆ state ∩ X)

shows

$(\forall t_1. \exists c_2' t_2. \forall x.$
 $(s_1 = t_1 (\subseteq \text{sources-aux } (\text{flow } cfs_2) s_1 x) \longrightarrow$
 $(c_1, t_1) \rightarrow^* (c_2', t_2) \wedge (c_2 = \text{SKIP}) = (c_2' = \text{SKIP})) \wedge$
 $(s_1 = t_1 (\subseteq \text{sources } (\text{flow } cfs_2) s_1 x) \longrightarrow s_2 x = t_2 x)) \wedge$
 $(\forall x. (\exists p \in U. \text{case } p \text{ of } (B, Y) \Rightarrow$
 $\exists s \in B. \exists y \in Y. \neg s: \text{dom } y \rightsquigarrow \text{dom } x) \longrightarrow \text{no-upd } (\text{flow } cfs_2) x)$

proof –

have $?P$

using A **by** (*simp split: if-split-asm*)

have $F: \text{avars } a \subseteq \{y. s: \text{dom } y \rightsquigarrow \text{dom } x\}$

proof (*cases state* $\subseteq X$)

case *True*

with E **have** $\text{interf } s = \text{interf } r$

by (*blast intro: interf-state*)

with D **and** $\langle ?P \rangle$ **show** $?thesis$

by (*erule-tac conjE, drule-tac bspec, auto simp: univ-states-if-def*)

next

case *False*

with D **and** $\langle ?P \rangle$ **show** $?thesis$

by (*erule-tac conjE, drule-tac bspec, auto simp: univ-states-if-def*)

qed

have $(c_1, s_1) = (x ::= a, s) \vee (c_1, s_1) = (\text{SKIP}, s(x := \text{aval } a \ s))$

using B **by** (*blast dest: small-stepsl-assign*)

thus $?thesis$

proof

assume $(c_1, s_1) = (x ::= a, s)$

moreover from *this* **have** $(x ::= a, s) \rightarrow^* \{cfs_2\} (c_2, s_2)$

using C **by** *simp*

hence $(c_2, s_2) = (x ::= a, s) \wedge \text{flow } cfs_2 = [] \vee$

$(c_2, s_2) = (\text{SKIP}, s(x := \text{aval } a \ s)) \wedge \text{flow } cfs_2 = [x ::= a]$

by (*rule small-stepsl-assign*)

moreover {

fix t

have $\exists c' t'. \forall y.$

$(y = x \longrightarrow$

$(s = t (\subseteq \text{sources-aux } [x ::= a] s x) \longrightarrow$

$(x ::= a, t) \rightarrow^* (c', t') \wedge c' = \text{SKIP}) \wedge$

$(s = t (\subseteq \text{sources } [x ::= a] s x) \longrightarrow \text{aval } a \ s = t' x)) \wedge$

$(y \neq x \longrightarrow$

$(s = t (\subseteq \text{sources-aux } [x ::= a] s y) \longrightarrow$

$(x ::= a, t) \rightarrow^* (c', t') \wedge c' = \text{SKIP}) \wedge$

$(s = t (\subseteq \text{sources } [x ::= a] s y) \longrightarrow s y = t' y))$

proof (*rule exI [of - SKIP], rule exI [of - t(x := aval a t)]*)

{

assume $s = t (\subseteq \text{sources } [x ::= a] s x)$

hence $s = t (\subseteq \{y. s: \text{dom } y \rightsquigarrow \text{dom } x \wedge y \in \text{avars } a\})$

by (*subst (asm) append-Nil [symmetric],*

simp only: sources.simps, auto)

```

    hence  $aval\ a\ s = aval\ a\ t$ 
    using  $F$  by (blast intro: avars-aval)
  }
  moreover {
    fix  $y$ 
    assume  $s = t$  ( $\subseteq sources\ [x ::= a]\ s\ y$ ) and  $y \neq x$ 
    hence  $s\ y = t\ y$ 
    by (subst (asm) append-Nil [symmetric],
        simp only: sources.simps, auto)
  }
  ultimately show  $\forall y.$ 
    ( $y = x \longrightarrow$ 
      ( $s = t$  ( $\subseteq sources\ aux\ [x ::= a]\ s\ x$ )  $\longrightarrow$ 
        ( $x ::= a, t$ )  $\rightarrow^*$  ( $SKIP, t(x := aval\ a\ t)$ )  $\wedge SKIP = SKIP$ )  $\wedge$ 
        ( $s = t$  ( $\subseteq sources\ [x ::= a]\ s\ x$ )  $\longrightarrow$ 
           $aval\ a\ s = (t(x := aval\ a\ t))\ x$ )  $\wedge$ 
        ( $y \neq x \longrightarrow$ 
          ( $s = t$  ( $\subseteq sources\ aux\ [x ::= a]\ s\ y$ )  $\longrightarrow$ 
            ( $x ::= a, t$ )  $\rightarrow^*$  ( $SKIP, t(x := aval\ a\ t)$ )  $\wedge SKIP = SKIP$ )  $\wedge$ 
            ( $s = t$  ( $\subseteq sources\ [x ::= a]\ s\ y$ )  $\longrightarrow$ 
               $s\ y = (t(x := aval\ a\ t))\ y$ )
          )
        )
      by simp
    )
  qed
}
ultimately show ?thesis
using <?P> by fastforce
next
  assume  $(c_1, s_1) = (SKIP, s(x := aval\ a\ s))$ 
  moreover from this have  $(SKIP, s(x := aval\ a\ s)) \rightarrow^*\{cfs_2\} (c_2, s_2)$ 
  using  $C$  by simp
  hence  $(c_2, s_2) = (SKIP, s(x := aval\ a\ s)) \wedge flow\ cfs_2 = []$ 
  by (rule small-steps-skip)
  ultimately show ?thesis
  by auto
qed
qed

lemma ctying2-correct-aux-seq:
  assumes
     $A: \bigwedge B' s\ c'\ c'' s_1\ s_2\ cfs_1\ cfs_2. B = B' \implies$ 
     $\exists r \in A. s = r (\subseteq state \cap X) \implies$ 
     $(c_1, s) \rightarrow^*\{cfs_1\} (c', s_1) \implies (c', s_1) \rightarrow^*\{cfs_2\} (c'', s_2) \implies$ 
     $(\forall t_1. \exists c_2' t_2. \forall x.$ 
       $(s_1 = t_1 (\subseteq sources\ aux\ (flow\ cfs_2)\ s_1\ x) \longrightarrow$ 
         $(c', t_1) \rightarrow^* (c_2', t_2) \wedge (c'' = SKIP) = (c_2' = SKIP)) \wedge$ 
         $(s_1 = t_1 (\subseteq sources\ (flow\ cfs_2)\ s_1\ x) \longrightarrow s_2\ x = t_2\ x)) \wedge$ 
       $(\forall x. (\exists p \in U. case\ p\ of\ (B, W) \implies$ 
         $\exists s \in B. \exists y \in W. \neg s: dom\ y \rightsquigarrow dom\ x) \longrightarrow$ 
         $no\ upd\ (flow\ cfs_2)\ x) \wedge$ 

```

$B: \bigwedge B' B'' C Z s c' c'' s_1 s_2 cfs_1 cfs_2. B = B' \implies B'' = B' \implies$
 $(U, v) \models c_2 (\subseteq B', Y) = \text{Some } (C, Z) \implies$
 $\exists r \in B'. s = r (\subseteq \text{state} \cap Y) \implies$
 $(c_2, s) \rightarrow^* \{cfs_1\} (c', s_1) \implies (c', s_1) \rightarrow^* \{cfs_2\} (c'', s_2) \implies$
 $(\forall t_1. \exists c_2' t_2. \forall x.$
 $(s_1 = t_1 (\subseteq \text{sources-aux } (\text{flow } cfs_2) s_1 x) \longrightarrow$
 $(c', t_1) \rightarrow^* (c_2', t_2) \wedge (c'' = \text{SKIP}) = (c_2' = \text{SKIP})) \wedge$
 $(s_1 = t_1 (\subseteq \text{sources } (\text{flow } cfs_2) s_1 x) \longrightarrow s_2 x = t_2 x)) \wedge$
 $(\forall x. (\exists p \in U. \text{case } p \text{ of } (B, W) \Rightarrow$
 $\exists s \in B. \exists y \in W. \neg s: \text{dom } y \rightsquigarrow \text{dom } x) \longrightarrow$
 $\text{no-upd } (\text{flow } cfs_2) x) \text{ and}$
 $C: (U, v) \models c_1 (\subseteq A, X) = \text{Some } (B, Y) \text{ and}$
 $D: (U, v) \models c_2 (\subseteq B, Y) = \text{Some } (C, Z) \text{ and}$
 $E: (c_1;; c_2, s) \rightarrow^* \{cfs_1\} (c', s_1) \text{ and}$
 $F: (c', s_1) \rightarrow^* \{cfs_2\} (c'', s_2) \text{ and}$
 $G: r \in A \text{ and}$
 $H: s = r (\subseteq \text{state} \cap X)$

shows

$(\forall t_1. \exists c_2' t_2. \forall x.$
 $(s_1 = t_1 (\subseteq \text{sources-aux } (\text{flow } cfs_2) s_1 x) \longrightarrow$
 $(c', t_1) \rightarrow^* (c_2', t_2) \wedge (c'' = \text{SKIP}) = (c_2' = \text{SKIP})) \wedge$
 $(s_1 = t_1 (\subseteq \text{sources } (\text{flow } cfs_2) s_1 x) \longrightarrow s_2 x = t_2 x)) \wedge$
 $(\forall x. (\exists p \in U. \text{case } p \text{ of } (B, W) \Rightarrow$
 $\exists s \in B. \exists y \in W. \neg s: \text{dom } y \rightsquigarrow \text{dom } x) \longrightarrow \text{no-upd } (\text{flow } cfs_2) x)$

proof –

have

$(\exists d' cfs. c' = d';; c_2 \wedge$
 $(c_1, s) \rightarrow^* \{cfs\} (d', s_1)) \vee$
 $(\exists s' cfs cfs'.$
 $(c_1, s) \rightarrow^* \{cfs\} (\text{SKIP}, s') \wedge$
 $(c_2, s') \rightarrow^* \{cfs'\} (c', s_1))$

using E **by** (*blast dest: small-steps1-seq*)

thus *?thesis*

proof (*rule disjE*, (*erule-tac exE*) $+$, (*erule-tac [2] exE*) $+$,
erule-tac [!] conjE)

fix $d' cfs$

assume

$I: c' = d';; c_2 \text{ and}$
 $J: (c_1, s) \rightarrow^* \{cfs\} (d', s_1)$

hence $(d';; c_2, s_1) \rightarrow^* \{cfs_2\} (c'', s_2)$

using F **by** *simp*

hence

$(\exists d'' cfs'. c'' = d'';; c_2 \wedge$
 $(d', s_1) \rightarrow^* \{cfs'\} (d'', s_2) \wedge$
 $\text{flow } cfs_2 = \text{flow } cfs') \vee$
 $(\exists s' cfs' cfs''.$
 $(d', s_1) \rightarrow^* \{cfs'\} (\text{SKIP}, s') \wedge$
 $(c_2, s') \rightarrow^* \{cfs''\} (c'', s_2) \wedge$
 $\text{flow } cfs_2 = \text{flow } cfs' @ \text{flow } cfs'')$

by (*blast dest: small-steps1-seq*)
 thus ?thesis
 proof (rule *disjE*, (*erule-tac exE*)+, (*erule-tac [2] exE*)+,
 (*erule-tac [!] conjE*)+)

fix d'' cfs'
 assume $(d', s_1) \rightarrow^*\{cfs'\} (d'', s_2)$
 hence K :
 $(\forall t_1. \exists c_2' t_2. \forall x.$
 $(s_1 = t_1 (\subseteq \text{sources-aux } (flow\ cfs')\ s_1\ x) \longrightarrow$
 $(d', t_1) \rightarrow^* (c_2', t_2) \wedge (d'' = SKIP) = (c_2' = SKIP)) \wedge$
 $(s_1 = t_1 (\subseteq \text{sources } (flow\ cfs')\ s_1\ x) \longrightarrow s_2\ x = t_2\ x)) \wedge$
 $(\forall x. (\exists p \in U. \text{case } p \text{ of } (B, W) \Rightarrow$
 $\exists s \in B. \exists y \in W. \neg s: \text{dom } y \rightsquigarrow \text{dom } x) \longrightarrow \text{no-upd } (flow\ cfs')\ x)$
 using A [*of B s cfs d' s₁ cfs' d'' s₂*] and J and G and H by *blast*
 moreover assume $c'' = d''$; c_2 and $flow\ cfs_2 = flow\ cfs'$
 moreover {
 fix t_1
 obtain c_2' and t_2 where L : $\forall x.$
 $(s_1 = t_1 (\subseteq \text{sources-aux } (flow\ cfs')\ s_1\ x) \longrightarrow$
 $(d', t_1) \rightarrow^* (c_2', t_2) \wedge (d'' = SKIP) = (c_2' = SKIP)) \wedge$
 $(s_1 = t_1 (\subseteq \text{sources } (flow\ cfs')\ s_1\ x) \longrightarrow s_2\ x = t_2\ x)$
 using K by *blast*
 have $\exists c_2' t_2. \forall x.$
 $(s_1 = t_1 (\subseteq \text{sources-aux } (flow\ cfs')\ s_1\ x) \longrightarrow$
 $(d'; c_2, t_1) \rightarrow^* (c_2', t_2) \wedge c_2' \neq SKIP) \wedge$
 $(s_1 = t_1 (\subseteq \text{sources } (flow\ cfs')\ s_1\ x) \longrightarrow s_2\ x = t_2\ x)$
 proof (rule *exI* [*of - c₂';; c₂*], rule *exI* [*of - t₂*])
 show $\forall x.$
 $(s_1 = t_1 (\subseteq \text{sources-aux } (flow\ cfs')\ s_1\ x) \longrightarrow$
 $(d'; c_2, t_1) \rightarrow^* (c_2'; c_2, t_2) \wedge c_2' \neq SKIP) \wedge$
 $(s_1 = t_1 (\subseteq \text{sources } (flow\ cfs')\ s_1\ x) \longrightarrow s_2\ x = t_2\ x)$
 using L by (*auto intro: star-seq2*)
 qed
 }
 ultimately show ?thesis
 using I by *auto*

next
 fix s' cfs' cfs''
 assume
 $K: (d', s_1) \rightarrow^*\{cfs'\} (SKIP, s')$ and
 $L: (c_2, s') \rightarrow^*\{cfs''\} (c'', s_2)$
 moreover have $M: s' = \text{run-flow } (flow\ cfs')\ s_1$
 using K by (*rule small-steps1-run-flow*)
 ultimately have N :
 $(\forall t_1. \exists c_2' t_2. \forall x.$
 $(s_1 = t_1 (\subseteq \text{sources-aux } (flow\ cfs')\ s_1\ x) \longrightarrow$
 $(d', t_1) \rightarrow^* (c_2', t_2) \wedge (SKIP = SKIP) = (c_2' = SKIP)) \wedge$
 $(s_1 = t_1 (\subseteq \text{sources } (flow\ cfs')\ s_1\ x) \longrightarrow$
 $\text{run-flow } (flow\ cfs')\ s_1\ x = t_2\ x)) \wedge$

$(\forall x. (\exists p \in U. \text{case } p \text{ of } (B, W) \Rightarrow$
 $\exists s \in B. \exists y \in W. \neg s: \text{dom } y \rightsquigarrow \text{dom } x) \longrightarrow \text{no-upd } (\text{flow } cfs') x)$
using A [of B s cfs d' s_1 cfs' $SKIP$ s'] **and** J **and** G **and** H **by** *blast*
have $O: s_2 = \text{run-flow } (\text{flow } cfs'') s'$
using L **by** (*rule small-stepsl-run-flow*)
moreover have $(c_1, s) \rightarrow^* \{cfs @ cfs'\} (SKIP, s')$
using J **and** K **by** (*simp add: small-stepsl-append*)
hence $(c_1, s) \Rightarrow s'$
by (*auto dest: small-stepsl-steps simp: big-iff-small*)
hence $s' \in \text{Univ } B (\subseteq \text{state} \cap Y)$
using C **and** G **and** H **by** (*erule-tac ctying2-approx, auto*)
ultimately have P :
 $(\forall t_1. \exists c_2' t_2. \forall x.$
 $(\text{run-flow } (\text{flow } cfs') s_1 = t_1$
 $(\subseteq \text{sources-aux } (\text{flow } cfs'') (\text{run-flow } (\text{flow } cfs') s_1) x) \longrightarrow$
 $(c_2, t_1) \rightarrow^* (c_2', t_2) \wedge (c'' = SKIP) = (c_2' = SKIP)) \wedge$
 $(\text{run-flow } (\text{flow } cfs') s_1 = t_1$
 $(\subseteq \text{sources } (\text{flow } cfs'') (\text{run-flow } (\text{flow } cfs') s_1) x) \longrightarrow$
 $\text{run-flow } (\text{flow } cfs'') (\text{run-flow } (\text{flow } cfs') s_1) x = t_2 x)) \wedge$
 $(\forall x. (\exists p \in U. \text{case } p \text{ of } (B, W) \Rightarrow$
 $\exists s \in B. \exists y \in W. \neg s: \text{dom } y \rightsquigarrow \text{dom } x) \longrightarrow \text{no-upd } (\text{flow } cfs'') x)$
using B [of B B C Z s' c_2 s' cfs'' c'' s_2]
and D **and** L **and** M **by** *simp*
moreover assume $\text{flow } cfs_2 = \text{flow } cfs' @ \text{flow } cfs''$
moreover {
fix t_1
obtain c_2' **and** t_2 **where** $Q: \forall x.$
 $(s_1 = t_1 (\subseteq \text{sources-aux } (\text{flow } cfs') s_1) x) \longrightarrow$
 $(d', t_1) \rightarrow^* (SKIP, t_2) \wedge (SKIP = SKIP) = (c_2' = SKIP)) \wedge$
 $(s_1 = t_1 (\subseteq \text{sources } (\text{flow } cfs') s_1) x) \longrightarrow$
 $\text{run-flow } (\text{flow } cfs') s_1 x = t_2 x)$
using N **by** *blast*
obtain c_3' **and** t_3 **where** $R: \forall x.$
 $(\text{run-flow } (\text{flow } cfs') s_1 = t_2$
 $(\subseteq \text{sources-aux } (\text{flow } cfs'') (\text{run-flow } (\text{flow } cfs') s_1) x) \longrightarrow$
 $(c_2, t_2) \rightarrow^* (c_3', t_3) \wedge (c'' = SKIP) = (c_3' = SKIP)) \wedge$
 $(\text{run-flow } (\text{flow } cfs') s_1 = t_2$
 $(\subseteq \text{sources } (\text{flow } cfs'') (\text{run-flow } (\text{flow } cfs') s_1) x) \longrightarrow$
 $\text{run-flow } (\text{flow } cfs'') (\text{run-flow } (\text{flow } cfs') s_1) x = t_3 x)$
using P **by** *blast*
{
fix x
assume $S: s_1 = t_1$
 $(\subseteq \text{sources-aux } (\text{flow } cfs' @ \text{flow } cfs'') s_1) x)$
moreover have $\text{sources-aux } (\text{flow } cfs') s_1 x \subseteq$
 $\text{sources-aux } (\text{flow } cfs' @ \text{flow } cfs'') s_1 x$
by (*rule sources-aux-append*)
ultimately have $(d', t_1) \rightarrow^* (SKIP, t_2)$
using Q **by** *blast*

hence $(d';; c_2, t_1) \rightarrow^* (SKIP;; c_2, t_2)$
 by (rule star-seq2)
 hence $(d';; c_2, t_1) \rightarrow^* (c_2, t_2)$
 by (blast intro: star-trans)
 moreover have $\text{run-flow } (\text{flow cfs}') s_1 = t_2$
 $(\subseteq \text{sources-aux } (\text{flow cfs}'') (\text{run-flow } (\text{flow cfs}') s_1) x)$
 proof
 fix y
 assume $y \in \text{sources-aux } (\text{flow cfs}'')$
 $(\text{run-flow } (\text{flow cfs}') s_1) x$
 hence $\text{sources } (\text{flow cfs}') s_1 y \subseteq$
 $\text{sources-aux } (\text{flow cfs}' @ \text{flow cfs}'') s_1 x$
 by (rule sources-aux-member)
 thus $\text{run-flow } (\text{flow cfs}') s_1 y = t_2 y$
 using Q and S by blast
 qed
 hence $(c_2, t_2) \rightarrow^* (c_3', t_3) \wedge (c'' = SKIP) = (c_3' = SKIP)$
 using R by simp
 ultimately have $(d';; c_2, t_1) \rightarrow^* (c_3', t_3) \wedge$
 $(c'' = SKIP) = (c_3' = SKIP)$
 by (blast intro: star-trans)
 }
 moreover {
 fix x
 assume $S: s_1 = t_1$
 $(\subseteq \text{sources } (\text{flow cfs}' @ \text{flow cfs}'') s_1 x)$
 have $\text{run-flow } (\text{flow cfs}') s_1 = t_2$
 $(\subseteq \text{sources } (\text{flow cfs}'') (\text{run-flow } (\text{flow cfs}') s_1) x)$
 proof
 fix y
 assume $y \in \text{sources } (\text{flow cfs}'')$
 $(\text{run-flow } (\text{flow cfs}') s_1) x$
 hence $\text{sources } (\text{flow cfs}') s_1 y \subseteq$
 $\text{sources } (\text{flow cfs}' @ \text{flow cfs}'') s_1 x$
 by (rule sources-member)
 thus $\text{run-flow } (\text{flow cfs}') s_1 y = t_2 y$
 using Q and S by blast
 qed
 hence $\text{run-flow } (\text{flow cfs}'') (\text{run-flow } (\text{flow cfs}') s_1) x = t_3 x$
 using R by simp
 }
 ultimately have $\exists c_2' t_2. \forall x.$
 $(s_1 = t_1 (\subseteq \text{sources-aux } (\text{flow cfs}' @ \text{flow cfs}'') s_1 x) \longrightarrow$
 $(d';; c_2, t_1) \rightarrow^* (c_2', t_2) \wedge (c'' = SKIP) = (c_2' = SKIP)) \wedge$
 $(s_1 = t_1 (\subseteq \text{sources } (\text{flow cfs}' @ \text{flow cfs}'') s_1 x) \longrightarrow$
 $\text{run-flow } (\text{flow cfs}'') (\text{run-flow } (\text{flow cfs}') s_1) x = t_2 x)$
 by auto
 }
 ultimately show ?thesis

using I and N and M and O by (auto simp: no-upd-append)
 qed
 next
 fix $s' \text{ cfs cfs'}$
 assume $(c_1, s) \rightarrow^* \{cfs\} (SKIP, s')$
 hence $(c_1, s) \Rightarrow s'$
 by (auto dest: small-steps1-steps simp: big-iff-small)
 hence $s' \in \text{Univ } B (\subseteq \text{state} \cap Y)$
 using C and G and H by (erule-tac ctying2-approx, auto)
 moreover assume $(c_2, s') \rightarrow^* \{cfs'\} (c', s_1)$
 ultimately show ?thesis
 using B [of $B B C Z s' cfs' c' s_1 cfs_2 c'' s_2$] and D and F by simp
 qed
 qed

lemma ctying2-correct-aux-if:

assumes

$A: \bigwedge U' B C s c' c'' s_1 s_2 cfs_1 cfs_2.$
 $U' = \text{insert } (\text{Univ? } A X, \text{bvars } b) U \implies B = B_1 \implies C_1 = C \implies$
 $\exists r \in B_1. s = r (\subseteq \text{state} \cap X) \implies$
 $(c_1, s) \rightarrow^* \{cfs_1\} (c', s_1) \implies (c', s_1) \rightarrow^* \{cfs_2\} (c'', s_2) \implies$
 $(\forall t_1. \exists c_2' t_2. \forall x.$
 $(s_1 = t_1 (\subseteq \text{sources-aux } (\text{flow } cfs_2) s_1 x) \longrightarrow$
 $(c', t_1) \rightarrow^* (c_2', t_2) \wedge (c'' = SKIP) = (c_2' = SKIP)) \wedge$
 $(s_1 = t_1 (\subseteq \text{sources } (\text{flow } cfs_2) s_1 x) \longrightarrow s_2 x = t_2 x)) \wedge$
 $(\forall x.$
 $((\exists s \in \text{Univ? } A X. \exists y \in \text{bvars } b. \neg s: \text{dom } y \rightsquigarrow \text{dom } x) \longrightarrow$
 $\text{no-upd } (\text{flow } cfs_2) x) \wedge$
 $((\exists p \in U. \text{case } p \text{ of } (B, W) \Rightarrow$
 $\exists s \in B. \exists y \in W. \neg s: \text{dom } y \rightsquigarrow \text{dom } x) \longrightarrow$
 $\text{no-upd } (\text{flow } cfs_2) x)) \text{ and}$
 $B: \bigwedge U' B C s c' c'' s_1 s_2 cfs_1 cfs_2.$
 $U' = \text{insert } (\text{Univ? } A X, \text{bvars } b) U \implies B = B_1 \implies C_2 = C \implies$
 $\exists r \in B_2. s = r (\subseteq \text{state} \cap X) \implies$
 $(c_2, s) \rightarrow^* \{cfs_1\} (c', s_1) \implies (c', s_1) \rightarrow^* \{cfs_2\} (c'', s_2) \implies$
 $(\forall t_1. \exists c_2' t_2. \forall x.$
 $(s_1 = t_1 (\subseteq \text{sources-aux } (\text{flow } cfs_2) s_1 x) \longrightarrow$
 $(c', t_1) \rightarrow^* (c_2', t_2) \wedge (c'' = SKIP) = (c_2' = SKIP)) \wedge$
 $(s_1 = t_1 (\subseteq \text{sources } (\text{flow } cfs_2) s_1 x) \longrightarrow s_2 x = t_2 x)) \wedge$
 $(\forall x.$
 $((\exists s \in \text{Univ? } A X. \exists y \in \text{bvars } b. \neg s: \text{dom } y \rightsquigarrow \text{dom } x) \longrightarrow$
 $\text{no-upd } (\text{flow } cfs_2) x) \wedge$
 $((\exists p \in U. \text{case } p \text{ of } (B, W) \Rightarrow$
 $\exists s \in B. \exists y \in W. \neg s: \text{dom } y \rightsquigarrow \text{dom } x) \longrightarrow$
 $\text{no-upd } (\text{flow } cfs_2) x)) \text{ and}$
 $C: \models b (\subseteq A, X) = (B_1, B_2) \text{ and}$
 $D: (\text{insert } (\text{Univ? } A X, \text{bvars } b) U, v) \models c_1 (\subseteq B_1, X) =$
 $\text{Some } (C_1, Y_1) \text{ and}$
 $E: (\text{insert } (\text{Univ? } A X, \text{bvars } b) U, v) \models c_2 (\subseteq B_2, X) =$

Some (C_2, Y_2) and
 $F: (IF\ b\ THEN\ c_1\ ELSE\ c_2, s) \rightarrow^*\{cfs_1\} (c', s_1)$ and
 $G: (c', s_1) \rightarrow^*\{cfs_2\} (c'', s_2)$ and
 $H: r \in A$ and
 $I: s = r (\subseteq state \cap X)$
 shows
 $(\forall t_1. \exists c_2' t_2. \forall x.$
 $(s_1 = t_1 (\subseteq sources_aux\ (flow\ cfs_2)\ s_1\ x) \longrightarrow$
 $(c', t_1) \rightarrow^* (c_2', t_2) \wedge (c'' = SKIP) = (c_2' = SKIP)) \wedge$
 $(s_1 = t_1 (\subseteq sources\ (flow\ cfs_2)\ s_1\ x) \longrightarrow s_2\ x = t_2\ x)) \wedge$
 $(\forall x. (\exists p \in U. case\ p\ of\ (B, W) \Rightarrow$
 $\exists s \in B. \exists y \in W. \neg s: dom\ y \rightsquigarrow dom\ x) \longrightarrow no_upd\ (flow\ cfs_2)\ x)$
 proof –
 let $?U' = insert\ (Univ?\ A\ X, bvars\ b)\ U$
 have $J: \forall cs\ t\ x. s = t (\subseteq sources_aux\ ((bvars\ b) \# cs)\ s\ x) \longrightarrow$
 $bval\ b\ s \neq bval\ b\ t \longrightarrow \neg Univ?\ A\ X: dom\ 'bvars\ b \rightsquigarrow \{dom\ x\}$
 proof (clarify del: notI)
 fix $cs\ t\ x$
 assume $s = t (\subseteq sources_aux\ ((bvars\ b) \# cs)\ s\ x)$
 moreover assume $bval\ b\ s \neq bval\ b\ t$
 hence $\neg s = t (\subseteq bvars\ b)$
 by (erule-tac contrapos-nn, auto dest: bvars-bval)
 ultimately have $\neg (\forall y \in bvars\ b. s: dom\ y \rightsquigarrow dom\ x)$
 by (blast dest: sources-aux-observe-hd)
 moreover {
 fix $r\ y$
 assume $r \in A$ and $y \in bvars\ b$ and $\neg s: dom\ y \rightsquigarrow dom\ x$
 moreover assume $state \subseteq X$ and $s = r (\subseteq state \cap X)$
 hence $interf\ s = interf\ r$
 by (blast intro: interf-state)
 ultimately have $\exists s \in A. \exists y \in bvars\ b. \neg s: dom\ y \rightsquigarrow dom\ x$
 by auto
 }
 ultimately show $\neg Univ?\ A\ X: dom\ 'bvars\ b \rightsquigarrow \{dom\ x\}$
 using H and I by (auto simp: univ-states-if-def)
 qed
 have
 $(c', s_1) = (IF\ b\ THEN\ c_1\ ELSE\ c_2, s) \vee$
 $bval\ b\ s \wedge (c_1, s) \rightarrow^*\{tl\ cfs_1\} (c', s_1) \vee$
 $\neg bval\ b\ s \wedge (c_2, s) \rightarrow^*\{tl\ cfs_1\} (c', s_1)$
 using F by (blast dest: small-steps1-if)
 thus ?thesis
 proof (rule disjE, erule-tac [2] disjE, erule-tac [2-3] conjE)
 assume $K: (c', s_1) = (IF\ b\ THEN\ c_1\ ELSE\ c_2, s)$
 hence $(IF\ b\ THEN\ c_1\ ELSE\ c_2, s) \rightarrow^*\{cfs_2\} (c'', s_2)$
 using G by simp
 hence
 $(c'', s_2) = (IF\ b\ THEN\ c_1\ ELSE\ c_2, s) \wedge$
 $flow\ cfs_2 = [] \vee$

$bval\ b\ s \wedge (c_1, s) \rightarrow^*\{tl\ cfs_2\} (c'', s_2) \wedge$
 $flow\ cfs_2 = \langle bvars\ b \rangle \# flow\ (tl\ cfs_2) \vee$
 $\neg bval\ b\ s \wedge (c_2, s) \rightarrow^*\{tl\ cfs_2\} (c'', s_2) \wedge$
 $flow\ cfs_2 = \langle bvars\ b \rangle \# flow\ (tl\ cfs_2)$
by (*rule small-steps-l-if*)
thus ?thesis
proof (*rule disjE*, *erule-tac* [2] *disjE*, (*erule-tac* [2-3] *conjE*)+)
assume $(c'', s_2) = (IF\ b\ THEN\ c_1\ ELSE\ c_2, s) \wedge flow\ cfs_2 = []$
thus ?thesis
using K **by** *auto*
next
assume $L: bval\ b\ s$
with C **and** H **and** I **have** $s \in Univ\ B_1 (\subseteq state \cap X)$
by (*drule-tac btyping2-approx* [**where** $s = s$], *auto*)
moreover assume $M: (c_1, s) \rightarrow^*\{tl\ cfs_2\} (c'', s_2)$
moreover from this have $N: s_2 = run-flow\ (flow\ (tl\ cfs_2))\ s$
by (*rule small-steps-l-run-flow*)
ultimately have $O:$
 $(\forall t_1. \exists c_2' t_2. \forall x.$
 $(s = t_1 (\subseteq sources- aux\ (flow\ (tl\ cfs_2))\ s\ x) \longrightarrow$
 $(c_1, t_1) \rightarrow^* (c_2', t_2) \wedge (c'' = SKIP) = (c_2' = SKIP)) \wedge$
 $(s = t_1 (\subseteq sources\ (flow\ (tl\ cfs_2))\ s\ x) \longrightarrow$
 $run-flow\ (flow\ (tl\ cfs_2))\ s\ x = t_2\ x)) \wedge$
 $(\forall x.$
 $((\exists s \in Univ? A\ X. \exists y \in bvars\ b. \neg s: dom\ y \rightsquigarrow dom\ x) \longrightarrow$
 $no-upd\ (flow\ (tl\ cfs_2))\ x) \wedge$
 $((\exists p \in U. case\ p\ of\ (B, W) \Rightarrow$
 $\exists s \in B. \exists y \in W. \neg s: dom\ y \rightsquigarrow dom\ x) \longrightarrow$
 $no-upd\ (flow\ (tl\ cfs_2))\ x))$
using A [*of* ? U' $B_1\ C_1\ s\ []\ c_1\ s\ tl\ cfs_2\ c''\ s_2$] **by** *simp*
moreover assume $flow\ cfs_2 = \langle bvars\ b \rangle \# flow\ (tl\ cfs_2)$
moreover {
fix t_1
have $\exists c_2' t_2. \forall x.$
 $(s = t_1 (\subseteq sources- aux\ (\langle bvars\ b \rangle \# flow\ (tl\ cfs_2))\ s\ x) \longrightarrow$
 $(IF\ b\ THEN\ c_1\ ELSE\ c_2, t_1) \rightarrow^* (c_2', t_2) \wedge$
 $(c'' = SKIP) = (c_2' = SKIP)) \wedge$
 $(s = t_1 (\subseteq sources\ (\langle bvars\ b \rangle \# flow\ (tl\ cfs_2))\ s\ x) \longrightarrow$
 $run-flow\ (flow\ (tl\ cfs_2))\ s\ x = t_2\ x)$
proof (*cases* $bval\ b\ t_1$)
case *True*
hence $P: (IF\ b\ THEN\ c_1\ ELSE\ c_2, t_1) \rightarrow (c_1, t_1) ..$
obtain c_2' **and** t_2 **where** $Q: \forall x.$
 $(s = t_1 (\subseteq sources- aux\ (flow\ (tl\ cfs_2))\ s\ x) \longrightarrow$
 $(c_1, t_1) \rightarrow^* (c_2', t_2) \wedge (c'' = SKIP) = (c_2' = SKIP)) \wedge$
 $(s = t_1 (\subseteq sources\ (flow\ (tl\ cfs_2))\ s\ x) \longrightarrow$
 $run-flow\ (flow\ (tl\ cfs_2))\ s\ x = t_2\ x)$
using O **by** *blast*
{

```

fix  $x$ 
assume  $s = t_1$ 
  ( $\subseteq$  sources-aux ( $\langle bvars\ b \rangle \# flow\ (tl\ cfs_2)$ )  $s\ x$ )
moreover have sources-aux ( $flow\ (tl\ cfs_2)$ )  $s\ x \subseteq$ 
  sources-aux ( $\langle bvars\ b \rangle \# flow\ (tl\ cfs_2)$ )  $s\ x$ 
  by (rule sources-aux-observe-tl)
ultimately have (IF  $b$  THEN  $c_1$  ELSE  $c_2, t_1 \rightarrow^* (c_2', t_2) \wedge$ 
  ( $c'' = SKIP$ ) = ( $c_2' = SKIP$ ))
  using  $P$  and  $Q$  by (blast intro: star-trans)
}
moreover {
  fix  $x$ 
  assume  $s = t_1$ 
  ( $\subseteq$  sources ( $\langle bvars\ b \rangle \# flow\ (tl\ cfs_2)$ )  $s\ x$ )
  moreover have sources ( $flow\ (tl\ cfs_2)$ )  $s\ x \subseteq$ 
    sources ( $\langle bvars\ b \rangle \# flow\ (tl\ cfs_2)$ )  $s\ x$ 
    by (rule sources-observe-tl)
  ultimately have run-flow ( $flow\ (tl\ cfs_2)$ )  $s\ x = t_2\ x$ 
  using  $Q$  by blast
}
ultimately show ?thesis
  by auto
next
assume  $P: \neg bval\ b\ t_1$ 
show ?thesis
proof (cases  $\exists x. s = t_1$ )
  ( $\subseteq$  sources-aux ( $\langle bvars\ b \rangle \# flow\ (tl\ cfs_2)$ )  $s\ x$ )
  from  $P$  have (IF  $b$  THEN  $c_1$  ELSE  $c_2, t_1 \rightarrow (c_2, t_1)$  ..
  moreover assume  $\exists x. s = t_1$ 
  ( $\subseteq$  sources-aux ( $\langle bvars\ b \rangle \# flow\ (tl\ cfs_2)$ )  $s\ x$ )
  hence  $\exists x. \neg Univ? A\ X: dom\ 'bvars\ b \rightsquigarrow \{dom\ x\}$ 
  using  $J$  and  $L$  and  $P$  by blast
  then obtain  $t_2$  where  $Q: (c_2, t_1) \Rightarrow t_2$ 
  using  $E$  by (blast dest: ctyping2-term)
  hence  $(c_2, t_1) \rightarrow^* (SKIP, t_2)$ 
  by (simp add: big-iff-small)
  ultimately have
     $R: (IF\ b\ THEN\ c_1\ ELSE\ c_2, t_1) \rightarrow^* (SKIP, t_2)$ 
    by (blast intro: star-trans)
  show ?thesis
  proof (cases  $c'' = SKIP$ )
    case True
    show ?thesis
    proof (rule exI [of - SKIP], rule exI [of -  $t_2$ ])
      {
        have (IF  $b$  THEN  $c_1$  ELSE  $c_2, t_1 \rightarrow^* (SKIP, t_2) \wedge$ 
          ( $c'' = SKIP$ ) = ( $SKIP = SKIP$ ))
          using  $R$  and True by simp
      }
    }

```

```

moreover {
  fix  $x$ 
  assume  $S: s = t_1$ 
   $(\subseteq \text{sources } (\langle \text{bvars } b \rangle \# \text{flow } (tl \text{ cfs}_2)) s x)$ 
  moreover have
     $\text{sources-aux } (\langle \text{bvars } b \rangle \# \text{flow } (tl \text{ cfs}_2)) s x \subseteq$ 
     $\text{sources } (\langle \text{bvars } b \rangle \# \text{flow } (tl \text{ cfs}_2)) s x$ 
    by  $(\text{rule sources-aux-sources})$ 
  ultimately have  $s = t_1$ 
     $(\subseteq \text{sources-aux } (\langle \text{bvars } b \rangle \# \text{flow } (tl \text{ cfs}_2)) s x)$ 
    by  $\text{blast}$ 
  hence  $T: \neg \text{Univ? } A \ X: \text{dom } \langle \text{bvars } b \rangle \rightsquigarrow \{\text{dom } x\}$ 
    using  $J$  and  $L$  and  $P$  by  $\text{blast}$ 
  hence  $U: \text{no-upd } (\langle \text{bvars } b \rangle \# \text{flow } (tl \text{ cfs}_2)) x$ 
    using  $O$  by  $\text{simp}$ 
  hence  $\text{run-flow } (\text{flow } (tl \text{ cfs}_2)) s x = s x$ 
    by  $(\text{simp add: no-upd-run-flow})$ 
  also from  $S$  and  $U$  have  $\dots = t_1 x$ 
    by  $(\text{blast dest: no-upd-sources})$ 
  also from  $E$  and  $Q$  and  $T$  have  $\dots = t_2 x$ 
    by  $(\text{drule-tac ctying2-confine, auto})$ 
  finally have  $\text{run-flow } (\text{flow } (tl \text{ cfs}_2)) s x = t_2 x$  .
}
ultimately show  $\forall x.$ 
   $(s = t_1$ 
     $(\subseteq \text{sources-aux } (\langle \text{bvars } b \rangle \# \text{flow } (tl \text{ cfs}_2)) s x) \longrightarrow$ 
     $(\text{IF } b \text{ THEN } c_1 \text{ ELSE } c_2, t_1) \rightarrow^* (\text{SKIP}, t_2) \wedge$ 
     $(c'' = \text{SKIP}) = (\text{SKIP} = \text{SKIP})) \wedge$ 
   $(s = t_1$ 
     $(\subseteq \text{sources } (\langle \text{bvars } b \rangle \# \text{flow } (tl \text{ cfs}_2)) s x) \longrightarrow$ 
     $\text{run-flow } (\text{flow } (tl \text{ cfs}_2)) s x = t_2 x)$ 
  by  $\text{blast}$ 
qed
next
case  $\text{False}$ 
show  $?thesis$ 
proof  $(\text{rule exI } [\text{of - IF } b \text{ THEN } c_1 \text{ ELSE } c_2],$ 
   $\text{rule exI } [\text{of - } t_1])$ 
  {
    have  $(\text{IF } b \text{ THEN } c_1 \text{ ELSE } c_2, t_1) \rightarrow^*$ 
     $(\text{IF } b \text{ THEN } c_1 \text{ ELSE } c_2, t_1) \wedge$ 
     $(c'' = \text{SKIP}) = (\text{IF } b \text{ THEN } c_1 \text{ ELSE } c_2 = \text{SKIP})$ 
    using  $\text{False}$  by  $\text{simp}$ 
  }
moreover {
  fix  $x$ 
  assume  $S: s = t_1$ 
   $(\subseteq \text{sources } (\langle \text{bvars } b \rangle \# \text{flow } (tl \text{ cfs}_2)) s x)$ 
  moreover have

```

$\text{sources-aux } (\langle \text{bvars } b \rangle \# \text{flow } (tl \text{ cfs}_2)) \text{ } s \text{ } x \subseteq$
 $\text{sources } (\langle \text{bvars } b \rangle \# \text{flow } (tl \text{ cfs}_2)) \text{ } s \text{ } x$
by (rule *sources-aux-sources*)
ultimately have $s = t_1$
 $(\subseteq \text{sources-aux } (\langle \text{bvars } b \rangle \# \text{flow } (tl \text{ cfs}_2)) \text{ } s \text{ } x)$
by *blast*
hence $\neg \text{Univ? } A \text{ } X: \text{dom } \text{' } \text{bvars } b \rightsquigarrow \{\text{dom } x\}$
using *J and L and P by blast*
hence $T: \text{no-upd } (\langle \text{bvars } b \rangle \# \text{flow } (tl \text{ cfs}_2)) \text{ } x$
using *O by simp*
hence $\text{run-flow } (\text{flow } (tl \text{ cfs}_2)) \text{ } s \text{ } x = s \text{ } x$
by (*simp add: no-upd-run-flow*)
also have $\dots = t_1 \text{ } x$
using *S and T by (blast dest: no-upd-sources)*
finally have $\text{run-flow } (\text{flow } (tl \text{ cfs}_2)) \text{ } s \text{ } x = t_1 \text{ } x$.
}
ultimately show $\forall x.$
 $(s = t_1$
 $(\subseteq \text{sources-aux } (\langle \text{bvars } b \rangle \# \text{flow } (tl \text{ cfs}_2)) \text{ } s \text{ } x) \longrightarrow$
 $(\text{IF } b \text{ THEN } c_1 \text{ ELSE } c_2, t_1) \rightarrow^*$
 $(\text{IF } b \text{ THEN } c_1 \text{ ELSE } c_2, t_1) \wedge$
 $(c'' = \text{SKIP}) = (\text{IF } b \text{ THEN } c_1 \text{ ELSE } c_2 = \text{SKIP})) \wedge$
 $(s = t_1$
 $(\subseteq \text{sources } (\langle \text{bvars } b \rangle \# \text{flow } (tl \text{ cfs}_2)) \text{ } s \text{ } x) \longrightarrow$
 $\text{run-flow } (\text{flow } (tl \text{ cfs}_2)) \text{ } s \text{ } x = t_1 \text{ } x)$
by *blast*
qed
qed
qed *blast*
qed
}
ultimately show *?thesis*
using *K and N by auto*
next
assume $L: \neg \text{bval } b \text{ } s$
with *C and H and I have* $s \in \text{Univ } B_2 (\subseteq \text{state} \cap X)$
by (*drule-tac btyping2-approx [where s = s], auto*)
moreover assume $M: (c_2, s) \rightarrow^* \{tl \text{ cfs}_2\} (c'', s_2)$
moreover from this have $N: s_2 = \text{run-flow } (\text{flow } (tl \text{ cfs}_2)) \text{ } s$
by (*rule small-steps1-run-flow*)
ultimately have *O:*
 $(\forall t_1. \exists c_2' t_2. \forall x.$
 $(s = t_1 (\subseteq \text{sources-aux } (\text{flow } (tl \text{ cfs}_2)) \text{ } s \text{ } x) \longrightarrow$
 $(c_2, t_1) \rightarrow^* (c_2', t_2) \wedge (c'' = \text{SKIP}) = (c_2' = \text{SKIP})) \wedge$
 $(s = t_1 (\subseteq \text{sources } (\text{flow } (tl \text{ cfs}_2)) \text{ } s \text{ } x) \longrightarrow$
 $\text{run-flow } (\text{flow } (tl \text{ cfs}_2)) \text{ } s \text{ } x = t_2 \text{ } x)) \wedge$
 $(\forall x.$
 $((\exists s \in \text{Univ? } A \text{ } X. \exists y \in \text{bvars } b. \neg s: \text{dom } y \rightsquigarrow \text{dom } x) \longrightarrow$
 $\text{no-upd } (\text{flow } (tl \text{ cfs}_2)) \text{ } x) \wedge$

```

(( $\exists p \in U$ . case  $p$  of  $(B, W) \Rightarrow$ 
 $\exists s \in B$ .  $\exists y \in W$ .  $\neg s$ :  $\text{dom } y \rightsquigarrow \text{dom } x \longrightarrow$ 
 $\text{no-upd } (\text{flow } (tl \text{ cfs}_2)) \ x)$ )
using  $B$  [of  $?U'$   $B_1 \ C_2 \ s \ [] \ c_2 \ s \ tl \ \text{cfs}_2 \ c'' \ s_2$ ] by simp
moreover assume  $\text{flow } \text{cfs}_2 = \langle \text{bvars } b \rangle \# \text{flow } (tl \ \text{cfs}_2)$ 
moreover {
  fix  $t_1$ 
  have  $\exists c_2' \ t_2$ .  $\forall x$ .
    ( $s = t_1 \ (\subseteq \text{sources-aux } (\langle \text{bvars } b \rangle \# \text{flow } (tl \ \text{cfs}_2)) \ s \ x) \longrightarrow$ 
    (IF  $b$  THEN  $c_1$  ELSE  $c_2, t_1) \rightarrow^* (c_2', t_2) \wedge$ 
    ( $c'' = \text{SKIP} = (c_2' = \text{SKIP})$ )  $\wedge$ 
    ( $s = t_1 \ (\subseteq \text{sources } (\langle \text{bvars } b \rangle \# \text{flow } (tl \ \text{cfs}_2)) \ s \ x) \longrightarrow$ 
     $\text{run-flow } (\text{flow } (tl \ \text{cfs}_2)) \ s \ x = t_2 \ x$ )
  proof (cases  $\neg \text{bval } b \ t_1$ )
    case True
    hence  $P$ : (IF  $b$  THEN  $c_1$  ELSE  $c_2, t_1) \rightarrow (c_2, t_1) \dots$ 
    obtain  $c_2'$  and  $t_2$  where  $Q$ :  $\forall x$ .
      ( $s = t_1 \ (\subseteq \text{sources-aux } (\text{flow } (tl \ \text{cfs}_2)) \ s \ x) \longrightarrow$ 
      ( $c_2, t_1) \rightarrow^* (c_2', t_2) \wedge (c'' = \text{SKIP}) = (c_2' = \text{SKIP})$ )  $\wedge$ 
      ( $s = t_1 \ (\subseteq \text{sources } (\text{flow } (tl \ \text{cfs}_2)) \ s \ x) \longrightarrow$ 
       $\text{run-flow } (\text{flow } (tl \ \text{cfs}_2)) \ s \ x = t_2 \ x$ )
      using  $O$  by blast
    }
  fix  $x$ 
  assume  $s = t_1$ 
    ( $\subseteq \text{sources-aux } (\langle \text{bvars } b \rangle \# \text{flow } (tl \ \text{cfs}_2)) \ s \ x$ )
  moreover have  $\text{sources-aux } (\text{flow } (tl \ \text{cfs}_2)) \ s \ x \subseteq$ 
     $\text{sources-aux } (\langle \text{bvars } b \rangle \# \text{flow } (tl \ \text{cfs}_2)) \ s \ x$ 
  by (rule sources-aux-observe-tl)
  ultimately have (IF  $b$  THEN  $c_1$  ELSE  $c_2, t_1) \rightarrow^* (c_2', t_2) \wedge$ 
    ( $c'' = \text{SKIP} = (c_2' = \text{SKIP})$ )
  using  $P$  and  $Q$  by (blast intro: star-trans)
}
moreover {
  fix  $x$ 
  assume  $s = t_1$ 
    ( $\subseteq \text{sources } (\langle \text{bvars } b \rangle \# \text{flow } (tl \ \text{cfs}_2)) \ s \ x$ )
  moreover have  $\text{sources } (\text{flow } (tl \ \text{cfs}_2)) \ s \ x \subseteq$ 
     $\text{sources } (\langle \text{bvars } b \rangle \# \text{flow } (tl \ \text{cfs}_2)) \ s \ x$ 
  by (rule sources-observe-tl)
  ultimately have  $\text{run-flow } (\text{flow } (tl \ \text{cfs}_2)) \ s \ x = t_2 \ x$ 
  using  $Q$  by blast
}
ultimately show ?thesis
by auto
next
case False
hence  $P$ :  $\text{bval } b \ t_1$ 
by simp

```


show ?thesis
proof (cases $\exists x. s = t_1$
 $(\subseteq \text{sources-aux } (\langle \text{bvars } b \rangle \# \text{flow } (tl \text{ cfs}_2)) s x)$
from P **have** $(IF \ b \ THEN \ c_1 \ ELSE \ c_2, t_1) \rightarrow (c_1, t_1) \ ..$
moreover assume $\exists x. s = t_1$
 $(\subseteq \text{sources-aux } (\langle \text{bvars } b \rangle \# \text{flow } (tl \text{ cfs}_2)) s x)$
hence $\exists x. \neg Univ? \ A \ X: dom \ ' \ \text{bvars } b \rightsquigarrow \{dom \ x\}$
using J **and** L **and** P **by** $blast$
then obtain t_2 **where** $Q: (c_1, t_1) \Rightarrow t_2$
using D **by** $(blast \ dest: \text{ctyping2-term})$
hence $(c_1, t_1) \rightarrow^* (SKIP, t_2)$
by $(simp \ add: \text{big-iff-small})$
ultimately have
 $R: (IF \ b \ THEN \ c_1 \ ELSE \ c_2, t_1) \rightarrow^* (SKIP, t_2)$
by $(blast \ intro: \text{star-trans})$
show ?thesis
proof (cases $c'' = SKIP$)
case $True$
show ?thesis
proof (rule exI [of - $SKIP$], rule exI [of - t_2])
 $\{$
have $(IF \ b \ THEN \ c_1 \ ELSE \ c_2, t_1) \rightarrow^* (SKIP, t_2) \wedge$
 $(c'' = SKIP) = (SKIP = SKIP)$
using R **and** $True$ **by** $simp$
 $\}$
moreover $\{$
fix x
assume $S: s = t_1$
 $(\subseteq \text{sources } (\langle \text{bvars } b \rangle \# \text{flow } (tl \text{ cfs}_2)) s x)$
moreover have
 $\text{sources-aux } (\langle \text{bvars } b \rangle \# \text{flow } (tl \text{ cfs}_2)) s x \subseteq$
 $\text{sources } (\langle \text{bvars } b \rangle \# \text{flow } (tl \text{ cfs}_2)) s x$
by $(rule \ \text{sources-aux-sources})$
ultimately have $s = t_1$
 $(\subseteq \text{sources-aux } (\langle \text{bvars } b \rangle \# \text{flow } (tl \text{ cfs}_2)) s x)$
by $blast$
hence $T: \neg Univ? \ A \ X: dom \ ' \ \text{bvars } b \rightsquigarrow \{dom \ x\}$
using J **and** L **and** P **by** $blast$
hence $U: no-upd (\langle \text{bvars } b \rangle \# \text{flow } (tl \text{ cfs}_2)) x$
using O **by** $simp$
hence $run-flow (\text{flow } (tl \text{ cfs}_2)) s x = s x$
by $(simp \ add: \text{no-upd-run-flow})$
also from S **and** U **have** $\dots = t_1 \ x$
by $(blast \ dest: \text{no-upd-sources})$
also from D **and** Q **and** T **have** $\dots = t_2 \ x$
by $(drule-tac \ \text{ctyping2-confine}, \ auto)$
finally have $run-flow (\text{flow } (tl \text{ cfs}_2)) s x = t_2 \ x \ .$
 $\}$
ultimately show $\forall x.$

```

    (s = t1
      (⊆ sources-aux (⟨bvars b⟩ # flow (tl cfs2)) s x) →
      (IF b THEN c1 ELSE c2, t1) →* (SKIP, t2) ∧
      (c'' = SKIP) = (SKIP = SKIP)) ∧
    (s = t1
      (⊆ sources (⟨bvars b⟩ # flow (tl cfs2)) s x) →
      run-flow (flow (tl cfs2)) s x = t2 x)
  by blast
qed
next
case False
show ?thesis
proof (rule exI [of - IF b THEN c1 ELSE c2],
  rule exI [of - t1])
{
  have (IF b THEN c1 ELSE c2, t1) →*
    (IF b THEN c1 ELSE c2, t1) ∧
    (c'' = SKIP) = (IF b THEN c1 ELSE c2 = SKIP)
  using False by simp
}
moreover {
  fix x
  assume S: s = t1
  (⊆ sources (⟨bvars b⟩ # flow (tl cfs2)) s x)
  moreover have
    sources-aux (⟨bvars b⟩ # flow (tl cfs2)) s x ⊆
    sources (⟨bvars b⟩ # flow (tl cfs2)) s x
  by (rule sources-aux-sources)
  ultimately have s = t1
    (⊆ sources-aux (⟨bvars b⟩ # flow (tl cfs2)) s x)
  by blast
  hence ¬ Univ? A X: dom ' bvars b ~> {dom x}
  using J and L and P by blast
  hence T: no-upd (⟨bvars b⟩ # flow (tl cfs2)) x
  using O by simp
  hence run-flow (flow (tl cfs2)) s x = s x
  by (simp add: no-upd-run-flow)
  also have ... = t1 x
  using S and T by (blast dest: no-upd-sources)
  finally have run-flow (flow (tl cfs2)) s x = t1 x .
}
ultimately show ∀ x.
  (s = t1
    (⊆ sources-aux (⟨bvars b⟩ # flow (tl cfs2)) s x) →
    (IF b THEN c1 ELSE c2, t1) →*
    (IF b THEN c1 ELSE c2, t1) ∧
    (c'' = SKIP) = (IF b THEN c1 ELSE c2 = SKIP)) ∧
  (s = t1
    (⊆ sources (⟨bvars b⟩ # flow (tl cfs2)) s x) →

```

```

      run-flow (flow (tl cfs2)) s x = t1 x)
    by blast
  qed
  qed
  qed blast
  qed
}
ultimately show ?thesis
using K and N by auto
qed
next
  assume bval b s and (c1, s) →*{tl cfs1} (c', s1)
  moreover from this and C and H and I have s ∈ Univ B1 (⊆ state ∩ X)
  by (drule-tac btyping2-approx [where s = s], auto)
  ultimately show ?thesis
  using A [of ?U' B1 C1 s tl cfs1 c' s1 cfs2 c'' s2] and G by simp
next
  assume ¬ bval b s and (c2, s) →*{tl cfs1} (c', s1)
  moreover from this and C and H and I have s ∈ Univ B2 (⊆ state ∩ X)
  by (drule-tac btyping2-approx [where s = s], auto)
  ultimately show ?thesis
  using B [of ?U' B1 C2 s tl cfs1 c' s1 cfs2 c'' s2] and G by simp
qed
qed

```

lemma *ctyping2-correct-aux-while*:

assumes

A: $\bigwedge B \ C' \ B' \ D' \ s \ c_1 \ c_2 \ s_1 \ s_2 \ cfs_1 \ cfs_2.$
 $B = B_1 \implies C' = C \implies B' = B_1' \implies$
 $(\forall s \in Univ? \ A \ X \cup Univ? \ C \ Y. \forall x \in bvars \ b. \text{All} \ (\text{interf } s \ (\text{dom } x))) \wedge$
 $(\forall p \in U. \text{case } p \text{ of } (B, W) \Rightarrow \forall s \in B. \forall x \in W. \text{All} \ (\text{interf } s \ (\text{dom } x))) \implies$
 $D = D' \implies \exists r \in B_1. \ s = r \ (\subseteq \text{state} \cap X) \implies$
 $(c, s) \rightarrow^*\{cfs_1\} (c_1, s_1) \implies (c_1, s_1) \rightarrow^*\{cfs_2\} (c_2, s_2) \implies$
 $\forall t_1. \exists c_2' \ t_2. \forall x.$
 $(s_1 = t_1 \ (\subseteq \text{sources-aux} \ (\text{flow } cfs_2) \ s_1 \ x) \longrightarrow$
 $(c_1, t_1) \rightarrow^* (c_2', t_2) \wedge (c_2 = \text{SKIP}) = (c_2' = \text{SKIP})) \wedge$
 $(s_1 = t_1 \ (\subseteq \text{sources} \ (\text{flow } cfs_2) \ s_1 \ x) \longrightarrow s_2 \ x = t_2 \ x) \text{ and}$
B: $\bigwedge B \ C' \ B' \ D'' \ s \ c_1 \ c_2 \ s_1 \ s_2 \ cfs_1 \ cfs_2.$
 $B = B_1 \implies C' = C \implies B' = B_1' \implies$
 $(\forall s \in Univ? \ A \ X \cup Univ? \ C \ Y. \forall x \in bvars \ b. \text{All} \ (\text{interf } s \ (\text{dom } x))) \wedge$
 $(\forall p \in U. \text{case } p \text{ of } (B, W) \Rightarrow \forall s \in B. \forall x \in W. \text{All} \ (\text{interf } s \ (\text{dom } x))) \implies$
 $D' = D'' \implies \exists r \in B_1'. \ s = r \ (\subseteq \text{state} \cap Y) \implies$
 $(c, s) \rightarrow^*\{cfs_1\} (c_1, s_1) \implies (c_1, s_1) \rightarrow^*\{cfs_2\} (c_2, s_2) \implies$
 $\forall t_1. \exists c_2' \ t_2. \forall x.$
 $(s_1 = t_1 \ (\subseteq \text{sources-aux} \ (\text{flow } cfs_2) \ s_1 \ x) \longrightarrow$
 $(c_1, t_1) \rightarrow^* (c_2', t_2) \wedge (c_2 = \text{SKIP}) = (c_2' = \text{SKIP})) \wedge$
 $(s_1 = t_1 \ (\subseteq \text{sources} \ (\text{flow } cfs_2) \ s_1 \ x) \longrightarrow s_2 \ x = t_2 \ x) \text{ and}$
C: $(\text{if } (\forall s \in Univ? \ A \ X \cup Univ? \ C \ Y. \forall x \in bvars \ b. \text{All} \ (\text{interf } s \ (\text{dom } x))) \wedge$
 $(\forall p \in U. \forall B \ W. \ p = (B, W) \longrightarrow (\forall s \in B. \forall x \in W. \text{All} \ (\text{interf } s \ (\text{dom } x))))$

then $\text{Some } (B_2 \cup B_2', \text{Univ}?? B_2 X \cap Y) \text{ else None} = \text{Some } (B, W)$ **and**
 $D: \models b (\subseteq A, X) = (B_1, B_2)$ **and**
 $E: \vdash c (\subseteq B_1, X) = (C, Y)$ **and**
 $F: \models b (\subseteq C, Y) = (B_1', B_2')$ **and**
 $G: (\{\}, \text{False}) \models c (\subseteq B_1, X) = \text{Some } (D, Z)$ **and**
 $H: (\{\}, \text{False}) \models c (\subseteq B_1', Y) = \text{Some } (D', Z')$
shows
 $\llbracket (\text{WHILE } b \text{ DO } c, s) \rightarrow^* \{cfs_1\} (c_1, s_1);$
 $(c_1, s_1) \rightarrow^* \{cfs_2\} (c_2, s_2);$
 $s \in \text{Univ } A (\subseteq \text{state} \cap X) \cup \text{Univ } C (\subseteq \text{state} \cap Y) \rrbracket \implies$
 $(\forall t_1. \exists c_2' t_2. \forall x.$
 $(s_1 = t_1 (\subseteq \text{sources-aux } (\text{flow } cfs_2) s_1 x) \longrightarrow$
 $(c_1, t_1) \rightarrow^* (c_2', t_2) \wedge (c_2 = \text{SKIP}) = (c_2' = \text{SKIP})) \wedge$
 $(s_1 = t_1 (\subseteq \text{sources } (\text{flow } cfs_2) s_1 x) \longrightarrow s_2 x = t_2 x)) \wedge$
 $(\forall x. (\exists p \in U. \text{case } p \text{ of } (B, W) \Rightarrow$
 $\exists s \in B. \exists y \in W. \neg s: \text{dom } y \rightsquigarrow \text{dom } x) \longrightarrow \text{no-upd } (\text{flow } cfs_2) x)$
proof (induction $cfs_1 @ cfs_2$ arbitrary: $cfs_1 cfs_2 s c_1 s_1$ rule: length-induct)
fix $cfs_1 cfs_2 s c_1 s_1$
assume
 $I: (\text{WHILE } b \text{ DO } c, s) \rightarrow^* \{cfs_1\} (c_1, s_1)$ **and**
 $J: (c_1, s_1) \rightarrow^* \{cfs_2\} (c_2, s_2)$
assume $\forall cfs. \text{length } cfs < \text{length } (cfs_1 @ cfs_2) \longrightarrow$
 $(\forall cfs_1 cfs_2. cfs = cfs_1 @ cfs_2 \longrightarrow$
 $(\forall s c_1 s_1. (\text{WHILE } b \text{ DO } c, s) \rightarrow^* \{cfs_1\} (c_1, s_1) \longrightarrow$
 $(c_1, s_1) \rightarrow^* \{cfs_2\} (c_2, s_2) \longrightarrow$
 $s \in \text{Univ } A (\subseteq \text{state} \cap X) \cup \text{Univ } C (\subseteq \text{state} \cap Y) \longrightarrow$
 $(\forall t_1. \exists c_2' t_2. \forall x.$
 $(s_1 = t_1 (\subseteq \text{sources-aux } (\text{flow } cfs_2) s_1 x) \longrightarrow$
 $(c_1, t_1) \rightarrow^* (c_2', t_2) \wedge (c_2 = \text{SKIP}) = (c_2' = \text{SKIP})) \wedge$
 $(s_1 = t_1 (\subseteq \text{sources } (\text{flow } cfs_2) s_1 x) \longrightarrow s_2 x = t_2 x)) \wedge$
 $(\forall x. (\exists (B, W) \in U. \exists s \in B. \exists y \in W. \neg s: \text{dom } y \rightsquigarrow \text{dom } x) \longrightarrow$
 $\text{no-upd } (\text{flow } cfs_2) x)))$
note $K = \text{this}$ [rule-format]
assume $L: s \in \text{Univ } A (\subseteq \text{state} \cap X) \cup \text{Univ } C (\subseteq \text{state} \cap Y)$
moreover {
fix s'
assume $s \in \text{Univ } A (\subseteq \text{state} \cap X)$ **and** $\text{bval } b s$
hence $N: s \in \text{Univ } B_1 (\subseteq \text{state} \cap X)$
using D **by** (drule-tac btyping2-approx, auto)
assume $(c, s) \Rightarrow s'$
hence $s' \in \text{Univ } D (\subseteq \text{state} \cap Z)$
using G **and** N **by** (rule ctyping2-approx)
moreover **have** $D \subseteq C \wedge Y \subseteq Z$
using E **and** G **by** (rule ctyping1-ctyping2)
ultimately **have** $s' \in \text{Univ } C (\subseteq \text{state} \cap Y)$
by blast
}
moreover {
fix s'

assume $s \in \text{Univ } C (\subseteq \text{state} \cap Y)$ and $\text{bval } b \ s$
 hence $N: s \in \text{Univ } B_1' (\subseteq \text{state} \cap Y)$
 using F by (*drule-tac btyping2-approx, auto*)
 assume $(c, s) \Rightarrow s'$
 hence $s' \in \text{Univ } D' (\subseteq \text{state} \cap Z')$
 using H and N by (*rule ctyping2-approx*)
 moreover obtain C' and Y' where $O: \vdash c (\subseteq B_1', Y) = (C', Y')$
 by (*cases $\vdash c (\subseteq B_1', Y)$, simp*)
 hence $D' \subseteq C' \wedge Y' \subseteq Z'$
 using H by (*rule ctyping1-ctyping2*)
 ultimately have $P: s' \in \text{Univ } C' (\subseteq \text{state} \cap Y')$
 by *blast*
 have $\vdash c (\subseteq C, Y) = (C, Y)$
 using E by (*rule ctyping1-idem*)
 moreover have $B_1' \subseteq C$
 using F by (*blast dest: btyping2-un-eq*)
 ultimately have $C' \subseteq C \wedge Y \subseteq Y'$
 by (*metis order-refl ctyping1-mono O*)
 hence $s' \in \text{Univ } C (\subseteq \text{state} \cap Y)$
 using P by *blast*
 }
 ultimately have M :
 $\forall s'. (c, s) \Rightarrow s' \longrightarrow \text{bval } b \ s \longrightarrow s' \in \text{Univ } C (\subseteq \text{state} \cap Y)$
 by *blast*
 have N :
 $(\forall s \in \text{Univ? } A \ X \cup \text{Univ? } C \ Y. \forall x \in \text{bvars } b. \text{All } (\text{interf } s (\text{dom } x))) \wedge$
 $(\forall p \in U. \forall B \ W. p = (B, W) \longrightarrow (\forall s \in B. \forall x \in W. \text{All } (\text{interf } s (\text{dom } x))))$
 using C by (*simp split: if-split-asm*)
 hence $\forall cs \ x. (\exists (B, Y) \in U.$
 $\exists s \in B. \exists y \in Y. \neg s: \text{dom } y \rightsquigarrow \text{dom } x) \longrightarrow \text{no-upd } cs \ x$
 by *auto*
 moreover {
 fix $r \ t_1$
 assume $O: r \in A$ and $P: s = r (\subseteq \text{state} \cap X)$
 have $Q: \forall x. \forall y \in \text{bvars } b. s: \text{dom } y \rightsquigarrow \text{dom } x$
 proof (*cases state $\subseteq X$*)
 case *True*
 with P have $\text{interf } s = \text{interf } r$
 by (*blast intro: interf-state*)
 with N and O show *?thesis*
 by (*erule-tac conjE, drule-tac bspec, auto simp: univ-states-if-def*)
 next
 case *False*
 with N and O show *?thesis*
 by (*erule-tac conjE, drule-tac bspec, auto simp: univ-states-if-def*)
 qed
 have $(c_1, s_1) = (\text{WHILE } b \text{ DO } c, s) \vee$

$(IF\ b\ THEN\ c;;\ WHILE\ b\ DO\ c\ ELSE\ SKIP,\ s) \rightarrow^*\{tl\ cfs_1\} (c_1,\ s_1)$
using I **by** (*blast dest: small-stepsl-while*)
hence $\exists c_2' t_2. \forall x.$
 $(s_1 = t_1 (\subseteq sources\text{-}aux\ (flow\ cfs_2)\ s_1\ x) \longrightarrow$
 $(c_1,\ t_1) \rightarrow^* (c_2',\ t_2) \wedge (c_2 = SKIP) = (c_2' = SKIP)) \wedge$
 $(s_1 = t_1 (\subseteq sources\ (flow\ cfs_2)\ s_1\ x) \longrightarrow s_2\ x = t_2\ x)$
proof
assume $R: (c_1,\ s_1) = (WHILE\ b\ DO\ c,\ s)$
hence $(WHILE\ b\ DO\ c,\ s) \rightarrow^*\{cfs_2\} (c_2,\ s_2)$
using J **by** *simp*
hence
 $(c_2,\ s_2) = (WHILE\ b\ DO\ c,\ s) \wedge$
 $flow\ cfs_2 = [] \vee$
 $(IF\ b\ THEN\ c;;\ WHILE\ b\ DO\ c\ ELSE\ SKIP,\ s) \rightarrow^*\{tl\ cfs_2\} (c_2,\ s_2) \wedge$
 $flow\ cfs_2 = flow\ (tl\ cfs_2)$
(is $?P \vee ?Q \wedge ?R)$
by (*rule small-stepsl-while*)
thus *?thesis*
proof (*rule disjE, erule-tac [2] conjE*)
assume $?P$
with R **show** *?thesis*
by *auto*
next
assume $?Q$ **and** $?R$
have
 $(c_2,\ s_2) = (IF\ b\ THEN\ c;;\ WHILE\ b\ DO\ c\ ELSE\ SKIP,\ s) \wedge$
 $flow\ (tl\ cfs_2) = [] \vee$
 $bval\ b\ s \wedge (c;;\ WHILE\ b\ DO\ c,\ s) \rightarrow^*\{tl2\ cfs_2\} (c_2,\ s_2) \wedge$
 $flow\ (tl\ cfs_2) = \langle bvars\ b \rangle \# flow\ (tl2\ cfs_2) \vee$
 $\neg\ bval\ b\ s \wedge (SKIP,\ s) \rightarrow^*\{tl2\ cfs_2\} (c_2,\ s_2) \wedge$
 $flow\ (tl\ cfs_2) = \langle bvars\ b \rangle \# flow\ (tl2\ cfs_2)$
using $\langle ?Q \rangle$ **by** (*rule small-stepsl-if*)
thus *?thesis*
proof (*erule-tac disjE, erule-tac [2] disjE, (erule-tac [2-3] conjE)+*)
assume $(c_2,\ s_2) = (IF\ b\ THEN\ c;;\ WHILE\ b\ DO\ c\ ELSE\ SKIP,\ s) \wedge$
 $flow\ (tl\ cfs_2) = []$
with R **and** $\langle ?R \rangle$ **show** *?thesis*
by *auto*
next
assume $S: bval\ b\ s$
with D **and** O **and** P **have** $T: s \in Univ\ B_1 (\subseteq state \cap X)$
by (*erule-tac btyping2-approx [where s = s], auto*)
assume $U: (c;;\ WHILE\ b\ DO\ c,\ s) \rightarrow^*\{tl2\ cfs_2\} (c_2,\ s_2)$
hence
 $(\exists c'\ cfs.\ c_2 = c';\ WHILE\ b\ DO\ c \wedge$
 $(c,\ s) \rightarrow^*\{cfs\} (c',\ s_2) \wedge$
 $flow\ (tl2\ cfs_2) = flow\ cfs) \vee$
 $(\exists s'\ cfs\ cfs'.\ length\ cfs' < length\ (tl2\ cfs_2) \wedge$
 $(c,\ s) \rightarrow^*\{cfs\} (SKIP,\ s') \wedge$

$(WHILE\ b\ DO\ c,\ s') \rightarrow^*\{cfs'\} (c_2,\ s_2) \wedge$
 $flow\ (tl2\ cfs_2) = flow\ cfs\ @\ flow\ cfs'$
by (rule *small-stepsl-seq*)
moreover assume $flow\ (tl\ cfs_2) = \langle bvars\ b \rangle \# flow\ (tl2\ cfs_2)$
moreover have $s_2 = run-flow\ (flow\ (tl2\ cfs_2))\ s$
using U **by** (rule *small-stepsl-run-flow*)
moreover {
fix $c'\ cfs$
assume $(c,\ s) \rightarrow^*\{cfs\} (c',\ run-flow\ (flow\ cfs)\ s)$
then obtain c_2' **and** t_2 **where** $V: \forall x.$
 $(s = t_1 (\subseteq sources-aux\ (flow\ cfs)\ s\ x) \rightarrow$
 $(c,\ t_1) \rightarrow^* (c_2',\ t_2) \wedge (c' = SKIP) = (c_2' = SKIP)) \wedge$
 $(s = t_1 (\subseteq sources\ (flow\ cfs)\ s\ x) \rightarrow$
 $run-flow\ (flow\ cfs)\ s\ x = t_2\ x)$
using $A\ [of\ B_1\ C\ B_1'\ D\ s\ \Box\ c\ s\ cfs\ c'$
 $run-flow\ (flow\ cfs)\ s]$ **and** N **and** T **by force**
{
fix x
assume $W: s = t_1 (\subseteq sources-aux\ (\langle bvars\ b \rangle \# flow\ cfs)\ s\ x)$
moreover have $sources-aux\ (flow\ cfs)\ s\ x \subseteq$
 $sources-aux\ (\langle bvars\ b \rangle \# (flow\ cfs))\ s\ x$
by (rule *sources-aux-observe-tl*)
ultimately have $(c,\ t_1) \rightarrow^* (c_2',\ t_2)$
using V **by blast**
hence $(c;;\ WHILE\ b\ DO\ c,\ t_1) \rightarrow^* (c_2';;\ WHILE\ b\ DO\ c,\ t_2)$
by (rule *star-seq2*)
moreover have $s = t_1 (\subseteq bvars\ b)$
using Q **and** W **by** (blast *dest: sources-aux-observe-hd*)
hence $bval\ b\ t_1$
using S **by** (blast *dest: bvars-bval*)
hence $(WHILE\ b\ DO\ c,\ t_1) \rightarrow^* (c;;\ WHILE\ b\ DO\ c,\ t_1)$
by (blast *intro: star-trans*)
ultimately have $(WHILE\ b\ DO\ c,\ t_1) \rightarrow^*$
 $(c_2';;\ WHILE\ b\ DO\ c,\ t_2) \wedge c_2';;\ WHILE\ b\ DO\ c \neq SKIP$
by (blast *intro: star-trans*)
}
moreover {
fix x
assume $s = t_1 (\subseteq sources\ (\langle bvars\ b \rangle \# flow\ cfs)\ s\ x)$
moreover have $sources\ (flow\ cfs)\ s\ x \subseteq$
 $sources\ (\langle bvars\ b \rangle \# (flow\ cfs))\ s\ x$
by (rule *sources-observe-tl*)
ultimately have $run-flow\ (flow\ cfs)\ s\ x = t_2\ x$
using V **by blast**
}
ultimately have $\exists c_2'\ t_2.\ \forall x.$
 $(s = t_1 (\subseteq sources-aux\ (\langle bvars\ b \rangle \# flow\ cfs)\ s\ x) \rightarrow$
 $(WHILE\ b\ DO\ c,\ t_1) \rightarrow^* (c_2',\ t_2) \wedge c_2' \neq SKIP) \wedge$
 $(s = t_1 (\subseteq sources\ (\langle bvars\ b \rangle \# flow\ cfs)\ s\ x) \rightarrow$

$run_flow (flow\ cfs)\ s\ x = t_2\ x)$
 by *blast*
 }
 moreover {
 fix $s'\ cfs\ cfs'$
 assume
 $V: length\ cfs' < length\ cfs_2 - Suc\ (Suc\ 0)$ and
 $W: (c, s) \rightarrow^* \{cfs\}\ (SKIP, s')$ and
 $X: (WHILE\ b\ DO\ c, s') \rightarrow^* \{cfs'\}$
 $(c_2, run_flow (flow\ cfs') (run_flow (flow\ cfs)\ s))$
 then obtain c_2' and t_2 where $\forall x.$
 $(s = t_1 (\subseteq sources_aux (flow\ cfs)\ s\ x) \longrightarrow$
 $(c, t_1) \rightarrow^* (c_2', t_2) \wedge (SKIP = SKIP) = (c_2' = SKIP)) \wedge$
 $(s = t_1 (\subseteq sources (flow\ cfs)\ s\ x) \longrightarrow s'\ x = t_2\ x)$
 using $A [of\ B_1\ C\ B_1'\ D\ s\ []\ c\ s\ cfs\ SKIP\ s']$
 and N and T by *force*
 moreover have $Y: s' = run_flow (flow\ cfs)\ s$
 using W by *(rule small-steps-l-run-flow)*
 ultimately have $Z: \forall x.$
 $(s = t_1 (\subseteq sources_aux (flow\ cfs)\ s\ x) \longrightarrow$
 $(c, t_1) \rightarrow^* (SKIP, t_2)) \wedge$
 $(s = t_1 (\subseteq sources (flow\ cfs)\ s\ x) \longrightarrow$
 $run_flow (flow\ cfs)\ s\ x = t_2\ x)$
 by *blast*
 assume $s_2 = run_flow (flow\ cfs') (run_flow (flow\ cfs)\ s)$
 moreover have $(c, s) \Rightarrow s'$
 using W by *(auto dest: small-steps-l-steps simp: big-iff-small)*
 hence $s' \in Univ\ C (\subseteq state \cap Y)$
 using M and S by *blast*
 ultimately obtain c_3' and t_3 where $AA: \forall x.$
 $(run_flow (flow\ cfs)\ s = t_2$
 $(\subseteq sources_aux (flow\ cfs') (run_flow (flow\ cfs)\ s)\ x) \longrightarrow$
 $(WHILE\ b\ DO\ c, t_2) \rightarrow^* (c_3', t_3) \wedge$
 $(c_2 = SKIP) = (c_3' = SKIP)) \wedge$
 $(run_flow (flow\ cfs)\ s = t_2$
 $(\subseteq sources (flow\ cfs') (run_flow (flow\ cfs)\ s)\ x) \longrightarrow$
 $run_flow (flow\ cfs') (run_flow (flow\ cfs)\ s)\ x = t_3\ x)$
 using $K [of\ cfs'\ []\ cfs'\ s'\ WHILE\ b\ DO\ c\ s']$
 and V and X and Y by *force*
 {
 fix x
 assume $AB: s = t_1$
 $(\subseteq sources_aux (\langle bvars\ b \rangle \# flow\ cfs @ flow\ cfs')\ s\ x)$
 moreover have $sources_aux (flow\ cfs)\ s\ x \subseteq$
 $sources_aux (flow\ cfs @ flow\ cfs')\ s\ x$
 by *(rule sources_aux-append)*
 moreover have $AC: sources_aux (flow\ cfs @ flow\ cfs')\ s\ x \subseteq$
 $sources_aux (\langle bvars\ b \rangle \# flow\ cfs @ flow\ cfs')\ s\ x$
 by *(rule sources_aux-observe-tl)*

ultimately have $(c, t_1) \rightarrow^* (SKIP, t_2)$
 using Z by *blast*
 hence $(c;; WHILE\ b\ DO\ c, t_1) \rightarrow^* (SKIP;; WHILE\ b\ DO\ c, t_2)$
 by (rule *star-seq2*)
 moreover have $s = t_1 (\subseteq bvars\ b)$
 using Q and AB by (blast dest: *sources-aux-observe-hd*)
 hence $bval\ b\ t_1$
 using S by (blast dest: *bvars-bval*)
 hence $(WHILE\ b\ DO\ c, t_1) \rightarrow^* (c;; WHILE\ b\ DO\ c, t_1)$
 by (blast intro: *star-trans*)
 ultimately have $(WHILE\ b\ DO\ c, t_1) \rightarrow^* (WHILE\ b\ DO\ c, t_2)$
 by (blast intro: *star-trans*)
 moreover have $run_flow\ (flow\ cfs)\ s = t_2$
 $(\subseteq sources_aux\ (flow\ cfs')\ (run_flow\ (flow\ cfs)\ s)\ x)$
 proof
 fix y
 assume $y \in sources_aux\ (flow\ cfs')$
 $(run_flow\ (flow\ cfs)\ s)\ x$
 hence $sources\ (flow\ cfs)\ s\ y \subseteq$
 $sources_aux\ (flow\ cfs\ @\ flow\ cfs')\ s\ x$
 by (rule *sources-aux-member*)
 hence $sources\ (flow\ cfs)\ s\ y \subseteq$
 $sources_aux\ (\langle bvars\ b \rangle \# flow\ cfs\ @\ flow\ cfs')\ s\ x$
 using AC by *simp*
 thus $run_flow\ (flow\ cfs)\ s\ y = t_2\ y$
 using Z and AB by *blast*
 qed
 hence $(WHILE\ b\ DO\ c, t_2) \rightarrow^* (c_3', t_3) \wedge$
 $(c_2 = SKIP) = (c_3' = SKIP)$
 using AA by *simp*
 ultimately have $(WHILE\ b\ DO\ c, t_1) \rightarrow^* (c_3', t_3) \wedge$
 $(c_2 = SKIP) = (c_3' = SKIP)$
 by (blast intro: *star-trans*)
 }
 moreover {
 fix x
 assume $AB: s = t_1$
 $(\subseteq sources\ (\langle bvars\ b \rangle \# flow\ cfs\ @\ flow\ cfs')\ s\ x)$
 have $run_flow\ (flow\ cfs)\ s = t_2$
 $(\subseteq sources\ (flow\ cfs')\ (run_flow\ (flow\ cfs)\ s)\ x)$
 proof
 fix y
 assume $y \in sources\ (flow\ cfs')$
 $(run_flow\ (flow\ cfs)\ s)\ x$
 hence $sources\ (flow\ cfs)\ s\ y \subseteq$
 $sources\ (flow\ cfs\ @\ flow\ cfs')\ s\ x$
 by (rule *sources-member*)
 moreover have $sources\ (flow\ cfs\ @\ flow\ cfs')\ s\ x \subseteq$
 $sources\ (\langle bvars\ b \rangle \# flow\ cfs\ @\ flow\ cfs')\ s\ x$

```

    by (rule sources-observe-tl)
  ultimately have sources (flow cfs) s y  $\subseteq$ 
    sources ( $\langle$ bvars b $\rangle$  # flow cfs @ flow cfs') s x
  by simp
  thus run-flow (flow cfs) s y = t2 y
  using Z and AB by blast
qed
hence run-flow (flow cfs') (run-flow (flow cfs) s) x = t3 x
  using AA by simp
}
ultimately have  $\exists c_3' t_3. \forall x.$ 
  (s = t1
    ( $\subseteq$  sources-aux ( $\langle$ bvars b $\rangle$  # flow cfs @ flow cfs') s x)  $\longrightarrow$ 
      (WHILE b DO c, t1)  $\rightarrow^*$  (c3', t3)  $\wedge$ 
      (c2 = SKIP) = (c3' = SKIP))  $\wedge$ 
  (s = t1
    ( $\subseteq$  sources ( $\langle$ bvars b $\rangle$  # flow cfs @ flow cfs') s x)  $\longrightarrow$ 
      run-flow (flow cfs') (run-flow (flow cfs) s) x = t3 x)
  by auto
}
ultimately show ?thesis
  using R and  $\langle ?R \rangle$  by (auto simp: run-flow-append)
next
assume
  S:  $\neg$  bval b s and
  T: flow (tl cfs2) =  $\langle$ bvars b $\rangle$  # flow (tl2 cfs2)
moreover assume (SKIP, s)  $\rightarrow^*\{tl2 cfs_2\}$  (c2, s2)
hence U: (c2, s2) = (SKIP, s)  $\wedge$  flow (tl2 cfs2) = []
  by (rule small-steps-skip)
show ?thesis
proof (rule exI [of - SKIP], rule exI [of - t1])
{
  fix x
  have (WHILE b DO c, t1)  $\rightarrow$ 
    (IF b THEN c;; WHILE b DO c ELSE SKIP, t1) ..
  moreover assume s = t1 ( $\subseteq$  sources-aux [ $\langle$ bvars b $\rangle$ ] s x)
  hence s = t1 ( $\subseteq$  bvars b)
  using Q by (blast dest: sources-aux-observe-hd)
  hence  $\neg$  bval b t1
  using S by (blast dest: bvars-bval)
  hence (IF b THEN c;; WHILE b DO c ELSE SKIP, t1)  $\rightarrow$ 
    (SKIP, t1) ..
  ultimately have (WHILE b DO c, t1)  $\rightarrow^*$  (SKIP, t1)
  by (blast intro: star-trans)
}
moreover {
  fix x
  assume s = t1 ( $\subseteq$  sources [ $\langle$ bvars b $\rangle$ ] s x)
  hence s x = t1 x

```

```

    by (subst (asm) append-Nil [symmetric],
        simp only: sources.simps, auto)
  }
  ultimately show  $\forall x.$ 
    ( $s_1 = t_1 (\subseteq \text{sources-aux } (\text{flow } cfs_2) s_1 x) \longrightarrow$ 
      ( $c_1, t_1 \rightarrow^* (\text{SKIP}, t_1) \wedge (c_2 = \text{SKIP}) = (\text{SKIP} = \text{SKIP})) \wedge$ 
      ( $s_1 = t_1 (\subseteq \text{sources } (\text{flow } cfs_2) s_1 x) \longrightarrow s_2 x = t_1 x$ )
    ) using R and T and U and  $\langle ?R \rangle$  by auto
  qed
qed
qed
next
assume (IF b THEN c;; WHILE b DO c ELSE SKIP, s)  $\rightarrow^*\{tl\ cfs_1\} (c_1, s_1)$ 
hence
  ( $c_1, s_1 = (\text{IF } b \text{ THEN } c;; \text{ WHILE } b \text{ DO } c \text{ ELSE SKIP}, s) \wedge$ 
     $\text{flow } (tl\ cfs_1) = [] \vee$ 
     $bval\ b\ s \wedge (c;; \text{ WHILE } b \text{ DO } c, s) \rightarrow^*\{tl2\ cfs_1\} (c_1, s_1) \wedge$ 
     $\text{flow } (tl\ cfs_1) = \langle bvars\ b \rangle \# \text{flow } (tl2\ cfs_1) \vee$ 
     $\neg bval\ b\ s \wedge (\text{SKIP}, s) \rightarrow^*\{tl2\ cfs_1\} (c_1, s_1) \wedge$ 
     $\text{flow } (tl\ cfs_1) = \langle bvars\ b \rangle \# \text{flow } (tl2\ cfs_1)$ 
  ) by (rule small-steps-l-if)
thus ?thesis
proof (rule disjE, erule-tac [2] disjE, erule-tac conjE,
  (erule-tac [2-3] conjE)+)
  assume R: ( $c_1, s_1 = (\text{IF } b \text{ THEN } c;; \text{ WHILE } b \text{ DO } c \text{ ELSE SKIP}, s)$ )
  hence (IF b THEN c;; WHILE b DO c ELSE SKIP, s)  $\rightarrow^*\{cfs_2\} (c_2, s_2)$ 
    using J by simp
  hence
    ( $c_2, s_2 = (\text{IF } b \text{ THEN } c;; \text{ WHILE } b \text{ DO } c \text{ ELSE SKIP}, s) \wedge$ 
       $\text{flow } cfs_2 = [] \vee$ 
       $bval\ b\ s \wedge (c;; \text{ WHILE } b \text{ DO } c, s) \rightarrow^*\{tl\ cfs_2\} (c_2, s_2) \wedge$ 
       $\text{flow } cfs_2 = \langle bvars\ b \rangle \# \text{flow } (tl\ cfs_2) \vee$ 
       $\neg bval\ b\ s \wedge (\text{SKIP}, s) \rightarrow^*\{tl\ cfs_2\} (c_2, s_2) \wedge$ 
       $\text{flow } cfs_2 = \langle bvars\ b \rangle \# \text{flow } (tl\ cfs_2)$ 
    ) by (rule small-steps-l-if)
  thus ?thesis
proof (erule-tac disjE, erule-tac [2] disjE, (erule-tac [2-3] conjE)+)
  assume ( $c_2, s_2 = (\text{IF } b \text{ THEN } c;; \text{ WHILE } b \text{ DO } c \text{ ELSE SKIP}, s) \wedge$ 
     $\text{flow } cfs_2 = []$ 
  )
  with R show ?thesis
    by auto
next
assume S:  $bval\ b\ s$ 
with D and O and P have T:  $s \in Univ\ B_1 (\subseteq \text{state} \cap X)$ 
  by (drule-tac btyping2-approx [where s = s], auto)
assume U: ( $c;; \text{ WHILE } b \text{ DO } c, s) \rightarrow^*\{tl\ cfs_2\} (c_2, s_2)$ 
hence
  ( $\exists c' cfs. c_2 = c'; \text{ WHILE } b \text{ DO } c \wedge$ 
    ( $c, s) \rightarrow^*\{cfs\} (c', s_2) \wedge$ 
  )

```

$flow\ (tl\ cfs_2) = flow\ cfs) \vee$
 $(\exists s' cfs\ cfs'.\ length\ cfs' < length\ (tl\ cfs_2) \wedge$
 $(c, s) \rightarrow^*\{cfs\}\ (SKIP, s') \wedge$
 $(WHILE\ b\ DO\ c, s') \rightarrow^*\{cfs'\}\ (c_2, s_2) \wedge$
 $flow\ (tl\ cfs_2) = flow\ cfs\ @\ flow\ cfs')$
by (rule *small-steps-l-seq*)
moreover assume $flow\ cfs_2 = \langle bvars\ b \rangle \# flow\ (tl\ cfs_2)$
moreover have $s_2 = run-flow\ (flow\ (tl\ cfs_2))\ s$
using U **by** (rule *small-steps-l-run-flow*)
moreover {
fix $c'\ cfs$
assume $(c, s) \rightarrow^*\{cfs\}\ (c', run-flow\ (flow\ cfs)\ s)$
then obtain c_2' **and** t_2 **where** $V: \forall x.$
 $(s = t_1 (\subseteq sources_aux\ (flow\ cfs)\ s\ x) \longrightarrow$
 $(c, t_1) \rightarrow^* (c_2', t_2) \wedge (c' = SKIP) = (c_2' = SKIP)) \wedge$
 $(s = t_1 (\subseteq sources\ (flow\ cfs)\ s\ x) \longrightarrow$
 $run-flow\ (flow\ cfs)\ s\ x = t_2\ x)$
using A [of $B_1\ C\ B_1'\ D\ s\ []\ c\ s\ cfs\ c'$
 $run-flow\ (flow\ cfs)\ s]$ **and** N **and** T **by force**
{
fix x
assume $W: s = t_1 (\subseteq sources_aux\ (\langle bvars\ b \rangle \# flow\ cfs)\ s\ x)$
moreover have $sources_aux\ (flow\ cfs)\ s\ x \subseteq$
 $sources_aux\ (\langle bvars\ b \rangle \# (flow\ cfs))\ s\ x$
by (rule *sources-aux-observe-tl*)
ultimately have $(c, t_1) \rightarrow^* (c_2', t_2)$
using V **by blast**
hence $(c;; WHILE\ b\ DO\ c, t_1) \rightarrow^* (c_2';; WHILE\ b\ DO\ c, t_2)$
by (rule *star-seq2*)
moreover have $s = t_1 (\subseteq bvars\ b)$
using Q **and** W **by** (blast *dest: sources-aux-observe-hd*)
hence $bval\ b\ t_1$
using S **by** (blast *dest: bvars-bval*)
hence $(IF\ b\ THEN\ c;; WHILE\ b\ DO\ c\ ELSE\ SKIP, t_1) \rightarrow$
 $(c;; WHILE\ b\ DO\ c, t_1) ..$
ultimately have
 $(IF\ b\ THEN\ c;; WHILE\ b\ DO\ c\ ELSE\ SKIP, t_1) \rightarrow^*$
 $(c_2';; WHILE\ b\ DO\ c, t_2) \wedge c_2';; WHILE\ b\ DO\ c \neq SKIP$
by (blast *intro: star-trans*)
}
moreover {
fix x
assume $s = t_1 (\subseteq sources\ (\langle bvars\ b \rangle \# flow\ cfs)\ s\ x)$
moreover have $sources\ (flow\ cfs)\ s\ x \subseteq$
 $sources\ (\langle bvars\ b \rangle \# (flow\ cfs))\ s\ x$
by (rule *sources-observe-tl*)
ultimately have $run-flow\ (flow\ cfs)\ s\ x = t_2\ x$
using V **by blast**
}

ultimately have $\exists c_2' t_2. \forall x.$
 $(s = t_1 (\subseteq \text{sources-aux } (\langle \text{bvars } b \rangle \# \text{flow cfs}) s x) \longrightarrow$
 $(\text{IF } b \text{ THEN } c;; \text{ WHILE } b \text{ DO } c \text{ ELSE SKIP}, t_1) \rightarrow^* (c_2', t_2) \wedge$
 $c_2' \neq \text{SKIP}) \wedge$
 $(s = t_1 (\subseteq \text{sources } (\langle \text{bvars } b \rangle \# \text{flow cfs}) s x) \longrightarrow$
 $\text{run-flow } (\text{flow cfs}) s x = t_2 x)$
by blast
}
moreover {
fix $s' \text{ cfs cfs'}$
assume
 $V: \text{length cfs}' < \text{length cfs}_2 - \text{Suc } 0 \text{ and}$
 $W: (c, s) \rightarrow^* \{\text{cfs}\} (\text{SKIP}, s') \text{ and}$
 $X: (\text{WHILE } b \text{ DO } c, s') \rightarrow^* \{\text{cfs}'\}$
 $(c_2, \text{run-flow } (\text{flow cfs}') (\text{run-flow } (\text{flow cfs}) s))$
then obtain c_2' **and** t_2 **where** $\forall x.$
 $(s = t_1 (\subseteq \text{sources-aux } (\text{flow cfs}) s x) \longrightarrow$
 $(c, t_1) \rightarrow^* (c_2', t_2) \wedge (\text{SKIP} = \text{SKIP}) = (c_2' = \text{SKIP})) \wedge$
 $(s = t_1 (\subseteq \text{sources } (\text{flow cfs}) s x) \longrightarrow s' x = t_2 x)$
using $A \text{ [of } B_1 \ C \ B_1' \ D \ s \] \ c \ s \ \text{cfs} \ \text{SKIP} \ s']$
and N **and** T **by force**
moreover have $Y: s' = \text{run-flow } (\text{flow cfs}) s$
using W **by** $(\text{rule small-stepsl-run-flow})$
ultimately have $Z: \forall x.$
 $(s = t_1 (\subseteq \text{sources-aux } (\text{flow cfs}) s x) \longrightarrow$
 $(c, t_1) \rightarrow^* (\text{SKIP}, t_2)) \wedge$
 $(s = t_1 (\subseteq \text{sources } (\text{flow cfs}) s x) \longrightarrow$
 $\text{run-flow } (\text{flow cfs}) s x = t_2 x)$
by blast
assume $s_2 = \text{run-flow } (\text{flow cfs}') (\text{run-flow } (\text{flow cfs}) s)$
moreover have $(c, s) \Rightarrow s'$
using W **by** $(\text{auto dest: small-stepsl-steps simp: big-iff-small})$
hence $s' \in \text{Univ } C (\subseteq \text{state} \cap Y)$
using M **and** S **by blast**
ultimately obtain c_3' **and** t_3 **where** $AA: \forall x.$
 $(\text{run-flow } (\text{flow cfs}) s = t_2$
 $(\subseteq \text{sources-aux } (\text{flow cfs}') (\text{run-flow } (\text{flow cfs}) s) x) \longrightarrow$
 $(\text{WHILE } b \text{ DO } c, t_2) \rightarrow^* (c_3', t_3) \wedge$
 $(c_2 = \text{SKIP}) = (c_3' = \text{SKIP})) \wedge$
 $(\text{run-flow } (\text{flow cfs}) s = t_2$
 $(\subseteq \text{sources } (\text{flow cfs}') (\text{run-flow } (\text{flow cfs}) s) x) \longrightarrow$
 $\text{run-flow } (\text{flow cfs}') (\text{run-flow } (\text{flow cfs}) s) x = t_3 x)$
using $K \text{ [of cfs'] cfs' s' WHILE } b \text{ DO } c \ s']$
and V **and** X **and** Y **by force**
{
fix x
assume $AB: s = t_1$
 $(\subseteq \text{sources-aux } (\langle \text{bvars } b \rangle \# \text{flow cfs} @ \text{flow cfs}') s x)$
moreover have $\text{sources-aux } (\text{flow cfs}) s x \subseteq$

sources-aux (*flow cfs* @ *flow cfs'*) *s x*
 by (*rule sources-aux-append*)
moreover have *AC*: *sources-aux* (*flow cfs* @ *flow cfs'*) *s x* \subseteq
sources-aux ($\langle \text{bvars } b \rangle \# \text{flow cfs @ flow cfs'} \rangle$ *s x*
 by (*rule sources-aux-observe-tl*)
ultimately have (*c*, *t*₁) \rightarrow^* (*SKIP*, *t*₂)
 using *Z* by *blast*
hence (*c*;; *WHILE* *b* *DO* *c*, *t*₁) \rightarrow^* (*SKIP*;; *WHILE* *b* *DO* *c*, *t*₂)
 by (*rule star-seq2*)
moreover have *s* = *t*₁ (\subseteq *bvars b*)
 using *Q* and *AB* by (*blast dest: sources-aux-observe-hd*)
hence *bval* *b* *t*₁
 using *S* by (*blast dest: bvars-bval*)
hence (*IF* *b* *THEN* *c*;; *WHILE* *b* *DO* *c* *ELSE* *SKIP*, *t*₁) \rightarrow
 (*c*;; *WHILE* *b* *DO* *c*, *t*₁) ..
ultimately have (*IF* *b* *THEN* *c*;; *WHILE* *b* *DO* *c* *ELSE* *SKIP*, *t*₁) \rightarrow^*
 (*WHILE* *b* *DO* *c*, *t*₂)
 by (*blast intro: star-trans*)
moreover have *run-flow* (*flow cfs*) *s* = *t*₂
 (\subseteq *sources-aux* (*flow cfs'*) (*run-flow* (*flow cfs*) *s*) *x*)
proof
 fix *y*
assume *y* \in *sources-aux* (*flow cfs'*)
 (*run-flow* (*flow cfs*) *s*) *x*
hence *sources* (*flow cfs*) *s y* \subseteq
sources-aux (*flow cfs* @ *flow cfs'*) *s x*
 by (*rule sources-aux-member*)
hence *sources* (*flow cfs*) *s y* \subseteq
sources-aux ($\langle \text{bvars } b \rangle \# \text{flow cfs @ flow cfs'} \rangle$ *s x*
 using *AC* by *simp*
thus *run-flow* (*flow cfs*) *s y* = *t*₂ *y*
 using *Z* and *AB* by *blast*
qed
hence (*WHILE* *b* *DO* *c*, *t*₂) \rightarrow^* (*c*₃', *t*₃) \wedge
 (*c*₂ = *SKIP*) = (*c*₃' = *SKIP*)
 using *AA* by *simp*
ultimately have
 (*IF* *b* *THEN* *c*;; *WHILE* *b* *DO* *c* *ELSE* *SKIP*, *t*₁) \rightarrow^*
 (*c*₃', *t*₃) \wedge (*c*₂ = *SKIP*) = (*c*₃' = *SKIP*)
 by (*blast intro: star-trans*)
}
moreover {
 fix *x*
assume *AB*: *s* = *t*₁
 (\subseteq *sources* ($\langle \text{bvars } b \rangle \# \text{flow cfs @ flow cfs'} \rangle$ *s x*)
have *run-flow* (*flow cfs*) *s* = *t*₂
 (\subseteq *sources* (*flow cfs'*) (*run-flow* (*flow cfs*) *s*) *x*)
proof
 fix *y*

```

assume  $y \in \text{sources } (\text{flow } cfs')$ 
   $(\text{run-flow } (\text{flow } cfs) \ s) \ x$ 
hence  $\text{sources } (\text{flow } cfs) \ s \ y \subseteq$ 
   $\text{sources } (\text{flow } cfs \ @ \ \text{flow } cfs') \ s \ x$ 
by  $(\text{rule sources-member})$ 
moreover have  $\text{sources } (\text{flow } cfs \ @ \ \text{flow } cfs') \ s \ x \subseteq$ 
   $\text{sources } (\langle \text{bvars } b \rangle \# \text{flow } cfs \ @ \ \text{flow } cfs') \ s \ x$ 
by  $(\text{rule sources-observe-tl})$ 
ultimately have  $\text{sources } (\text{flow } cfs) \ s \ y \subseteq$ 
   $\text{sources } (\langle \text{bvars } b \rangle \# \text{flow } cfs \ @ \ \text{flow } cfs') \ s \ x$ 
by  $\text{simp}$ 
thus  $\text{run-flow } (\text{flow } cfs) \ s \ y = t_2 \ y$ 
using  $Z$  and  $AB$  by  $\text{blast}$ 
qed
hence  $\text{run-flow } (\text{flow } cfs') \ (\text{run-flow } (\text{flow } cfs) \ s) \ x = t_3 \ x$ 
using  $AA$  by  $\text{simp}$ 
}
ultimately have  $\exists c_3' \ t_3. \forall x.$ 
   $(s = t_1$ 
     $(\subseteq \text{sources-aux } (\langle \text{bvars } b \rangle \# \text{flow } cfs \ @ \ \text{flow } cfs') \ s \ x) \longrightarrow$ 
     $(\text{IF } b \ \text{THEN } c;; \ \text{WHILE } b \ \text{DO } c \ \text{ELSE } \text{SKIP}, \ t_1) \rightarrow^* (c_3', \ t_3) \wedge$ 
     $(c_2 = \text{SKIP}) = (c_3' = \text{SKIP})) \wedge$ 
   $(s = t_1$ 
     $(\subseteq \text{sources } (\langle \text{bvars } b \rangle \# \text{flow } cfs \ @ \ \text{flow } cfs') \ s \ x) \longrightarrow$ 
     $\text{run-flow } (\text{flow } cfs') \ (\text{run-flow } (\text{flow } cfs) \ s) \ x = t_3 \ x)$ 
  by  $\text{auto}$ 
}
ultimately show  $?thesis$ 
using  $R$  by  $(\text{auto simp: run-flow-append})$ 
next
assume
   $S: \neg \text{bval } b \ s$  and
   $T: \text{flow } cfs_2 = \langle \text{bvars } b \rangle \# \text{flow } (tl \ cfs_2)$ 
assume  $(\text{SKIP}, \ s) \rightarrow^* \{tl \ cfs_2\} \ (c_2, \ s_2)$ 
hence  $U: (c_2, \ s_2) = (\text{SKIP}, \ s) \wedge \text{flow } (tl \ cfs_2) = []$ 
by  $(\text{rule small-steps1-skip})$ 
show  $?thesis$ 
proof  $(\text{rule exI } [of \ - \ \text{SKIP}], \text{rule exI } [of \ - \ t_1])$ 
{
  fix  $x$ 
  assume  $s = t_1 \ (\subseteq \text{sources-aux } [\langle \text{bvars } b \rangle] \ s \ x)$ 
  hence  $s = t_1 \ (\subseteq \text{bvars } b)$ 
  using  $Q$  by  $(\text{blast dest: sources-aux-observe-hd})$ 
  hence  $\neg \text{bval } b \ t_1$ 
  using  $S$  by  $(\text{blast dest: bvars-bval})$ 
  hence  $(\text{IF } b \ \text{THEN } c;; \ \text{WHILE } b \ \text{DO } c \ \text{ELSE } \text{SKIP}, \ t_1) \rightarrow$ 
   $(\text{SKIP}, \ t_1) \ ..$ 
}
moreover {

```

```

fix  $x$ 
assume  $s = t_1 \ (\subseteq \text{sources} \ [\langle bvars \ b \rangle] \ s \ x)$ 
hence  $s \ x = t_1 \ x$ 
  by (subst (asm) append-Nil [symmetric],
    simp only: sources.simps, auto)
}
ultimately show  $\forall x.$ 
  ( $s_1 = t_1 \ (\subseteq \text{sources-aux} \ (\text{flow } cfs_2) \ s_1 \ x) \longrightarrow$ 
    ( $c_1, t_1 \rightarrow^* (SKIP, t_1) \wedge (c_2 = SKIP) = (SKIP = SKIP)$ )  $\wedge$ 
    ( $s_1 = t_1 \ (\subseteq \text{sources} \ (\text{flow } cfs_2) \ s_1 \ x) \longrightarrow s_2 \ x = t_1 \ x$ )
  using  $R$  and  $T$  and  $U$  by auto
qed
qed
next
assume  $R: \text{bval } b \ s$ 
with  $D$  and  $O$  and  $P$  have  $S: s \in \text{Univ } B_1 \ (\subseteq \text{state} \cap X)$ 
  by (drule-tac btyping2-approx [where s = s], auto)
assume ( $c;; \text{WHILE } b \text{ DO } c, s \rightarrow^* \{tl2 \ cfs_1\} (c_1, s_1)$ )
hence
  ( $\exists c' \ cfs'. c_1 = c';; \text{WHILE } b \text{ DO } c \wedge$ 
    ( $c, s \rightarrow^* \{cfs'\} (c', s_1) \wedge$ 
       $\text{flow } (tl2 \ cfs_1) = \text{flow } cfs' \vee$ 
    ( $\exists s' \ cfs' \ cfs''. \text{length } cfs'' < \text{length } (tl2 \ cfs_1) \wedge$ 
      ( $c, s \rightarrow^* \{cfs'\} (SKIP, s') \wedge$ 
        ( $\text{WHILE } b \text{ DO } c, s' \rightarrow^* \{cfs''\} (c_1, s_1) \wedge$ 
           $\text{flow } (tl2 \ cfs_1) = \text{flow } cfs' @ \text{flow } cfs''$ )
      by (rule small-steps1-seq)
    moreover {
      fix  $c' \ cfs$ 
      assume
         $T: (c, s) \rightarrow^* \{cfs\} (c', s_1)$  and
         $U: c_1 = c';; \text{WHILE } b \text{ DO } c$ 
      hence  $V: (c';; \text{WHILE } b \text{ DO } c, s_1) \rightarrow^* \{cfs_2\} (c_2, s_2)$ 
        using  $J$  by simp
      hence  $W: s_2 = \text{run-flow } (\text{flow } cfs_2) \ s_1$ 
        by (rule small-steps1-run-flow)
      have
        ( $\exists c'' \ cfs'. c_2 = c'';; \text{WHILE } b \text{ DO } c \wedge$ 
          ( $c', s_1 \rightarrow^* \{cfs'\} (c'', s_2) \wedge$ 
             $\text{flow } cfs_2 = \text{flow } cfs' \vee$ 
          ( $\exists s' \ cfs' \ cfs''. \text{length } cfs'' < \text{length } cfs_2 \wedge$ 
            ( $c', s_1 \rightarrow^* \{cfs'\} (SKIP, s') \wedge$ 
              ( $\text{WHILE } b \text{ DO } c, s' \rightarrow^* \{cfs''\} (c_2, s_2) \wedge$ 
                 $\text{flow } cfs_2 = \text{flow } cfs' @ \text{flow } cfs''$ )
            using  $V$  by (rule small-steps1-seq)
          moreover {
            fix  $c'' \ cfs'$ 
            assume ( $c', s_1 \rightarrow^* \{cfs'\} (c'', s_2)$ )
            then obtain  $c_2'$  and  $t_2$  where  $X: \forall x.$ 

```


$(s_1 = t_1 (\subseteq \text{sources-aux } (\text{flow cfs}') s_1 x) \longrightarrow$
 $(c', t_1) \rightarrow^* (c_2', t_2) \wedge (c'' = \text{SKIP}) = (c_2' = \text{SKIP})) \wedge$
 $(s_1 = t_1 (\subseteq \text{sources } (\text{flow cfs}') s_1 x) \longrightarrow$
 $\text{run-flow } (\text{flow cfs}_2) s_1 x = t_2 x)$
using A [of $B_1 \ C \ B_1' \ D \ s \ \text{cfs} \ c' \ s_1 \ \text{cfs}' \ c''$
 $\text{run-flow } (\text{flow cfs}_2) s_1]$ **and** N **and** S **and** T **and** W **by force**
assume
 $Y: c_2 = c'';$ **WHILE** b **DO** c **and**
 $Z: \text{flow cfs}_2 = \text{flow cfs}'$
have *?thesis*
proof (*rule exI* [of $- c_2'$; **WHILE** b **DO** c], *rule exI* [of $- t_2$])
from U **and** W **and** X **and** Y **and** Z **show** $\forall x.$
 $(s_1 = t_1 (\subseteq \text{sources-aux } (\text{flow cfs}_2) s_1 x) \longrightarrow$
 $(c_1, t_1) \rightarrow^* (c_2'; \text{WHILE } b \text{ DO } c, t_2) \wedge$
 $(c_2 = \text{SKIP}) = (c_2'; \text{WHILE } b \text{ DO } c = \text{SKIP})) \wedge$
 $(s_1 = t_1 (\subseteq \text{sources } (\text{flow cfs}_2) s_1 x) \longrightarrow s_2 x = t_2 x)$
by (*auto intro: star-seq2*)
qed
}
moreover {
fix $s' \ \text{cfs}' \ \text{cfs}''$
assume
 $X: \text{length } \text{cfs}'' < \text{length } \text{cfs}_2$ **and**
 $Y: (c', s_1) \rightarrow^* \{\text{cfs}'\} (\text{SKIP}, s')$ **and**
 $Z: (\text{WHILE } b \text{ DO } c, s') \rightarrow^* \{\text{cfs}''\} (c_2, s_2)$
then obtain c_2' **and** t_2 **where** $\forall x.$
 $(s_1 = t_1 (\subseteq \text{sources-aux } (\text{flow cfs}') s_1 x) \longrightarrow$
 $(c', t_1) \rightarrow^* (c_2', t_2) \wedge (\text{SKIP} = \text{SKIP}) = (c_2' = \text{SKIP})) \wedge$
 $(s_1 = t_1 (\subseteq \text{sources } (\text{flow cfs}') s_1 x) \longrightarrow s' x = t_2 x)$
using A [of $B_1 \ C \ B_1' \ D \ s \ \text{cfs} \ c' \ s_1 \ \text{cfs}' \ \text{SKIP} \ s'$]
and N **and** S **and** T **by force**
moreover have $AA: s' = \text{run-flow } (\text{flow cfs}') s_1$
using Y **by** (*rule small-stepsl-run-flow*)
ultimately have $AB: \forall x.$
 $(s_1 = t_1 (\subseteq \text{sources-aux } (\text{flow cfs}') s_1 x) \longrightarrow$
 $(c', t_1) \rightarrow^* (\text{SKIP}, t_2)) \wedge$
 $(s_1 = t_1 (\subseteq \text{sources } (\text{flow cfs}') s_1 x) \longrightarrow$
 $\text{run-flow } (\text{flow cfs}') s_1 x = t_2 x)$
by blast
have $AC: s_2 = \text{run-flow } (\text{flow cfs}'') s'$
using Z **by** (*rule small-stepsl-run-flow*)
moreover have $(c, s) \rightarrow^* \{\text{cfs} @ \text{cfs}'\} (\text{SKIP}, s')$
using T **and** Y **by** (*simp add: small-stepsl-append*)
hence $(c, s) \Rightarrow s'$
by (*auto dest: small-stepsl-steps simp: big-iff-small*)
hence $s' \in \text{Univ } C (\subseteq \text{state} \cap Y)$
using M **and** R **by blast**
ultimately obtain c_2' **and** t_3 **where** $AD: \forall x.$
 $(\text{run-flow } (\text{flow cfs}') s_1 = t_2$

$(\subseteq \text{sources-aux } (\text{flow cfs}'') (\text{run-flow } (\text{flow cfs}') s_1) x) \longrightarrow$
 $(\text{WHILE } b \text{ DO } c, t_2) \rightarrow^* (c_2', t_3) \wedge$
 $(c_2 = \text{SKIP}) = (c_2' = \text{SKIP})) \wedge$
 $(\text{run-flow } (\text{flow cfs}') s_1 = t_2$
 $(\subseteq \text{sources } (\text{flow cfs}'') (\text{run-flow } (\text{flow cfs}') s_1) x) \longrightarrow$
 $\text{run-flow } (\text{flow cfs}'') (\text{run-flow } (\text{flow cfs}') s_1) x = t_3 x)$
using K [of $\text{cfs}'' \sqcup \text{cfs}'' s' \text{ WHILE } b \text{ DO } c s'$]
and X **and** Z **and** AA **by force**
moreover assume $\text{flow cfs}_2 = \text{flow cfs}' @ \text{flow cfs}''$
moreover {
fix x
assume $AE: s_1 = t_1$
 $(\subseteq \text{sources-aux } (\text{flow cfs}' @ \text{flow cfs}'') s_1 x)$
moreover have $\text{sources-aux } (\text{flow cfs}') s_1 x \subseteq$
 $\text{sources-aux } (\text{flow cfs}' @ \text{flow cfs}'') s_1 x$
by (rule *sources-aux-append*)
ultimately have $(c', t_1) \rightarrow^* (\text{SKIP}, t_2)$
using AB **by blast**
hence $(c';; \text{WHILE } b \text{ DO } c, t_1) \rightarrow^* (\text{SKIP};; \text{WHILE } b \text{ DO } c, t_2)$
by (rule *star-seq2*)
hence $(c';; \text{WHILE } b \text{ DO } c, t_1) \rightarrow^* (\text{WHILE } b \text{ DO } c, t_2)$
by (blast *intro: star-trans*)
moreover have $\text{run-flow } (\text{flow cfs}') s_1 = t_2$
 $(\subseteq \text{sources-aux } (\text{flow cfs}'') (\text{run-flow } (\text{flow cfs}') s_1) x)$
proof
fix y
assume $y \in \text{sources-aux } (\text{flow cfs}'')$
 $(\text{run-flow } (\text{flow cfs}') s_1) x$
hence $\text{sources } (\text{flow cfs}') s_1 y \subseteq$
 $\text{sources-aux } (\text{flow cfs}' @ \text{flow cfs}'') s_1 x$
by (rule *sources-aux-member*)
thus $\text{run-flow } (\text{flow cfs}') s_1 y = t_2 y$
using AB **and** AE **by blast**
qed
hence $(\text{WHILE } b \text{ DO } c, t_2) \rightarrow^* (c_2', t_3) \wedge$
 $(c_2 = \text{SKIP}) = (c_2' = \text{SKIP})$
using AD **by simp**
ultimately have $(c';; \text{WHILE } b \text{ DO } c, t_1) \rightarrow^* (c_2', t_3) \wedge$
 $(c_2 = \text{SKIP}) = (c_2' = \text{SKIP})$
by (blast *intro: star-trans*)
}
moreover {
fix x
assume $AE: s_1 = t_1$
 $(\subseteq \text{sources } (\text{flow cfs}' @ \text{flow cfs}'') s_1 x)$
have $\text{run-flow } (\text{flow cfs}') s_1 = t_2$
 $(\subseteq \text{sources } (\text{flow cfs}'') (\text{run-flow } (\text{flow cfs}') s_1) x)$
proof
fix y

```

    assume  $y \in \text{sources } (\text{flow } cfs'')$ 
    (run-flow (flow cfs')  $s_1$ )  $x$ 
  hence  $\text{sources } (\text{flow } cfs') s_1 y \subseteq$ 
     $\text{sources } (\text{flow } cfs' @ \text{flow } cfs'') s_1 x$ 
    by (rule sources-member)
  thus run-flow (flow cfs')  $s_1 y = t_2 y$ 
    using AB and AE by blast
qed
  hence run-flow (flow cfs'')
    (run-flow (flow cfs')  $s_1$ )  $x = t_3 x$ 
    using AD by simp
}
ultimately have ?thesis
  by (metis U AA AC)
}
ultimately have ?thesis
  by blast
}
moreover {
  fix  $s' cfs cfs'$ 
  assume
     $\text{length } cfs' < \text{length } (tl2 cfs_1)$  and
     $(c, s) \rightarrow^*\{cfs\} (SKIP, s')$  and
     $(WHILE\ b\ DO\ c, s') \rightarrow^*\{cfs'\} (c_1, s_1)$ 
  moreover from this have  $(c, s) \Rightarrow s'$ 
    by (auto dest: small-stepsl-steps simp: big-iff-small)
  hence  $s' \in Univ\ C (\subseteq state \cap Y)$ 
    using M and R by blast
  ultimately have ?thesis
    using K [of  $cfs' @ cfs_2 cfs' cfs_2 s' c_1 s_1$ ] and J by force
}
ultimately show ?thesis
  by blast
next
  assume  $(SKIP, s) \rightarrow^*\{tl2 cfs_1\} (c_1, s_1)$ 
  hence  $(c_1, s_1) = (SKIP, s)$ 
    by (blast dest: small-stepsl-skip)
  moreover from this have  $(c_2, s_2) = (SKIP, s) \wedge \text{flow } cfs_2 = []$ 
    using J by (blast dest: small-stepsl-skip)
  ultimately show ?thesis
    by auto
qed
qed
}
moreover {
  fix  $r t_1$ 
  assume O:  $r \in C$  and P:  $s = r (\subseteq state \cap Y)$ 
  have Q:  $\forall x. \forall y \in bvars\ b. s: \text{dom } y \rightsquigarrow \text{dom } x$ 
  proof (cases  $state \subseteq Y$ )

```

```

case True
with P have interf s = interf r
  by (blast intro: interf-state)
with N and O show ?thesis
  by (erule-tac conjE, drule-tac bspec,
    auto simp: univ-states-if-def)
next
case False
with N and O show ?thesis
  by (erule-tac conjE, drule-tac bspec,
    auto simp: univ-states-if-def)
qed
have  $(c_1, s_1) = (WHILE\ b\ DO\ c, s) \vee$ 
   $(IF\ b\ THEN\ c;;\ WHILE\ b\ DO\ c\ ELSE\ SKIP, s) \rightarrow^*\{tl\ cfs_1\} (c_1, s_1)$ 
  using I by (blast dest: small-steps-l-while)
hence  $\exists c_2' t_2. \forall x.$ 
   $(s_1 = t_1 (\subseteq sources\ aux\ (flow\ cfs_2)\ s_1\ x) \longrightarrow$ 
     $(c_1, t_1) \rightarrow^* (c_2', t_2) \wedge (c_2 = SKIP) = (c_2' = SKIP)) \wedge$ 
     $(s_1 = t_1 (\subseteq sources\ (flow\ cfs_2)\ s_1\ x) \longrightarrow s_2\ x = t_2\ x)$ 
proof
  assume R:  $(c_1, s_1) = (WHILE\ b\ DO\ c, s)$ 
  hence  $(WHILE\ b\ DO\ c, s) \rightarrow^*\{cfs_2\} (c_2, s_2)$ 
    using J by simp
  hence
     $(c_2, s_2) = (WHILE\ b\ DO\ c, s) \wedge$ 
     $flow\ cfs_2 = [] \vee$ 
     $(IF\ b\ THEN\ c;;\ WHILE\ b\ DO\ c\ ELSE\ SKIP, s) \rightarrow^*\{tl\ cfs_2\} (c_2, s_2) \wedge$ 
     $flow\ cfs_2 = flow\ (tl\ cfs_2)$ 
    (is  $?P \vee ?Q \wedge ?R$ )
    by (rule small-steps-l-while)
  thus ?thesis
proof (rule disjE, erule-tac [2] conjE)
  assume ?P
  with R show ?thesis
    by auto
next
assume ?Q and ?R
have
   $(c_2, s_2) = (IF\ b\ THEN\ c;;\ WHILE\ b\ DO\ c\ ELSE\ SKIP, s) \wedge$ 
   $flow\ (tl\ cfs_2) = [] \vee$ 
   $bval\ b\ s \wedge (c;;\ WHILE\ b\ DO\ c, s) \rightarrow^*\{tl2\ cfs_2\} (c_2, s_2) \wedge$ 
   $flow\ (tl\ cfs_2) = \langle bvars\ b \rangle \# flow\ (tl2\ cfs_2) \vee$ 
   $\neg\ bval\ b\ s \wedge (SKIP, s) \rightarrow^*\{tl2\ cfs_2\} (c_2, s_2) \wedge$ 
   $flow\ (tl\ cfs_2) = \langle bvars\ b \rangle \# flow\ (tl2\ cfs_2)$ 
  using  $\langle ?Q \rangle$  by (rule small-steps-l-if)
thus ?thesis
proof (erule-tac disjE, erule-tac [2] disjE, (erule-tac [2-3] conjE)+)
  assume  $(c_2, s_2) = (IF\ b\ THEN\ c;;\ WHILE\ b\ DO\ c\ ELSE\ SKIP, s) \wedge$ 
   $flow\ (tl\ cfs_2) = []$ 

```

with R and $\langle ?R \rangle$ show $?thesis$
 by *auto*
 next
 assume $S: bval\ b\ s$
 with F and O and P have $T: s \in Univ\ B_1' (\subseteq state \cap Y)$
 by (*drule-tac btyping2-approx [where $s = s$], auto*)
 assume $U: (c;; WHILE\ b\ DO\ c, s) \rightarrow^*\{tl2\ cfs_2\} (c_2, s_2)$
 hence
 ($\exists\ c'\ cfs. c_2 = c';; WHILE\ b\ DO\ c \wedge$
 $(c, s) \rightarrow^*\{cfs\} (c', s_2) \wedge$
 $flow\ (tl2\ cfs_2) = flow\ cfs) \vee$
 $(\exists\ s'\ cfs\ cfs'. length\ cfs' < length\ (tl2\ cfs_2) \wedge$
 $(c, s) \rightarrow^*\{cfs\} (SKIP, s') \wedge$
 $(WHILE\ b\ DO\ c, s') \rightarrow^*\{cfs'\} (c_2, s_2) \wedge$
 $flow\ (tl2\ cfs_2) = flow\ cfs @ flow\ cfs')$
 by (*rule small-steps-Seq*)
 moreover assume $flow\ (tl\ cfs_2) = \langle bvars\ b \rangle \# flow\ (tl2\ cfs_2)$
 moreover have $s_2 = run-flow\ (flow\ (tl2\ cfs_2))\ s$
 using U by (*rule small-steps-run-flow*)
 moreover {
 fix $c'\ cfs$
 assume $(c, s) \rightarrow^*\{cfs\} (c', run-flow\ (flow\ cfs)\ s)$
 then obtain c_2' and t_2 where $V: \forall x.$
 $(s = t_1 (\subseteq sources-aux\ (flow\ cfs)\ s\ x) \longrightarrow$
 $(c, t_1) \rightarrow^* (c_2', t_2) \wedge (c' = SKIP) = (c_2' = SKIP)) \wedge$
 $(s = t_1 (\subseteq sources\ (flow\ cfs)\ s\ x) \longrightarrow$
 $run-flow\ (flow\ cfs)\ s\ x = t_2\ x)$
 using B [*of $B_1\ C\ B_1'\ D'\ s\ []\ c\ s\ cfs\ c'$*]
 $run-flow\ (flow\ cfs)\ s]$ and N and T by *force*
 {
 fix x
 assume $W: s = t_1 (\subseteq sources-aux\ (\langle bvars\ b \rangle \# flow\ cfs)\ s\ x)$
 moreover have $sources-aux\ (flow\ cfs)\ s\ x \subseteq$
 $sources-aux\ (\langle bvars\ b \rangle \# (flow\ cfs))\ s\ x$
 by (*rule sources-aux-observe-tl*)
 ultimately have $(c, t_1) \rightarrow^* (c_2', t_2)$
 using V by *blast*
 hence $(c;; WHILE\ b\ DO\ c, t_1) \rightarrow^* (c_2';; WHILE\ b\ DO\ c, t_2)$
 by (*rule star-Seq2*)
 moreover have $s = t_1 (\subseteq bvars\ b)$
 using Q and W by (*blast dest: sources-aux-observe-hd*)
 hence $bval\ b\ t_1$
 using S by (*blast dest: bvars-bval*)
 hence $(WHILE\ b\ DO\ c, t_1) \rightarrow^* (c;; WHILE\ b\ DO\ c, t_1)$
 by (*blast intro: star-trans*)
 ultimately have $(WHILE\ b\ DO\ c, t_1) \rightarrow^*$
 $(c_2';; WHILE\ b\ DO\ c, t_2) \wedge c_2';; WHILE\ b\ DO\ c \neq SKIP$
 by (*blast intro: star-trans*)
 }
 }

moreover {
 fix x
 assume $s = t_1 (\subseteq \text{sources } (\langle \text{bvars } b \rangle \# \text{flow cfs}) s x)$
 moreover have $\text{sources } (\text{flow cfs}) s x \subseteq$
 $\text{sources } (\langle \text{bvars } b \rangle \# (\text{flow cfs})) s x$
 by (rule *sources-observe-tl*)
 ultimately have $\text{run-flow } (\text{flow cfs}) s x = t_2 x$
 using V **by** *blast*
}

ultimately have $\exists c_2' t_2. \forall x.$
 $(s = t_1 (\subseteq \text{sources-aux } (\langle \text{bvars } b \rangle \# \text{flow cfs}) s x) \longrightarrow$
 $(\text{WHILE } b \text{ DO } c, t_1) \rightarrow^* (c_2', t_2) \wedge c_2' \neq \text{SKIP}) \wedge$
 $(s = t_1 (\subseteq \text{sources } (\langle \text{bvars } b \rangle \# \text{flow cfs}) s x) \longrightarrow$
 $\text{run-flow } (\text{flow cfs}) s x = t_2 x)$
 by *blast*
}

moreover {
 fix $s' \text{ cfs cfs}'$
 assume
 $V: \text{length cfs}' < \text{length cfs}_2 - \text{Suc } (\text{Suc } 0) \text{ and}$
 $W: (c, s) \rightarrow^* \{ \text{cfs} \} (\text{SKIP}, s') \text{ and}$
 $X: (\text{WHILE } b \text{ DO } c, s') \rightarrow^* \{ \text{cfs}' \}$
 $(c_2, \text{run-flow } (\text{flow cfs}') (\text{run-flow } (\text{flow cfs}) s))$
 then obtain c_2' **and** t_2 **where** $\forall x.$
 $(s = t_1 (\subseteq \text{sources-aux } (\text{flow cfs}) s x) \longrightarrow$
 $(c, t_1) \rightarrow^* (c_2', t_2) \wedge (\text{SKIP} = \text{SKIP}) = (c_2' = \text{SKIP})) \wedge$
 $(s = t_1 (\subseteq \text{sources } (\text{flow cfs}) s x) \longrightarrow s' x = t_2 x)$
 using B [of $B_1 \ C \ B_1' \ D' \ s \ [] \ c \ s \ \text{cfs} \ \text{SKIP} \ s'$]
 and N **and** T **by** *force*
 moreover have $Y: s' = \text{run-flow } (\text{flow cfs}) s$
 using W **by** (rule *small-steps-l-run-flow*)
 ultimately have $Z: \forall x.$
 $(s = t_1 (\subseteq \text{sources-aux } (\text{flow cfs}) s x) \longrightarrow$
 $(c, t_1) \rightarrow^* (\text{SKIP}, t_2)) \wedge$
 $(s = t_1 (\subseteq \text{sources } (\text{flow cfs}) s x) \longrightarrow$
 $\text{run-flow } (\text{flow cfs}) s x = t_2 x)$
 by *blast*
 assume $s_2 = \text{run-flow } (\text{flow cfs}') (\text{run-flow } (\text{flow cfs}) s)$
 moreover have $(c, s) \Rightarrow s'$
 using W **by** (auto dest: *small-steps-l-steps simp: big-iff-small*)
 hence $s' \in \text{Univ } C (\subseteq \text{state} \cap Y)$
 using M **and** S **by** *blast*
 ultimately obtain c_3' **and** t_3 **where** $AA: \forall x.$
 $(\text{run-flow } (\text{flow cfs}) s = t_2$
 $(\subseteq \text{sources-aux } (\text{flow cfs}') (\text{run-flow } (\text{flow cfs}) s) x) \longrightarrow$
 $(\text{WHILE } b \text{ DO } c, t_2) \rightarrow^* (c_3', t_3) \wedge$
 $(c_2 = \text{SKIP}) = (c_3' = \text{SKIP})) \wedge$
 $(\text{run-flow } (\text{flow cfs}) s = t_2$
 $(\subseteq \text{sources } (\text{flow cfs}') (\text{run-flow } (\text{flow cfs}) s) x) \longrightarrow$

```

    run-flow (flow cfs') (run-flow (flow cfs) s) x = t3 x)
  using K [of cfs' [] cfs' s' WHILE b DO c s']
  and V and X and Y by force
{
  fix x
  assume AB: s = t1
    (⊆ sources-aux (⟨bvars b⟩ # flow cfs @ flow cfs') s x)
  moreover have sources-aux (flow cfs) s x ⊆
    sources-aux (flow cfs @ flow cfs') s x
    by (rule sources-aux-append)
  moreover have AC: sources-aux (flow cfs @ flow cfs') s x ⊆
    sources-aux (⟨bvars b⟩ # flow cfs @ flow cfs') s x
    by (rule sources-aux-observe-tl)
  ultimately have (c, t1) →* (SKIP, t2)
    using Z by blast
  hence (c;; WHILE b DO c, t1) →* (SKIP;; WHILE b DO c, t2)
    by (rule star-seq2)
  moreover have s = t1 (⊆ bvars b)
    using Q and AB by (blast dest: sources-aux-observe-hd)
  hence bval b t1
    using S by (blast dest: bvars-bval)
  hence (WHILE b DO c, t1) →* (c;; WHILE b DO c, t1)
    by (blast intro: star-trans)
  ultimately have (WHILE b DO c, t1) →* (WHILE b DO c, t2)
    by (blast intro: star-trans)
  moreover have run-flow (flow cfs) s = t2
    (⊆ sources-aux (flow cfs') (run-flow (flow cfs) s) x)
  proof
    fix y
    assume y ∈ sources-aux (flow cfs')
      (run-flow (flow cfs) s) x
    hence sources (flow cfs) s y ⊆
      sources-aux (flow cfs @ flow cfs') s x
      by (rule sources-aux-member)
    hence sources (flow cfs) s y ⊆
      sources-aux (⟨bvars b⟩ # flow cfs @ flow cfs') s x
      using AC by simp
    thus run-flow (flow cfs) s y = t2 y
      using Z and AB by blast
  qed
  hence (WHILE b DO c, t2) →* (c3', t3) ∧
    (c2 = SKIP) = (c3' = SKIP)
    using AA by simp
  ultimately have (WHILE b DO c, t1) →* (c3', t3) ∧
    (c2 = SKIP) = (c3' = SKIP)
    by (blast intro: star-trans)
}
moreover {
  fix x

```

```

assume  $AB: s = t_1$ 
  ( $\subseteq$  sources ( $\langle bvars\ b \rangle \# flow\ cfs @ flow\ cfs'$ )  $s\ x$ )
have run-flow (flow cfs)  $s = t_2$ 
  ( $\subseteq$  sources (flow cfs') (run-flow (flow cfs)  $s$ )  $x$ )
proof
  fix  $y$ 
  assume  $y \in sources\ (flow\ cfs')$ 
    (run-flow (flow cfs)  $s$ )  $x$ 
  hence sources (flow cfs)  $s\ y \subseteq$ 
    sources (flow cfs @ flow cfs')  $s\ x$ 
    by (rule sources-member)
  moreover have sources (flow cfs @ flow cfs')  $s\ x \subseteq$ 
    sources ( $\langle bvars\ b \rangle \# flow\ cfs @ flow\ cfs'$ )  $s\ x$ 
    by (rule sources-observe-tl)
  ultimately have sources (flow cfs)  $s\ y \subseteq$ 
    sources ( $\langle bvars\ b \rangle \# flow\ cfs @ flow\ cfs'$ )  $s\ x$ 
    by simp
  thus run-flow (flow cfs)  $s\ y = t_2\ y$ 
    using  $Z$  and  $AB$  by blast
qed
hence run-flow (flow cfs') (run-flow (flow cfs)  $s$ )  $x = t_3\ x$ 
  using  $AA$  by simp
}
ultimately have  $\exists c_3' t_3. \forall x.$ 
  ( $s = t_1$ 
    ( $\subseteq$  sources-aux ( $\langle bvars\ b \rangle \# flow\ cfs @ flow\ cfs'$ )  $s\ x$ )  $\longrightarrow$ 
      (WHILE  $b\ DO\ c, t_1 \rightarrow^* (c_3', t_3) \wedge$ 
        ( $c_2 = SKIP = (c_3' = SKIP)$ )  $\wedge$ 
      ( $s = t_1$ 
        ( $\subseteq$  sources ( $\langle bvars\ b \rangle \# flow\ cfs @ flow\ cfs'$ )  $s\ x$ )  $\longrightarrow$ 
          run-flow (flow cfs') (run-flow (flow cfs)  $s$ )  $x = t_3\ x$ )
        by auto
      )
    )
  }
ultimately show ?thesis
  using  $R$  and  $\langle ?R \rangle$  by (auto simp: run-flow-append)
next
assume
   $S: \neg bval\ b\ s$  and
   $T: flow\ (tl\ cfs_2) = \langle bvars\ b \rangle \# flow\ (tl2\ cfs_2)$ 
assume (SKIP,  $s$ )  $\rightarrow^* \{tl2\ cfs_2\} (c_2, s_2)$ 
hence  $U: (c_2, s_2) = (SKIP, s) \wedge flow\ (tl2\ cfs_2) = []$ 
  by (rule small-steps1-skip)
show ?thesis
proof (rule exI [of - SKIP], rule exI [of -  $t_1$ ])
  {
    fix  $x$ 
    have (WHILE  $b\ DO\ c, t_1 \rightarrow$ 
      (IF  $b\ THEN\ c;;\ WHILE\ b\ DO\ c\ ELSE\ SKIP, t_1$ )  $..$ 
    )
    moreover assume  $s = t_1 (\subseteq sources-aux\ [\langle bvars\ b \rangle]\ s\ x)$ 
  }

```



```

    hence  $s = t_1 (\subseteq \text{bvars } b)$ 
    using  $Q$  by (blast dest: sources-aux-observe-hd)
    hence  $\neg \text{bval } b \ t_1$ 
    using  $S$  by (blast dest: bvars-bval)
    hence  $(\text{IF } b \ \text{THEN } c;; \ \text{WHILE } b \ \text{DO } c \ \text{ELSE } \text{SKIP}, t_1) \rightarrow$ 
       $(\text{SKIP}, t_1) ..$ 
    ultimately have  $(\text{WHILE } b \ \text{DO } c, t_1) \rightarrow^* (\text{SKIP}, t_1)$ 
      by (blast intro: star-trans)
  }
  moreover {
    fix  $x$ 
    assume  $s = t_1 (\subseteq \text{sources } [\langle \text{bvars } b \rangle] \ s \ x)$ 
    hence  $s \ x = t_1 \ x$ 
    by (subst (asm) append-Nil [symmetric],
        simp only: sources.simps, auto)
  }
  ultimately show  $\forall x.$ 
     $(s_1 = t_1 (\subseteq \text{sources-aux } (\text{flow } cfs_2) \ s_1 \ x) \longrightarrow$ 
       $(c_1, t_1) \rightarrow^* (\text{SKIP}, t_1) \wedge (c_2 = \text{SKIP}) = (\text{SKIP} = \text{SKIP})) \wedge$ 
       $(s_1 = t_1 (\subseteq \text{sources } (\text{flow } cfs_2) \ s_1 \ x) \longrightarrow s_2 \ x = t_1 \ x)$ 
      using  $R$  and  $T$  and  $U$  and  $\langle ?R \rangle$  by auto
  qed
qed
qed
next
assume  $(\text{IF } b \ \text{THEN } c;; \ \text{WHILE } b \ \text{DO } c \ \text{ELSE } \text{SKIP}, s) \rightarrow^* \{tl \ cfs_1\} (c_1, s_1)$ 
hence
 $(c_1, s_1) = (\text{IF } b \ \text{THEN } c;; \ \text{WHILE } b \ \text{DO } c \ \text{ELSE } \text{SKIP}, s) \wedge$ 
 $\text{flow } (tl \ cfs_1) = [] \vee$ 
 $\text{bval } b \ s \wedge (c;; \ \text{WHILE } b \ \text{DO } c, s) \rightarrow^* \{tl2 \ cfs_1\} (c_1, s_1) \wedge$ 
 $\text{flow } (tl \ cfs_1) = \langle \text{bvars } b \rangle \# \text{flow } (tl2 \ cfs_1) \vee$ 
 $\neg \text{bval } b \ s \wedge (\text{SKIP}, s) \rightarrow^* \{tl2 \ cfs_1\} (c_1, s_1) \wedge$ 
 $\text{flow } (tl \ cfs_1) = \langle \text{bvars } b \rangle \# \text{flow } (tl2 \ cfs_1)$ 
by (rule small-steps-l-if)
thus ?thesis
proof (rule disjE, erule-tac [2] disjE, erule-tac conjE,
      (erule-tac [2-3] conjE)+)
  assume  $R: (c_1, s_1) = (\text{IF } b \ \text{THEN } c;; \ \text{WHILE } b \ \text{DO } c \ \text{ELSE } \text{SKIP}, s)$ 
  hence  $(\text{IF } b \ \text{THEN } c;; \ \text{WHILE } b \ \text{DO } c \ \text{ELSE } \text{SKIP}, s) \rightarrow^* \{cfs_2\} (c_2, s_2)$ 
    using  $J$  by simp
  hence
     $(c_2, s_2) = (\text{IF } b \ \text{THEN } c;; \ \text{WHILE } b \ \text{DO } c \ \text{ELSE } \text{SKIP}, s) \wedge$ 
     $\text{flow } cfs_2 = [] \vee$ 
     $\text{bval } b \ s \wedge (c;; \ \text{WHILE } b \ \text{DO } c, s) \rightarrow^* \{tl \ cfs_2\} (c_2, s_2) \wedge$ 
     $\text{flow } cfs_2 = \langle \text{bvars } b \rangle \# \text{flow } (tl \ cfs_2) \vee$ 
     $\neg \text{bval } b \ s \wedge (\text{SKIP}, s) \rightarrow^* \{tl \ cfs_2\} (c_2, s_2) \wedge$ 
     $\text{flow } cfs_2 = \langle \text{bvars } b \rangle \# \text{flow } (tl \ cfs_2)$ 
    by (rule small-steps-l-if)
  thus ?thesis

```

proof (*erule-tac* *disjE*, *erule-tac* [2] *disjE*, (*erule-tac* [2-3] *conjE*)+)
assume $(c_2, s_2) = (IF\ b\ THEN\ c;;\ WHILE\ b\ DO\ c\ ELSE\ SKIP, s) \wedge$
 $flow\ cfs_2 = []$
with R **show** *?thesis*
by *auto*
next
assume $S: bval\ b\ s$
with F **and** O **and** P **have** $T: s \in Univ\ B_1' (\subseteq state \cap Y)$
by (*drule-tac* *btyping2-approx* [**where** $s = s$], *auto*)
assume $U: (c;;\ WHILE\ b\ DO\ c, s) \rightarrow^*\{tl\ cfs_2\} (c_2, s_2)$
hence
 $(\exists\ c'\ cfs. c_2 = c';\ WHILE\ b\ DO\ c \wedge$
 $(c, s) \rightarrow^*\{cfs\} (c', s_2) \wedge$
 $flow\ (tl\ cfs_2) = flow\ cfs) \vee$
 $(\exists\ s'\ cfs\ cfs'. length\ cfs' < length\ (tl\ cfs_2) \wedge$
 $(c, s) \rightarrow^*\{cfs\} (SKIP, s') \wedge$
 $(WHILE\ b\ DO\ c, s') \rightarrow^*\{cfs'\} (c_2, s_2) \wedge$
 $flow\ (tl\ cfs_2) = flow\ cfs @ flow\ cfs')$
by (*rule small-steps-sl-seq*)
moreover **assume** $flow\ cfs_2 = \langle bvars\ b \rangle \# flow\ (tl\ cfs_2)$
moreover **have** $s_2 = run-flow\ (flow\ (tl\ cfs_2))\ s$
using U **by** (*rule small-steps-sl-run-flow*)
moreover {
fix $c'\ cfs$
assume $(c, s) \rightarrow^*\{cfs\} (c', run-flow\ (flow\ cfs)\ s)$
then **obtain** c_2' **and** t_2 **where** $V: \forall x.$
 $(s = t_1 (\subseteq sources-aux\ (flow\ cfs)\ s\ x) \longrightarrow$
 $(c, t_1) \rightarrow^* (c_2', t_2) \wedge (c' = SKIP) = (c_2' = SKIP)) \wedge$
 $(s = t_1 (\subseteq sources\ (flow\ cfs)\ s\ x) \longrightarrow$
 $run-flow\ (flow\ cfs)\ s\ x = t_2\ x)$
using $B [of\ B_1\ C\ B_1'\ D'\ s\ []\ c\ s\ cfs\ c']$
 $run-flow\ (flow\ cfs)\ s]$ **and** N **and** T **by** *force*
{
fix x
assume $W: s = t_1 (\subseteq sources-aux\ (\langle bvars\ b \rangle \# flow\ cfs)\ s\ x)$
moreover **have** $sources-aux\ (flow\ cfs)\ s\ x \subseteq$
 $sources-aux\ (\langle bvars\ b \rangle \# (flow\ cfs))\ s\ x$
by (*rule sources-aux-observe-tl*)
ultimately **have** $(c, t_1) \rightarrow^* (c_2', t_2)$
using V **by** *blast*
hence $(c;;\ WHILE\ b\ DO\ c, t_1) \rightarrow^* (c_2';\ WHILE\ b\ DO\ c, t_2)$
by (*rule star-seq2*)
moreover **have** $s = t_1 (\subseteq bvars\ b)$
using Q **and** W **by** (*blast dest: sources-aux-observe-hd*)
hence $bval\ b\ t_1$
using S **by** (*blast dest: bvars-bval*)
hence $(IF\ b\ THEN\ c;;\ WHILE\ b\ DO\ c\ ELSE\ SKIP, t_1) \rightarrow$
 $(c;;\ WHILE\ b\ DO\ c, t_1) ..$
ultimately **have**

$(IF\ b\ THEN\ c;;\ WHILE\ b\ DO\ c\ ELSE\ SKIP,\ t_1) \rightarrow^*$
 $(c_2';;\ WHILE\ b\ DO\ c,\ t_2) \wedge c_2';;\ WHILE\ b\ DO\ c \neq SKIP$
by (*blast intro: star-trans*)
}
moreover {
fix x
assume $s = t_1 (\subseteq sources (\langle bvars\ b \rangle \# flow\ cfs)\ s\ x)$
moreover **have** $sources (flow\ cfs)\ s\ x \subseteq$
 $sources (\langle bvars\ b \rangle \# (flow\ cfs))\ s\ x$
by (*rule sources-observe-tl*)
ultimately **have** $run-flow (flow\ cfs)\ s\ x = t_2\ x$
using V **by** *blast*
}
ultimately **have** $\exists c_2'\ t_2.\ \forall x.$
 $(s = t_1 (\subseteq sources_aux (\langle bvars\ b \rangle \# flow\ cfs)\ s\ x) \longrightarrow$
 $(IF\ b\ THEN\ c;;\ WHILE\ b\ DO\ c\ ELSE\ SKIP,\ t_1) \rightarrow^* (c_2',\ t_2) \wedge$
 $c_2' \neq SKIP) \wedge$
 $(s = t_1 (\subseteq sources (\langle bvars\ b \rangle \# flow\ cfs)\ s\ x) \longrightarrow$
 $run-flow (flow\ cfs)\ s\ x = t_2\ x)$
by *blast*
}
moreover {
fix $s'\ cfs\ cfs'$
assume
 $V: length\ cfs' < length\ cfs_2 - Suc\ 0$ **and**
 $W: (c,\ s) \rightarrow^* \{cfs\}\ (SKIP,\ s')$ **and**
 $X: (WHILE\ b\ DO\ c,\ s') \rightarrow^* \{cfs'\}$
 $(c_2,\ run-flow (flow\ cfs') (run-flow (flow\ cfs)\ s))$
then **obtain** c_2' **and** t_2 **where** $\forall x.$
 $(s = t_1 (\subseteq sources_aux (flow\ cfs)\ s\ x) \longrightarrow$
 $(c,\ t_1) \rightarrow^* (c_2',\ t_2) \wedge (SKIP = SKIP) = (c_2' = SKIP)) \wedge$
 $(s = t_1 (\subseteq sources (flow\ cfs)\ s\ x) \longrightarrow s'\ x = t_2\ x)$
using $B\ [of\ B_1\ C\ B_1'\ D'\ s\ \sqcup\ c\ s\ cfs\ SKIP\ s']$
and N **and** T **by** *force*
moreover **have** $Y: s' = run-flow (flow\ cfs)\ s$
using W **by** (*rule small-steps1-run-flow*)
ultimately **have** $Z: \forall x.$
 $(s = t_1 (\subseteq sources_aux (flow\ cfs)\ s\ x) \longrightarrow$
 $(c,\ t_1) \rightarrow^* (SKIP,\ t_2)) \wedge$
 $(s = t_1 (\subseteq sources (flow\ cfs)\ s\ x) \longrightarrow$
 $run-flow (flow\ cfs)\ s\ x = t_2\ x)$
by *blast*
assume $s_2 = run-flow (flow\ cfs') (run-flow (flow\ cfs)\ s)$
moreover **have** $(c,\ s) \Rightarrow s'$
using W **by** (*auto dest: small-steps1-steps simp: big-iff-small*)
hence $s' \in Univ\ C (\subseteq state \cap Y)$
using M **and** S **by** *blast*
ultimately **obtain** c_3' **and** t_3 **where** $AA: \forall x.$
 $(run-flow (flow\ cfs)\ s = t_2$

$(\subseteq \text{sources-aux } (\text{flow cfs}') (\text{run-flow } (\text{flow cfs}) s) x) \longrightarrow$
 $(\text{WHILE } b \text{ DO } c, t_2) \rightarrow^* (c_3', t_3) \wedge$
 $(c_2 = \text{SKIP}) = (c_3' = \text{SKIP})) \wedge$
 $(\text{run-flow } (\text{flow cfs}) s = t_2$
 $(\subseteq \text{sources } (\text{flow cfs}') (\text{run-flow } (\text{flow cfs}) s) x) \longrightarrow$
 $\text{run-flow } (\text{flow cfs}') (\text{run-flow } (\text{flow cfs}) s) x = t_3 x)$
using K [of $\text{cfs}' \sqcup \text{cfs}' s' \text{ WHILE } b \text{ DO } c s'$]
and V **and** X **and** Y **by force**
{
fix x
assume $AB: s = t_1$
 $(\subseteq \text{sources-aux } (\langle \text{bvars } b \rangle \# \text{flow cfs } @ \text{flow cfs}') s x)$
moreover have $\text{sources-aux } (\text{flow cfs}) s x \subseteq$
 $\text{sources-aux } (\text{flow cfs } @ \text{flow cfs}') s x$
by (rule *sources-aux-append*)
moreover have $AC: \text{sources-aux } (\text{flow cfs } @ \text{flow cfs}') s x \subseteq$
 $\text{sources-aux } (\langle \text{bvars } b \rangle \# \text{flow cfs } @ \text{flow cfs}') s x$
by (rule *sources-aux-observe-tl*)
ultimately have $(c, t_1) \rightarrow^* (\text{SKIP}, t_2)$
using Z **by** *blast*
hence $(c;; \text{WHILE } b \text{ DO } c, t_1) \rightarrow^* (\text{SKIP};; \text{WHILE } b \text{ DO } c, t_2)$
by (rule *star-seq2*)
moreover have $s = t_1 (\subseteq \text{bvars } b)$
using Q **and** AB **by** (blast *dest: sources-aux-observe-hd*)
hence $\text{bval } b t_1$
using S **by** (blast *dest: bvars-bval*)
hence $(\text{IF } b \text{ THEN } c;; \text{WHILE } b \text{ DO } c \text{ ELSE } \text{SKIP}, t_1) \rightarrow$
 $(c;; \text{WHILE } b \text{ DO } c, t_1) ..$
ultimately have $(\text{IF } b \text{ THEN } c;; \text{WHILE } b \text{ DO } c \text{ ELSE } \text{SKIP}, t_1) \rightarrow^*$
 $(\text{WHILE } b \text{ DO } c, t_2)$
by (blast *intro: star-trans*)
moreover have $\text{run-flow } (\text{flow cfs}) s = t_2$
 $(\subseteq \text{sources-aux } (\text{flow cfs}') (\text{run-flow } (\text{flow cfs}) s) x)$
proof
fix y
assume $y \in \text{sources-aux } (\text{flow cfs}')$
 $(\text{run-flow } (\text{flow cfs}) s) x$
hence $\text{sources } (\text{flow cfs}) s y \subseteq$
 $\text{sources-aux } (\text{flow cfs } @ \text{flow cfs}') s x$
by (rule *sources-aux-member*)
hence $\text{sources } (\text{flow cfs}) s y \subseteq$
 $\text{sources-aux } (\langle \text{bvars } b \rangle \# \text{flow cfs } @ \text{flow cfs}') s x$
using AC **by** *simp*
thus $\text{run-flow } (\text{flow cfs}) s y = t_2 y$
using Z **and** AB **by** *blast*
qed
hence $(\text{WHILE } b \text{ DO } c, t_2) \rightarrow^* (c_3', t_3) \wedge$
 $(c_2 = \text{SKIP}) = (c_3' = \text{SKIP})$
using AA **by** *simp*

```

ultimately have
  (IF b THEN c;; WHILE b DO c ELSE SKIP, t1) →*
    (c3', t3) ∧ (c2 = SKIP) = (c3' = SKIP)
  by (blast intro: star-trans)
}
moreover {
  fix x
  assume AB: s = t1
  (⊆ sources (⟨bvars b⟩ # flow cfs @ flow cfs') s x)
  have run-flow (flow cfs) s = t2
  (⊆ sources (flow cfs') (run-flow (flow cfs) s) x)
  proof
    fix y
    assume y ∈ sources (flow cfs')
    (run-flow (flow cfs) s) x
    hence sources (flow cfs) s y ⊆
      sources (flow cfs @ flow cfs') s x
    by (rule sources-member)
    moreover have sources (flow cfs @ flow cfs') s x ⊆
      sources (⟨bvars b⟩ # flow cfs @ flow cfs') s x
    by (rule sources-observe-tl)
    ultimately have sources (flow cfs) s y ⊆
      sources (⟨bvars b⟩ # flow cfs @ flow cfs') s x
    by simp
    thus run-flow (flow cfs) s y = t2 y
    using Z and AB by blast
  qed
  hence run-flow (flow cfs') (run-flow (flow cfs) s) x = t3 x
  using AA by simp
}
ultimately have ∃ c3' t3. ∀ x.
  (s = t1
    (⊆ sources-aux (⟨bvars b⟩ # flow cfs @ flow cfs') s x) →
      (IF b THEN c;; WHILE b DO c ELSE SKIP, t1) →* (c3', t3) ∧
        (c2 = SKIP) = (c3' = SKIP)) ∧
  (s = t1
    (⊆ sources (⟨bvars b⟩ # flow cfs @ flow cfs') s x) →
      run-flow (flow cfs') (run-flow (flow cfs) s) x = t3 x)
  by auto
}
ultimately show ?thesis
  using R by (auto simp: run-flow-append)
next
assume
  S: ¬ bval b s and
  T: flow cfs2 = ⟨bvars b⟩ # flow (tl cfs2)
assume (SKIP, s) →* {tl cfs2} (c2, s2)
hence U: (c2, s2) = (SKIP, s) ∧ flow (tl cfs2) = []
  by (rule small-steps-skip)

```

```

show ?thesis
proof (rule exI [of - SKIP], rule exI [of - t1])
{
  fix x
  assume s = t1 ( $\subseteq$  sources-aux [ $\langle$ bvars b $\rangle$ ] s x)
  hence s = t1 ( $\subseteq$  bvars b)
  using Q by (blast dest: sources-aux-observe-hd)
  hence  $\neg$  bval b t1
  using S by (blast dest: bvars-bval)
  hence (IF b THEN c;; WHILE b DO c ELSE SKIP, t1)  $\rightarrow$ 
    (SKIP, t1) ..
}
moreover {
  fix x
  assume s = t1 ( $\subseteq$  sources [ $\langle$ bvars b $\rangle$ ] s x)
  hence s x = t1 x
  by (subst (asm) append-Nil [symmetric],
    simp only: sources.simps, auto)
}
ultimately show  $\forall x$ .
  (s1 = t1 ( $\subseteq$  sources-aux (flow cfs2) s1 x)  $\longrightarrow$ 
    (c1, t1)  $\rightarrow^*$  (SKIP, t1)  $\wedge$  (c2 = SKIP) = (SKIP = SKIP))  $\wedge$ 
  (s1 = t1 ( $\subseteq$  sources (flow cfs2) s1 x)  $\longrightarrow$  s2 x = t1 x)
  using R and T and U by auto
qed
qed
next
assume R: bval b s
with F and O and P have S: s  $\in$  Univ B1' ( $\subseteq$  state  $\cap$  Y)
  by (drule-tac btyping2-approx [where s = s], auto)
assume (c;; WHILE b DO c, s)  $\rightarrow^*\{tl2\ cfs_1\}$  (c1, s1)
hence
  ( $\exists$  c' cfs'. c1 = c';; WHILE b DO c  $\wedge$ 
    (c, s)  $\rightarrow^*\{cfs'\}$  (c', s1)  $\wedge$ 
    flow (tl2 cfs1) = flow cfs')  $\vee$ 
  ( $\exists$  s' cfs' cfs''. length cfs'' < length (tl2 cfs1)  $\wedge$ 
    (c, s)  $\rightarrow^*\{cfs'\}$  (SKIP, s')  $\wedge$ 
    (WHILE b DO c, s')  $\rightarrow^*\{cfs''\}$  (c1, s1)  $\wedge$ 
    flow (tl2 cfs1) = flow cfs' @ flow cfs'')
  by (rule small-steps1-seq)
moreover {
  fix c' cfs
  assume
    T: (c, s)  $\rightarrow^*\{cfs\}$  (c', s1) and
    U: c1 = c';; WHILE b DO c
  hence V: (c';; WHILE b DO c, s1)  $\rightarrow^*\{cfs_2\}$  (c2, s2)
    using J by simp
  hence W: s2 = run-flow (flow cfs2) s1
    by (rule small-steps1-run-flow)
}

```

have
 $(\exists c'' \text{ cfs}'. c_2 = c'';; \text{ WHILE } b \text{ DO } c \wedge$
 $(c', s_1) \rightarrow^* \{\text{cfs}'\} (c'', s_2) \wedge$
 $\text{flow cfs}_2 = \text{flow cfs}') \vee$
 $(\exists s' \text{ cfs}' \text{ cfs}''. \text{length cfs}'' < \text{length cfs}_2 \wedge$
 $(c', s_1) \rightarrow^* \{\text{cfs}'\} (\text{SKIP}, s') \wedge$
 $(\text{ WHILE } b \text{ DO } c, s') \rightarrow^* \{\text{cfs}''\} (c_2, s_2) \wedge$
 $\text{flow cfs}_2 = \text{flow cfs}' @ \text{flow cfs}'')$
using V **by** (rule *small-stepsl-seq*)
moreover {
fix $c'' \text{ cfs}'$
assume $(c', s_1) \rightarrow^* \{\text{cfs}'\} (c'', s_2)$
then obtain c_2' **and** t_2 **where** $X: \forall x.$
 $(s_1 = t_1 (\subseteq \text{sources-aux } (\text{flow cfs}') s_1 x) \rightarrow$
 $(c', t_1) \rightarrow^* (c_2', t_2) \wedge (c'' = \text{SKIP}) = (c_2' = \text{SKIP})) \wedge$
 $(s_1 = t_1 (\subseteq \text{sources } (\text{flow cfs}') s_1 x) \rightarrow$
 $\text{run-flow } (\text{flow cfs}_2) s_1 x = t_2 x)$
using B [of $B_1 \ C \ B_1' \ D' \ s \ \text{cfs} \ c' \ s_1 \ \text{cfs}' \ c''$
 $\text{run-flow } (\text{flow cfs}_2) s_1]$ **and** N **and** S **and** T **and** W **by force**
assume
 $Y: c_2 = c'';; \text{ WHILE } b \text{ DO } c$ **and**
 $Z: \text{flow cfs}_2 = \text{flow cfs}'$
have *?thesis*
proof (rule *exI* [of - c_2' ;; $\text{ WHILE } b \text{ DO } c$], rule *exI* [of - t_2])
from U **and** W **and** X **and** Y **and** Z **show** $\forall x.$
 $(s_1 = t_1 (\subseteq \text{sources-aux } (\text{flow cfs}_2) s_1 x) \rightarrow$
 $(c_1, t_1) \rightarrow^* (c_2';; \text{ WHILE } b \text{ DO } c, t_2) \wedge$
 $(c_2 = \text{SKIP}) = (c_2';; \text{ WHILE } b \text{ DO } c = \text{SKIP})) \wedge$
 $(s_1 = t_1 (\subseteq \text{sources } (\text{flow cfs}_2) s_1 x) \rightarrow s_2 x = t_2 x)$
by (auto intro: *star-seq2*)
qed
}
moreover {
fix $s' \text{ cfs}' \text{ cfs}''$
assume
 $X: \text{length cfs}'' < \text{length cfs}_2$ **and**
 $Y: (c', s_1) \rightarrow^* \{\text{cfs}'\} (\text{SKIP}, s')$ **and**
 $Z: (\text{ WHILE } b \text{ DO } c, s') \rightarrow^* \{\text{cfs}''\} (c_2, s_2)$
then obtain c_2' **and** t_2 **where** $\forall x.$
 $(s_1 = t_1 (\subseteq \text{sources-aux } (\text{flow cfs}') s_1 x) \rightarrow$
 $(c', t_1) \rightarrow^* (c_2', t_2) \wedge (\text{SKIP} = \text{SKIP}) = (c_2' = \text{SKIP})) \wedge$
 $(s_1 = t_1 (\subseteq \text{sources } (\text{flow cfs}') s_1 x) \rightarrow s' x = t_2 x)$
using B [of $B_1 \ C \ B_1' \ D' \ s \ \text{cfs} \ c' \ s_1 \ \text{cfs}' \ \text{SKIP} \ s'$
and N **and** S **and** T **by force**
moreover have $AA: s' = \text{run-flow } (\text{flow cfs}') s_1$
using Y **by** (rule *small-stepsl-run-flow*)
ultimately have $AB: \forall x.$
 $(s_1 = t_1 (\subseteq \text{sources-aux } (\text{flow cfs}') s_1 x) \rightarrow$
 $(c', t_1) \rightarrow^* (\text{SKIP}, t_2)) \wedge$

$(s_1 = t_1 (\subseteq \text{sources } (\text{flow } cfs') s_1 x) \longrightarrow$
 $\text{run-flow } (\text{flow } cfs') s_1 x = t_2 x)$
 by *blast*
 have $AC: s_2 = \text{run-flow } (\text{flow } cfs'') s'$
 using Z by (*rule small-steps-l-run-flow*)
 moreover have $(c, s) \rightarrow^* \{cfs @ cfs'\} (SKIP, s')$
 using T and Y by (*simp add: small-steps-l-append*)
 hence $(c, s) \Rightarrow s'$
 by (*auto dest: small-steps-l-steps simp: big-iff-small*)
 hence $s' \in \text{Univ } C (\subseteq \text{state} \cap Y)$
 using M and R by *blast*
 ultimately obtain c_2' and t_3 where $AD: \forall x.$
 $(\text{run-flow } (\text{flow } cfs') s_1 = t_2$
 $(\subseteq \text{sources-aux } (\text{flow } cfs'') (\text{run-flow } (\text{flow } cfs') s_1) x) \longrightarrow$
 $(\text{WHILE } b \text{ DO } c, t_2) \rightarrow^* (c_2', t_3) \wedge$
 $(c_2 = SKIP) = (c_2' = SKIP)) \wedge$
 $(\text{run-flow } (\text{flow } cfs') s_1 = t_2$
 $(\subseteq \text{sources } (\text{flow } cfs'') (\text{run-flow } (\text{flow } cfs') s_1) x) \longrightarrow$
 $\text{run-flow } (\text{flow } cfs'') (\text{run-flow } (\text{flow } cfs') s_1) x = t_3 x)$
 using K [*of cfs'' [] cfs'' s' WHILE b DO c s*]
 and X and Z and AA by *force*
 moreover assume $\text{flow } cfs_2 = \text{flow } cfs' @ \text{flow } cfs''$
 moreover {
 fix x
 assume $AE: s_1 = t_1$
 $(\subseteq \text{sources-aux } (\text{flow } cfs' @ \text{flow } cfs'') s_1 x)$
 moreover have $\text{sources-aux } (\text{flow } cfs') s_1 x \subseteq$
 $\text{sources-aux } (\text{flow } cfs' @ \text{flow } cfs'') s_1 x$
 by (*rule sources-aux-append*)
 ultimately have $(c', t_1) \rightarrow^* (SKIP, t_2)$
 using AB by *blast*
 hence $(c';; \text{WHILE } b \text{ DO } c, t_1) \rightarrow^* (SKIP;; \text{WHILE } b \text{ DO } c, t_2)$
 by (*rule star-seq2*)
 hence $(c';; \text{WHILE } b \text{ DO } c, t_1) \rightarrow^* (\text{WHILE } b \text{ DO } c, t_2)$
 by (*blast intro: star-trans*)
 moreover have $\text{run-flow } (\text{flow } cfs') s_1 = t_2$
 $(\subseteq \text{sources-aux } (\text{flow } cfs'') (\text{run-flow } (\text{flow } cfs') s_1) x)$
 proof
 fix y
 assume $y \in \text{sources-aux } (\text{flow } cfs'')$
 $(\text{run-flow } (\text{flow } cfs') s_1) x$
 hence $\text{sources } (\text{flow } cfs') s_1 y \subseteq$
 $\text{sources-aux } (\text{flow } cfs' @ \text{flow } cfs'') s_1 x$
 by (*rule sources-aux-member*)
 thus $\text{run-flow } (\text{flow } cfs') s_1 y = t_2 y$
 using AB and AE by *blast*
 qed
 hence $(\text{WHILE } b \text{ DO } c, t_2) \rightarrow^* (c_2', t_3) \wedge$
 $(c_2 = SKIP) = (c_2' = SKIP)$


```

    using AD by simp
    ultimately have  $(c';; \text{WHILE } b \text{ DO } c, t_1) \rightarrow^* (c_2', t_3) \wedge$ 
       $(c_2 = \text{SKIP}) = (c_2' = \text{SKIP})$ 
    by (blast intro: star-trans)
  }
  moreover {
    fix x
    assume AE:  $s_1 = t_1$ 
       $(\subseteq \text{sources } (\text{flow } cfs' @ \text{flow } cfs'') s_1 x)$ 
    have  $\text{run-flow } (\text{flow } cfs') s_1 = t_2$ 
       $(\subseteq \text{sources } (\text{flow } cfs'') (\text{run-flow } (\text{flow } cfs') s_1) x)$ 
    proof
      fix y
      assume  $y \in \text{sources } (\text{flow } cfs'')$ 
         $(\text{run-flow } (\text{flow } cfs') s_1) x$ 
      hence  $\text{sources } (\text{flow } cfs') s_1 y \subseteq$ 
         $\text{sources } (\text{flow } cfs' @ \text{flow } cfs'') s_1 x$ 
      by (rule sources-member)
      thus  $\text{run-flow } (\text{flow } cfs') s_1 y = t_2 y$ 
      using AB and AE by blast
    qed
    hence  $\text{run-flow } (\text{flow } cfs'')$ 
       $(\text{run-flow } (\text{flow } cfs') s_1) x = t_3 x$ 
    using AD by simp
  }
  ultimately have ?thesis
    by (metis U AA AC)
}
ultimately have ?thesis
  by blast
}
moreover {
  fix  $s' cfs cfs'$ 
  assume
     $\text{length } cfs' < \text{length } (tl2 cfs_1)$  and
     $(c, s) \rightarrow^* \{cfs\} (\text{SKIP}, s')$  and
     $(\text{WHILE } b \text{ DO } c, s') \rightarrow^* \{cfs'\} (c_1, s_1)$ 
  moreover from this have  $(c, s) \Rightarrow s'$ 
    by (auto dest: small-stepsl-steps simp: big-iff-small)
  hence  $s' \in \text{Univ } C (\subseteq \text{state} \cap Y)$ 
    using M and R by blast
  ultimately have ?thesis
    using  $K [of cfs' @ cfs_2 cfs' cfs_2 s' c_1 s_1]$  and J by force
}
ultimately show ?thesis
  by blast
next
  assume  $(\text{SKIP}, s) \rightarrow^* \{tl2 cfs_1\} (c_1, s_1)$ 
  hence  $(c_1, s_1) = (\text{SKIP}, s)$ 

```

by (blast dest: small-steps-l-skip)
 moreover from this have $(c_2, s_2) = (SKIP, s) \wedge \text{flow } cfs_2 = []$
 using J by (blast dest: small-steps-l-skip)
 ultimately show ?thesis
 by auto
 qed
 qed
 }
 ultimately show
 $(\forall t_1. \exists c_2' t_2. \forall x.$
 $(s_1 = t_1 (\subseteq \text{sources-aux } (\text{flow } cfs_2) s_1 x) \longrightarrow$
 $(c_1, t_1) \rightarrow^* (c_2', t_2) \wedge (c_2 = SKIP) = (c_2' = SKIP)) \wedge$
 $(s_1 = t_1 (\subseteq \text{sources } (\text{flow } cfs_2) s_1 x) \longrightarrow s_2 x = t_2 x)) \wedge$
 $(\forall x. (\exists (B, Y) \in U. \exists s \in B. \exists y \in Y. \neg s: \text{dom } y \rightsquigarrow \text{dom } x) \longrightarrow$
 $\text{no-upd } (\text{flow } cfs_2) x)$
 using L by auto
 qed

lemma *ctyping2-correct-aux*:

$\llbracket (U, v) \models c (\subseteq A, X) = \text{Some } (B, Y); s \in \text{Univ } A (\subseteq \text{state} \cap X);$
 $(c, s) \rightarrow^* \{cfs_1\} (c_1, s_1); (c_1, s_1) \rightarrow^* \{cfs_2\} (c_2, s_2) \rrbracket \implies$
 $\text{ok-flow-aux } U c_1 c_2 s_1 s_2 (\text{flow } cfs_2)$
proof (induction $(U, v) c A X$ arbitrary: $B Y U v s c_1 c_2 s_1 s_2 cfs_1 cfs_2$
 rule: *ctyping2.induct*)
 fix $A X C Z U v c_1 c_2 c' c'' s s_1 s_2 cfs_1 cfs_2$
 show
 $\llbracket \bigwedge B Y s c' c'' s_1 s_2 cfs_1 cfs_2.$
 $(U, v) \models c_1 (\subseteq A, X) = \text{Some } (B, Y) \implies$
 $s \in \text{Univ } A (\subseteq \text{state} \cap X) \implies$
 $(c_1, s) \rightarrow^* \{cfs_1\} (c', s_1) \implies$
 $(c', s_1) \rightarrow^* \{cfs_2\} (c'', s_2) \implies$
 $(\forall t_1. \exists c_2' t_2. \forall x.$
 $(s_1 = t_1 (\subseteq \text{sources-aux } (\text{flow } cfs_2) s_1 x) \longrightarrow$
 $(c', t_1) \rightarrow^* (c_2', t_2) \wedge (c'' = SKIP) = (c_2' = SKIP)) \wedge$
 $(s_1 = t_1 (\subseteq \text{sources } (\text{flow } cfs_2) s_1 x) \longrightarrow s_2 x = t_2 x)) \wedge$
 $(\forall x. (\exists (B, W) \in U. \exists s \in B. \exists y \in W. \neg s: \text{dom } y \rightsquigarrow \text{dom } x) \longrightarrow$
 $\text{no-upd } (\text{flow } cfs_2) x);$
 $\bigwedge p B Y C Z s c' c'' s_1 s_2 cfs_1 cfs_2.$
 $(U, v) \models c_1 (\subseteq A, X) = \text{Some } p \implies$
 $(B, Y) = p \implies$
 $(U, v) \models c_2 (\subseteq B, Y) = \text{Some } (C, Z) \implies$
 $s \in \text{Univ } B (\subseteq \text{state} \cap Y) \implies$
 $(c_2, s) \rightarrow^* \{cfs_1\} (c', s_1) \implies$
 $(c', s_1) \rightarrow^* \{cfs_2\} (c'', s_2) \implies$
 $(\forall t_1. \exists c_2'' t_2. \forall x.$
 $(s_1 = t_1 (\subseteq \text{sources-aux } (\text{flow } cfs_2) s_1 x) \longrightarrow$
 $(c', t_1) \rightarrow^* (c_2'', t_2) \wedge (c'' = SKIP) = (c_2'' = SKIP)) \wedge$
 $(s_1 = t_1 (\subseteq \text{sources } (\text{flow } cfs_2) s_1 x) \longrightarrow s_2 x = t_2 x)) \wedge$
 $(\forall x. (\exists (B, W) \in U. \exists s \in B. \exists y \in W. \neg s: \text{dom } y \rightsquigarrow \text{dom } x) \longrightarrow$

$no_upd \ (flow \ cfs_2) \ x);$
 $(U, v) \models c_1;; c_2 \ (\subseteq A, X) = Some \ (C, Z);$
 $s \in Univ \ A \ (\subseteq state \cap X);$
 $(c_1;; c_2, s) \rightarrow^*\{cfs_1\} \ (c', s_1);$
 $(c', s_1) \rightarrow^*\{cfs_2\} \ (c'', s_2)] \Longrightarrow$
 $(\forall t_1. \exists c_2' \ t_2. \forall x.$
 $\quad (s_1 = t_1 \ (\subseteq sources_aux \ (flow \ cfs_2) \ s_1 \ x) \longrightarrow$
 $\quad (c', t_1) \rightarrow^* (c_2', t_2) \wedge (c'' = SKIP) = (c_2' = SKIP)) \wedge$
 $\quad (s_1 = t_1 \ (\subseteq sources \ (flow \ cfs_2) \ s_1 \ x) \longrightarrow s_2 \ x = t_2 \ x)) \wedge$
 $\quad (\forall x. (\exists (B, W) \in U. \exists s \in B. \exists y \in W. \neg s: dom \ y \rightsquigarrow dom \ x) \longrightarrow$
 $\quad no_upd \ (flow \ cfs_2) \ x)$
by (*auto del: conjI split: option.split-asm,*
rule ctyping2-correct-aux-seq)

next

fix $A \ X \ C \ Y \ U \ v \ b \ c_1 \ c_2 \ c' \ c'' \ s \ s_1 \ s_2 \ cfs_1 \ cfs_2$

show

$\llbracket \bigwedge U' \ p \ B_1 \ B_2 \ C \ Y \ s \ c' \ c'' \ s_1 \ s_2 \ cfs_1 \ cfs_2.$
 $\quad (U', p) = (insert \ (Univ? \ A \ X, \ bvars \ b) \ U, \models b \ (\subseteq A, X)) \Longrightarrow$
 $\quad (B_1, B_2) = p \Longrightarrow$
 $\quad (U', v) \models c_1 \ (\subseteq B_1, X) = Some \ (C, Y) \Longrightarrow$
 $\quad s \in Univ \ B_1 \ (\subseteq state \cap X) \Longrightarrow$
 $\quad (c_1, s) \rightarrow^*\{cfs_1\} \ (c', s_1) \Longrightarrow$
 $\quad (c', s_1) \rightarrow^*\{cfs_2\} \ (c'', s_2) \Longrightarrow$
 $\quad (\forall t_1. \exists c_2' \ t_2. \forall x.$
 $\quad \quad (s_1 = t_1 \ (\subseteq sources_aux \ (flow \ cfs_2) \ s_1 \ x) \longrightarrow$
 $\quad \quad (c', t_1) \rightarrow^* (c_2', t_2) \wedge (c'' = SKIP) = (c_2' = SKIP)) \wedge$
 $\quad \quad (s_1 = t_1 \ (\subseteq sources \ (flow \ cfs_2) \ s_1 \ x) \longrightarrow s_2 \ x = t_2 \ x)) \wedge$
 $\quad \quad (\forall x. (\exists (B, W) \in U'. \exists s \in B. \exists y \in W. \neg s: dom \ y \rightsquigarrow dom \ x) \longrightarrow$
 $\quad \quad no_upd \ (flow \ cfs_2) \ x);$
 $\bigwedge U' \ p \ B_1 \ B_2 \ C \ Y \ s \ c' \ c'' \ s_1 \ s_2 \ cfs_1 \ cfs_2.$
 $\quad (U', p) = (insert \ (Univ? \ A \ X, \ bvars \ b) \ U, \models b \ (\subseteq A, X)) \Longrightarrow$
 $\quad (B_1, B_2) = p \Longrightarrow$
 $\quad (U', v) \models c_2 \ (\subseteq B_2, X) = Some \ (C, Y) \Longrightarrow$
 $\quad s \in Univ \ B_2 \ (\subseteq state \cap X) \Longrightarrow$
 $\quad (c_2, s) \rightarrow^*\{cfs_1\} \ (c', s_1) \Longrightarrow$
 $\quad (c', s_1) \rightarrow^*\{cfs_2\} \ (c'', s_2) \Longrightarrow$
 $\quad (\forall t_1. \exists c_2'' \ t_2. \forall x.$
 $\quad \quad (s_1 = t_1 \ (\subseteq sources_aux \ (flow \ cfs_2) \ s_1 \ x) \longrightarrow$
 $\quad \quad (c', t_1) \rightarrow^* (c_2'', t_2) \wedge (c'' = SKIP) = (c_2'' = SKIP)) \wedge$
 $\quad \quad (s_1 = t_1 \ (\subseteq sources \ (flow \ cfs_2) \ s_1 \ x) \longrightarrow s_2 \ x = t_2 \ x)) \wedge$
 $\quad \quad (\forall x. (\exists (B, W) \in U'. \exists s \in B. \exists y \in W. \neg s: dom \ y \rightsquigarrow dom \ x) \longrightarrow$
 $\quad \quad no_upd \ (flow \ cfs_2) \ x);$
 $(U, v) \models IF \ b \ THEN \ c_1 \ ELSE \ c_2 \ (\subseteq A, X) = Some \ (C, Y);$
 $s \in Univ \ A \ (\subseteq state \cap X);$
 $(IF \ b \ THEN \ c_1 \ ELSE \ c_2, s) \rightarrow^*\{cfs_1\} \ (c', s_1);$
 $(c', s_1) \rightarrow^*\{cfs_2\} \ (c'', s_2)] \Longrightarrow$
 $(\forall t_1. \exists c_2' \ t_2. \forall x.$
 $\quad (s_1 = t_1 \ (\subseteq sources_aux \ (flow \ cfs_2) \ s_1 \ x) \longrightarrow$
 $\quad (c', t_1) \rightarrow^* (c_2', t_2) \wedge (c'' = SKIP) = (c_2' = SKIP)) \wedge$

$(s_1 = t_1 (\subseteq \text{sources} (\text{flow } cfs_2) s_1 x) \longrightarrow s_2 x = t_2 x)) \wedge$
 $(\forall x. (\exists (B, W) \in U. \exists s \in B. \exists y \in W. \neg s: \text{dom } y \rightsquigarrow \text{dom } x) \longrightarrow$
 $\text{no-upd } (\text{flow } cfs_2) x)$
by (*auto del: conjI split: option.split-asm prod.split-asm,*
rule ctying2-correct-aux-if)

next

fix $A X B Y U v b c c_1 c_2 s s_1 s_2 cfs_1 cfs_2$

show

$\llbracket \bigwedge B_1 B_2 C Y B_1' B_2' D Z s c_1 c_2 s_1 s_2 cfs_1 cfs_2.$
 $(B_1, B_2) = \models b (\subseteq A, X) \implies$
 $(C, Y) = \vdash c (\subseteq B_1, X) \implies$
 $(B_1', B_2') = \models b (\subseteq C, Y) \implies$
 $\forall (B, W) \in \text{insert } (\text{Univ? } A X \cup \text{Univ? } C Y, \text{bvars } b) U.$
 $B: \text{dom } ' W \rightsquigarrow \text{UNIV} \implies$
 $(\{\}, \text{False}) \models c (\subseteq B_1, X) = \text{Some } (D, Z) \implies$
 $s \in \text{Univ } B_1 (\subseteq \text{state} \cap X) \implies$
 $(c, s) \rightarrow^* \{cfs_1\} (c_1, s_1) \implies$
 $(c_1, s_1) \rightarrow^* \{cfs_2\} (c_2, s_2) \implies$
 $(\forall t_1. \exists c_2' t_2. \forall B_1.$
 $(s_1 = t_1 (\subseteq \text{sources-aux } (\text{flow } cfs_2) s_1 B_1) \longrightarrow$
 $(c_1, t_1) \rightarrow^* (c_2', t_2) \wedge (c_2 = \text{SKIP}) = (c_2' = \text{SKIP})) \wedge$
 $(s_1 = t_1 (\subseteq \text{sources } (\text{flow } cfs_2) s_1 B_1) \longrightarrow s_2 B_1 = t_2 B_1)) \wedge$
 $(\forall x. (\exists (B, W) \in \{\}. \exists s \in B. \exists y \in W. \neg s: \text{dom } y \rightsquigarrow \text{dom } x) \longrightarrow$
 $\text{no-upd } (\text{flow } cfs_2) x);$
 $\bigwedge B_1 B_2 C Y B_1' B_2' D' Z' s c_1 c_2 s_1 s_2 cfs_1 cfs_2.$
 $(B_1, B_2) = \models b (\subseteq A, X) \implies$
 $(C, Y) = \vdash c (\subseteq B_1, X) \implies$
 $(B_1', B_2') = \models b (\subseteq C, Y) \implies$
 $\forall (B, W) \in \text{insert } (\text{Univ? } A X \cup \text{Univ? } C Y, \text{bvars } b) U.$
 $B: \text{dom } ' W \rightsquigarrow \text{UNIV} \implies$
 $(\{\}, \text{False}) \models c (\subseteq B_1', Y) = \text{Some } (D', Z') \implies$
 $s \in \text{Univ } B_1' (\subseteq \text{state} \cap Y) \implies$
 $(c, s) \rightarrow^* \{cfs_1\} (c_1, s_1) \implies$
 $(c_1, s_1) \rightarrow^* \{cfs_2\} (c_2, s_2) \implies$
 $(\forall t_1. \exists c_2' t_2. \forall B_1.$
 $(s_1 = t_1 (\subseteq \text{sources-aux } (\text{flow } cfs_2) s_1 B_1) \longrightarrow$
 $(c_1, t_1) \rightarrow^* (c_2', t_2) \wedge (c_2 = \text{SKIP}) = (c_2' = \text{SKIP})) \wedge$
 $(s_1 = t_1 (\subseteq \text{sources } (\text{flow } cfs_2) s_1 B_1) \longrightarrow s_2 B_1 = t_2 B_1)) \wedge$
 $(\forall x. (\exists (B, W) \in \{\}. \exists s \in B. \exists y \in W. \neg s: \text{dom } y \rightsquigarrow \text{dom } x) \longrightarrow$
 $\text{no-upd } (\text{flow } cfs_2) x);$
 $(U, v) \models \text{WHILE } b \text{ DO } c (\subseteq A, X) = \text{Some } (B, Y);$
 $s \in \text{Univ } A (\subseteq \text{state} \cap X);$
 $(\text{WHILE } b \text{ DO } c, s) \rightarrow^* \{cfs_1\} (c_1, s_1);$
 $(c_1, s_1) \rightarrow^* \{cfs_2\} (c_2, s_2) \rrbracket \implies$
 $(\forall t_1. \exists c_2' t_2. \forall x.$
 $(s_1 = t_1 (\subseteq \text{sources-aux } (\text{flow } cfs_2) s_1 x) \longrightarrow$
 $(c_1, t_1) \rightarrow^* (c_2', t_2) \wedge (c_2 = \text{SKIP}) = (c_2' = \text{SKIP})) \wedge$
 $(s_1 = t_1 (\subseteq \text{sources } (\text{flow } cfs_2) s_1 x) \longrightarrow s_2 x = t_2 x)) \wedge$
 $(\forall x. (\exists (B, W) \in U. \exists s \in B. \exists y \in W. \neg s: \text{dom } y \rightsquigarrow \text{dom } x) \longrightarrow$

$no-upd \ (flow \ cfs_2) \ x)$
by (*auto del: conjI split: option.split-asm prod.split-asm,*
rule ctying2-correct-aux-while, assumption+, blast)
qed (*auto del: conjI split: prod.split-asm*)

theorem *ctying2-correct:*

assumes $A: (U, v) \models c \ (\subseteq A, X) = Some \ (B, Y)$

shows *correct c A X*

proof –

{
fix $c_1 \ c_2 \ s_1 \ s_2 \ cfs \ t_1$
assume *ok-flow-aux* $U \ c_1 \ c_2 \ s_1 \ s_2 \ (flow \ cfs)$
then obtain c_2' **and** t_2 **where** $A: \forall x.$
 $(s_1 = t_1 \ (\subseteq \ sources\text{-}aux \ (flow \ cfs) \ s_1 \ x) \longrightarrow$
 $(c_1, t_1) \rightarrow^* (c_2', t_2) \wedge (c_2 = SKIP) = (c_2' = SKIP)) \wedge$
 $(s_1 = t_1 \ (\subseteq \ sources \ (flow \ cfs) \ s_1 \ x) \longrightarrow s_2 \ x = t_2 \ x)$
by *blast*
have $\exists c_2' \ t_2. \forall x. s_1 = t_1 \ (\subseteq \ sources \ (flow \ cfs) \ s_1 \ x) \longrightarrow$
 $(c_1, t_1) \rightarrow^* (c_2', t_2) \wedge (c_2 = SKIP) = (c_2' = SKIP) \wedge s_2 \ x = t_2 \ x$
proof (*rule exI [of - c₂'], rule exI [of - t₂]*)
have $\forall x. s_1 = t_1 \ (\subseteq \ sources \ (flow \ cfs) \ s_1 \ x) \longrightarrow$
 $s_1 = t_1 \ (\subseteq \ sources\text{-}aux \ (flow \ cfs) \ s_1 \ x)$
proof (*rule allI, rule impI*)
fix x
assume $s_1 = t_1 \ (\subseteq \ sources \ (flow \ cfs) \ s_1 \ x)$
moreover have *sources-aux* $(flow \ cfs) \ s_1 \ x \subseteq$
 $sources \ (flow \ cfs) \ s_1 \ x$
by (*rule sources-aux-sources*)
ultimately show $s_1 = t_1 \ (\subseteq \ sources\text{-}aux \ (flow \ cfs) \ s_1 \ x)$
by *blast*
qed
with A **show** $\forall x. s_1 = t_1 \ (\subseteq \ sources \ (flow \ cfs) \ s_1 \ x) \longrightarrow$
 $(c_1, t_1) \rightarrow^* (c_2', t_2) \wedge (c_2 = SKIP) = (c_2' = SKIP) \wedge s_2 \ x = t_2 \ x$
by *auto*
qed
}
with A **show** *?thesis*
by (*clarsimp dest!: small-steps-stepsl simp: correct-def,*
drule-tac ctying2-correct-aux, auto)
qed

end

end

5 Degeneracy to stateless level-based information flow control

```

theory Degeneracy
  imports Correctness HOL-IMP.Sec-TypingT
begin

```

The goal of this concluding section is to prove the degeneracy of the information flow correctness notion and the static type system defined in this paper to the classical counterparts addressed in [7], section 9.2.6, and formalized in [5] and [6], in case of a stateless level-based information flow correctness policy.

First of all, locale *noninterf* is interpreted within the context of the class *sec* defined in [5], as follows.

- Parameter *dom* is instantiated as function *sec*, which also sets the type variable standing for the type of the domains to *nat*.
- Parameter *interf* is instantiated as the predicate such that for any program state, the output is *True* just in case the former input level may interfere with, namely is not larger than, the latter one.
- Parameter *state* is instantiated as the empty set, consistently with the fact that the policy is represented by a single, stateless interference predicate.

Next, the information flow security notion implied by theorem *noninterference* in [6] is formalized as a predicate *secure* taking a program as input. This notion is then proven to be implied, in the degenerate interpretation described above, by the information flow correctness notion formalized as predicate *correct* (theorem *correct-secure*). Particularly:

- This theorem demands the additional assumption that the *state set* *A* input to *correct* is nonempty, since *correct* is vacuously true for $A = \{\}$.
- In order for this theorem to hold, predicate *secure* needs to slightly differ from the information flow security notion implied by theorem *noninterference*, in that it requires state t' to exist if there also exists some variable with a level not larger than l , namely if condition $s = t$ ($\leq l$) is satisfied *nontrivially* – actually, no leakage may arise from two initial states disagreeing on the value of *every* variable. In fact, predicate *correct* requires a nontrivial configuration (c_2', t_2) to exist in case condition $s_1 = t_1$ ($\subseteq \text{sources } cs \ s_1 \ x$) is satisfied *for some variable* x .

Finally, the static type system *ctyping2* is proven to be equivalent to the *sec-type* one defined in [6] in the above degenerate interpretation (theorems *ctyping2-sec-type* and *sec-type-ctyping2*). The former theorem, which proves that a *pass* verdict from *ctyping2* implies the issuance of a *pass* verdict from *sec-type* as well, demands the additional assumptions that (a) the *state set* input to *ctyping2* is nonempty, (b) the input program does not contain any loop with *Bc True* as boolean condition, and (c) the input program has undergone *constant folding*, as addressed in [7], section 3.1.3 for arithmetic expressions and in [7], section 3.2.1 for boolean expressions. Why?

This need arises from the different ways in which the two type systems handle “dead” conditional branches. Type system *sec-type* does not try to detect “dead” branches; it simply applies its full range of information flow security checks to any conditional branch contained in the input program, even if it actually is a “dead” one. On the contrary, type system *ctyping2* detects “dead” branches whenever boolean conditions can be evaluated at compile time, and applies only a subset of its information flow correctness checks to such branches.

As parameter *state* is instantiated as the empty set, boolean conditions containing variables cannot be evaluated at compile time, yet they can if they only contain constants. Thus, assumption (a) prevents *ctyping2* from handling the entire input program as a “dead” branch, while assumptions (b) and (c) ensure that *ctyping2* will not detect any “dead” conditional branch within the program. On the whole, those assumptions guarantee that *ctyping2*, like *sec-type*, applies its full range of checks to *any* conditional branch contained in the input program, as required for theorem *ctyping2-sec-type* to hold.

5.1 Global context definitions and proofs

```
fun cgood :: com  $\Rightarrow$  bool where
  cgood (c1;; c2) = (cgood c1  $\wedge$  cgood c2) |
  cgood (IF - THEN c1 ELSE c2) = (cgood c1  $\wedge$  cgood c2) |
  cgood (WHILE b DO c) = (b  $\neq$  Bc True  $\wedge$  cgood c) |
  cgood - = True
```

```
fun seq :: com  $\Rightarrow$  com  $\Rightarrow$  com where
  seq SKIP c = c |
  seq c SKIP = c |
  seq c1 c2 = c1;; c2
```

```
fun ifc :: bexp  $\Rightarrow$  com  $\Rightarrow$  com  $\Rightarrow$  com where
  ifc (Bc True) c - = c |
  ifc (Bc False) - c = c |
  ifc b c1 c2 = (if c1 = c2 then c1 else IF b THEN c1 ELSE c2)
```

fun *while* :: *bexp* \Rightarrow *com* \Rightarrow *com* **where**
while (*Bc False*) = *SKIP* |
while *b c* = *WHILE b DO c*

primrec *csimp* :: *com* \Rightarrow *com* **where**
csimp SKIP = *SKIP* |
csimp (*x ::= a*) = *x ::= asimp a* |
csimp (*c₁;; c₂*) = *seq (csimp c₁) (csimp c₂)* |
csimp (*IF b THEN c₁ ELSE c₂*) = *ifc (bsimp b) (csimp c₁) (csimp c₂)* |
csimp (*WHILE b DO c*) = *while (bsimp b) (csimp c)*

lemma *not-size*:
size (not b) \leq *Suc (size b)*
by (*induction b rule: not.induct, simp-all*)

lemma *and-size*:
size (and b₁ b₂) \leq *Suc (size b₁ + size b₂)*
by (*induction b₁ b₂ rule: and.induct, simp-all*)

lemma *less-size*:
size (less a₁ a₂) = 0
by (*induction a₁ a₂ rule: less.induct, simp-all*)

lemma *bsimp-size*:
size (bsimp b) \leq *size b*
by (*induction b, auto intro: le-trans not-size and-size simp: less-size*)

lemma *seq-size*:
size (seq c₁ c₂) \leq *Suc (size c₁ + size c₂)*
by (*induction c₁ c₂ rule: seq.induct, simp-all*)

lemma *ifc-size*:
size (ifc b c₁ c₂) \leq *Suc (size c₁ + size c₂)*
by (*induction b c₁ c₂ rule: ifc.induct, simp-all*)

lemma *while-size*:
size (while b c) \leq *Suc (size c)*
by (*induction b c rule: while.induct, simp-all*)

lemma *csimp-size*:
size (csimp c) \leq *size c*
by (*induction c, auto intro: le-trans seq-size ifc-size while-size*)

lemma *avars-arsimp*:
avars a = {} \Longrightarrow $\exists i. asimp a = N i$

by (*induction a, auto*)

lemma *seq-match* [*dest!*]:

seq (*csimp c₁*) (*csimp c₂*) = *c₁*;; *c₂* \implies *csimp c₁* = *c₁* \wedge *csimp c₂* = *c₂*
by (*rule seq.cases* [*of* (*csimp c₁*, *csimp c₂*)],
insert csimp-size [*of c₁*], *insert csimp-size* [*of c₂*], *simp-all*)

lemma *ifc-match* [*dest!*]:

ifc (*bsimp b*) (*csimp c₁*) (*csimp c₂*) = *IF b THEN c₁ ELSE c₂* \implies
bsimp b = *b* \wedge ($\forall v. b \neq Bc\ v$) \wedge *csimp c₁* = *c₁* \wedge *csimp c₂* = *c₂*
by (*insert csimp-size* [*of c₁*], *insert csimp-size* [*of c₂*],
subgoal-tac csimp c₁ \neq IF b THEN c₁ ELSE c₂, auto intro: ifc.cases
[of (bsimp b, csimp c₁, csimp c₂)] split: if-split-asm)

lemma *while-match* [*dest!*]:

while (*bsimp b*) (*csimp c*) = *WHILE b DO c* \implies
bsimp b = *b* \wedge *b* $\neq Bc\ False$ \wedge *csimp c* = *c*
by (*rule while.cases* [*of* (*bsimp b*, *csimp c*)], *auto*)

5.2 Local context definitions and proofs

context *sec*

begin

interpretation *noninterf* $\lambda s. (\leq)\ sec\ \{\}$

by (*unfold-locales, simp*)

notation *interf-set* ($\langle (- : - \rightsquigarrow -) \rangle$) [*51, 51, 51*] *50*)

notation *univ-states-if* ($\langle (Univ? - -) \rangle$) [*51, 75*] *75*)

notation *atyping* ($\langle (- \models -'(\subseteq -')) \rangle$) [*51, 51*] *50*)

notation *btyping2-aux* ($\langle (\models -'(\subseteq -, -')) \rangle$) [*51*] *55*)

notation *btyping2* ($\langle (\models -'(\subseteq -, -')) \rangle$) [*51*] *55*)

notation *ctyping1* ($\langle (\vdash -'(\subseteq -, -')) \rangle$) [*51*] *55*)

notation *ctyping2* ($\langle (- \models -'(\subseteq -, -')) \rangle$) [*51, 51*] *55*)

abbreviation *eq-le-ext* :: *state* \Rightarrow *state* \Rightarrow *level* \Rightarrow *bool*

($\langle (- = -'(\leq -)) \rangle$) [*51, 51, 0*] *50*) **where**
s = *t* (\leq *l*) \equiv *s* = *t* (\leq *l*) \wedge ($\exists x :: vname. sec\ x \leq l$)

definition *secure* :: *com* \Rightarrow *bool* **where**

secure c $\equiv \forall s\ s'\ t\ l. (c, s) \Rightarrow s' \wedge s = t\ (\leq\ l) \longrightarrow$
($\exists t'. (c, t) \Rightarrow t' \wedge s' = t'\ (\leq\ l)$)

definition *levels* :: *config set* \Rightarrow *level set* **where**

levels U $\equiv insert\ 0\ (sec\ ' \bigcup\ (snd\ ' \{(B, Y) \in U. B \neq \{\}\}))$

lemma *avars-finite*:
finite (avars a)
by (*induction a, simp-all*)

lemma *avars-in*:
 $n < \text{sec } a \implies \text{sec } a \in \text{sec } ' \text{avars } a$
by (*induction a, auto simp: max-def*)

lemma *avars-sec*:
 $x \in \text{avars } a \implies \text{sec } x \leq \text{sec } a$
by (*induction a, auto*)

lemma *avars-ub*:
 $\text{sec } a \leq l = (\forall x \in \text{avars } a. \text{sec } x \leq l)$
by (*induction a, auto*)

lemma *bvars-finite*:
finite (bvars b)
by (*induction b, simp-all add: avars-finite*)

lemma *bvars-in*:
 $n < \text{sec } b \implies \text{sec } b \in \text{sec } ' \text{bvars } b$
by (*induction b, auto dest!: avars-in simp: max-def*)

lemma *bvars-sec*:
 $x \in \text{bvars } b \implies \text{sec } x \leq \text{sec } b$
by (*induction b, auto dest: avars-sec*)

lemma *bvars-ub*:
 $\text{sec } b \leq l = (\forall x \in \text{bvars } b. \text{sec } x \leq l)$
by (*induction b, auto simp: avars-ub*)

lemma *levels-insert*:
assumes
 $A: A \neq \{\}$ **and**
 $B: \text{finite } (\text{levels } U)$
shows $\text{finite } (\text{levels } (\text{insert } (A, \text{bvars } b) U)) \wedge$
 $\text{Max } (\text{levels } (\text{insert } (A, \text{bvars } b) U)) = \text{max } (\text{sec } b) (\text{Max } (\text{levels } U))$
 $(\text{is finite } (\text{levels } ?U') \wedge ?P)$
proof –
have $C: \text{levels } ?U' = \text{sec } ' \text{bvars } b \cup \text{levels } U$
using A **by** (*auto simp: image-def levels-def univ-states-if-def*)
hence $D: \text{finite } (\text{levels } ?U')$
using B **by** (*simp add: bvars-finite*)
moreover have $?P$
proof (*rule Max-eqI [OF D]*)
fix l

```

    assume  $l \in \text{levels } (\text{insert } (A, \text{bvars } b) \ U)$ 
    thus  $l \leq \text{max } (\text{sec } b) \ (\text{Max } (\text{levels } U))$ 
    using  $C$  by (auto dest:  $\text{Max-ge } [OF \ B] \ \text{bvars-sec}$ )
next
  show  $\text{max } (\text{sec } b) \ (\text{Max } (\text{levels } U)) \in \text{levels } (\text{insert } (A, \text{bvars } b) \ U)$ 
  using  $C$  by (insert  $\text{Max-in } [OF \ B]$ ,
    fastforce dest:  $\text{bvars-in simp: max-def not-le levels-def}$ )
qed
ultimately show ?thesis ..
qed

```

lemma *sources-le*:

```

 $y \in \text{sources } cs \ s \ x \implies \text{sec } y \leq \text{sec } x$ 
and sources-aux-le:
 $y \in \text{sources-aux } cs \ s \ x \implies \text{sec } y \leq \text{sec } x$ 
by (induction  $cs \ s \ x$  and  $cs \ s \ x$  rule: sources-induct,
  auto split: com-flow.split-asm if-split-asm, fastforce+)

```

lemma *bsimp-btyping2-aux-not [intro]*:

```

 $\llbracket \text{bsimp } b = b \implies \forall v. b \neq Bc \ v \implies \models b \ (\subseteq A, X) = \text{None};$ 
 $\text{not } (\text{bsimp } b) = \text{Not } b \rrbracket \implies \models b \ (\subseteq A, X) = \text{None}$ 
by (rule not.cases [of bsimp b], auto)

```

lemma *bsimp-btyping2-aux-and [intro]*:

```

assumes
  A:  $\llbracket \text{bsimp } b_1 = b_1; \forall v. b_1 \neq Bc \ v \rrbracket \implies \models b_1 \ (\subseteq A, X) = \text{None}$  and
  B:  $\text{and } (\text{bsimp } b_1) \ (\text{bsimp } b_2) = \text{And } b_1 \ b_2$ 
shows  $\models b_1 \ (\subseteq A, X) = \text{None}$ 
proof -
  {
    assume  $\text{bsimp } b_2 = \text{And } b_1 \ b_2$ 
    hence  $Bc \ \text{True} = b_1$ 
    by (insert bsimp-size [of  $b_2$ ], simp)
  }
  moreover {
    assume  $\text{bsimp } b_2 = \text{And } (Bc \ \text{True}) \ b_2$ 
    hence False
    by (insert bsimp-size [of  $b_2$ ], simp)
  }
  moreover {
    assume  $\text{bsimp } b_1 = \text{And } b_1 \ b_2$ 
    hence False
    by (insert bsimp-size [of  $b_1$ ], simp)
  }
  ultimately have  $\text{bsimp } b_1 = b_1 \wedge (\forall v. b_1 \neq Bc \ v)$ 
  using  $B$  by (auto intro: and.cases [of  $(\text{bsimp } b_1, \text{bsimp } b_2)$ ])
  thus ?thesis
  using  $A$  by simp

```

qed

lemma *bsimp-btyping2-aux-less* [elim]:

$\llbracket \text{less } (asimp\ a_1)\ (asimp\ a_2) = \text{Less } a_1\ a_2;$
 $\text{avars } a_1 = \{\}; \text{ avars } a_2 = \{\} \rrbracket \implies \text{False}$
by (*fastforce dest: avars-asimp*)

lemma *bsimp-btyping2-aux*:

$\llbracket bsimp\ b = b; \forall v. b \neq Bc\ v \rrbracket \implies \models b\ (\subseteq A, X) = \text{None}$
by (*induction b, auto split: option.split*)

lemma *bsimp-btyping2*:

$\llbracket bsimp\ b = b; \forall v. b \neq Bc\ v \rrbracket \implies \models b\ (\subseteq A, X) = (A, A)$
by (*auto dest: bsimp-btyping2-aux [of - A X] simp: btyping2-def*)

lemma *csimp-ctyping2-if*:

$\llbracket \bigwedge U' B B'. U' = U \implies B = B_1 \implies \{\} = B' \implies B_1 \neq \{\} \implies \text{False}; s \in A;$
 $\models b\ (\subseteq A, X) = (B_1, B_2); bsimp\ b = b; \forall v. b \neq Bc\ v \rrbracket \implies$
 False
by (*drule bsimp-btyping2 [of - A X], auto*)

lemma *csimp-ctyping2-while*:

$\llbracket (\text{if } P \text{ then } \text{Some } (B_2 \cup B_2', Y) \text{ else } \text{None}) = \text{Some } (\{\}, Z); s \in A;$
 $\models b\ (\subseteq A, X) = (B_1, B_2); bsimp\ b = b; b \neq Bc\ \text{True}; b \neq Bc\ \text{False} \rrbracket \implies$
 False
by (*drule bsimp-btyping2 [of - A X], auto split: if-split-asm*)

lemma *csimp-ctyping2*:

$\llbracket (U, v) \models c\ (\subseteq A, X) = \text{Some } (B, Y); A \neq \{\}; cgood\ c; csimp\ c = c \rrbracket \implies$
 $B \neq \{\}$

proof (*induction (U, v) c A X arbitrary: B Y U v rule: ctyping2.induct*)

fix *A X B Y U v c₁ c₂*

show

$\llbracket \bigwedge B Y. (U, v) \models c_1\ (\subseteq A, X) = \text{Some } (B, Y) \implies$
 $A \neq \{\} \implies cgood\ c_1 \implies csimp\ c_1 = c_1 \implies$
 $B \neq \{\};$
 $\bigwedge_p B Y C Z. (U, v) \models c_1\ (\subseteq A, X) = \text{Some } p \implies$
 $(B, Y) = p \implies (U, v) \models c_2\ (\subseteq B, Y) = \text{Some } (C, Z) \implies$
 $B \neq \{\} \implies cgood\ c_2 \implies csimp\ c_2 = c_2 \implies$
 $C \neq \{\};$
 $(U, v) \models c_1;; c_2\ (\subseteq A, X) = \text{Some } (B, Y);$
 $A \neq \{\}; cgood\ (c_1;; c_2);$
 $csimp\ (c_1;; c_2) = c_1;; c_2 \rrbracket \implies$
 $B \neq \{\}$

by (*fastforce split: option.split-asm*)

next

fix *A X C Y U v b c₁ c₂*

show

$\llbracket \bigwedge U' p B_1 B_2 C Y.$
 $(U', p) = (\text{insert } (\text{Univ? } A X, \text{bvars } b) U, \models b (\subseteq A, X)) \implies$
 $(B_1, B_2) = p \implies (U', v) \models c_1 (\subseteq B_1, X) = \text{Some } (C, Y) \implies$
 $B_1 \neq \{\} \implies \text{cgood } c_1 \implies \text{csimp } c_1 = c_1 \implies$
 $C \neq \{\};$
 $\bigwedge U' p B_1 B_2 C Y.$
 $(U', p) = (\text{insert } (\text{Univ? } A X, \text{bvars } b) U, \models b (\subseteq A, X)) \implies$
 $(B_1, B_2) = p \implies (U', v) \models c_2 (\subseteq B_2, X) = \text{Some } (C, Y) \implies$
 $B_2 \neq \{\} \implies \text{cgood } c_2 \implies \text{csimp } c_2 = c_2 \implies$
 $C \neq \{\};$
 $(U, v) \models \text{IF } b \text{ THEN } c_1 \text{ ELSE } c_2 (\subseteq A, X) = \text{Some } (C, Y);$
 $A \neq \{\}; \text{cgood } (\text{IF } b \text{ THEN } c_1 \text{ ELSE } c_2);$
 $\text{csimp } (\text{IF } b \text{ THEN } c_1 \text{ ELSE } c_2) = \text{IF } b \text{ THEN } c_1 \text{ ELSE } c_2 \rrbracket \implies$
 $C \neq \{\}$
by (*auto split: option.split-asm prod.split-asm,*
rule csimp-ctyping2-if)
next
fix $A X B Z U v b c$
show
 $\llbracket \bigwedge B_1 B_2 C Y B_1' B_2' B Z.$
 $(B_1, B_2) = \models b (\subseteq A, X) \implies$
 $(C, Y) = \vdash c (\subseteq B_1, X) \implies$
 $(B_1', B_2') = \models b (\subseteq C, Y) \implies$
 $\forall (B, W) \in \text{insert } (\text{Univ? } A X \cup \text{Univ? } C Y, \text{bvars } b) U.$
 $B: \text{sec ' } W \rightsquigarrow \text{UNIV} \implies$
 $(\{\}, \text{False}) \models c (\subseteq B_1, X) = \text{Some } (B, Z) \implies$
 $B_1 \neq \{\} \implies \text{cgood } c \implies \text{csimp } c = c \implies$
 $B \neq \{\};$
 $\bigwedge B_1 B_2 C Y B_1' B_2' B Z.$
 $(B_1, B_2) = \models b (\subseteq A, X) \implies$
 $(C, Y) = \vdash c (\subseteq B_1, X) \implies$
 $(B_1', B_2') = \models b (\subseteq C, Y) \implies$
 $\forall (B, W) \in \text{insert } (\text{Univ? } A X \cup \text{Univ? } C Y, \text{bvars } b) U.$
 $B: \text{sec ' } W \rightsquigarrow \text{UNIV} \implies$
 $(\{\}, \text{False}) \models c (\subseteq B_1', Y) = \text{Some } (B, Z) \implies$
 $B_1' \neq \{\} \implies \text{cgood } c \implies \text{csimp } c = c \implies$
 $B \neq \{\};$
 $(U, v) \models \text{WHILE } b \text{ DO } c (\subseteq A, X) = \text{Some } (B, Z);$
 $A \neq \{\}; \text{cgood } (\text{WHILE } b \text{ DO } c);$
 $\text{csimp } (\text{WHILE } b \text{ DO } c) = \text{WHILE } b \text{ DO } c \rrbracket \implies$
 $B \neq \{\}$
by (*auto split: option.split-asm prod.split-asm,*
rule csimp-ctyping2-while)
qed (*simp-all split: if-split-asm*)

theorem *correct-secure:*
assumes
 $A: \text{correct } c A X$ **and**

```

    B:  $A \neq \{\}$ 
  shows secure c
proof -
  {
    fix  $s\ s'\ t\ l$  and  $x :: \text{vname}$ 
    assume  $(c, s) \Rightarrow s'$ 
    then obtain  $cfs$  where  $C: (c, s) \rightarrow^* \{cfs\} (SKIP, s')$ 
      by (auto dest: small-steps-stepsl simp: big-iff-small)
    assume  $D: s = t (\leq l)$ 
    have  $E: \forall x. \text{sec } x \leq l \longrightarrow s = t (\subseteq \text{sources } (\text{flow } cfs) s\ x)$ 
    proof (rule allI, rule impI)
      fix  $x :: \text{vname}$ 
      assume  $\text{sec } x \leq l$ 
      moreover have  $\text{sources } (\text{flow } cfs) s\ x \subseteq \{y. \text{sec } y \leq \text{sec } x\}$ 
        by (rule subsetI, simp, rule sources-le)
      ultimately show  $s = t (\subseteq \text{sources } (\text{flow } cfs) s\ x)$ 
        using  $D$  by auto
    qed
    assume  $\forall s\ c_1\ c_2\ s_1\ s_2\ cfs.$ 
       $(c, s) \rightarrow^* (c_1, s_1) \wedge (c_1, s_1) \rightarrow^* \{cfs\} (c_2, s_2) \longrightarrow$ 
       $(\forall t_1. \exists c_2'\ t_2. \forall x.$ 
         $s_1 = t_1 (\subseteq \text{sources } (\text{flow } cfs) s_1\ x) \longrightarrow$ 
         $(c_1, t_1) \rightarrow^* (c_2', t_2) \wedge (c_2 = SKIP) = (c_2' = SKIP) \wedge$ 
         $s_2\ x = t_2\ x)$ 
    note  $F = \text{this}$  [rule-format]
    obtain  $t'$  where  $G: \forall x.$ 
       $s = t (\subseteq \text{sources } (\text{flow } cfs) s\ x) \longrightarrow$ 
       $(c, t) \rightarrow^* (SKIP, t') \wedge s'\ x = t'\ x$ 
    using  $F$  [of  $s\ c\ s\ cfs\ SKIP\ s'\ t$ ] and  $C$  by blast
    assume  $H: \text{sec } x \leq l$ 
    {
      have  $s = t (\subseteq \text{sources } (\text{flow } cfs) s\ x)$ 
      using  $E$  and  $H$  by simp
      hence  $(c, t) \Rightarrow t'$ 
      using  $G$  by (simp add: big-iff-small)
    }
    moreover {
      fix  $x :: \text{vname}$ 
      assume  $\text{sec } x \leq l$ 
      hence  $s = t (\subseteq \text{sources } (\text{flow } cfs) s\ x)$ 
      using  $E$  by simp
      hence  $s'\ x = t'\ x$ 
      using  $G$  by simp
    }
    ultimately have  $\exists t'. (c, t) \Rightarrow t' \wedge s' = t' (\leq l)$ 
    by auto
  }
with  $A$  and  $B$  show ?thesis
  by (auto simp: correct-def secure-def split: if-split-asm)

```

qed

lemma *ctyping2-sec-type-assign* [elim]:

assumes

$A: (\text{if } ((\exists s. s \in \text{Univ? } A \ X) \longrightarrow (\forall y \in \text{avars } a. \text{sec } y \leq \text{sec } x)) \wedge$
 $(\forall p \in U. \forall B \ Y. p = (B, Y) \longrightarrow B = \{\} \vee (\forall y \in Y. \text{sec } y \leq \text{sec } x))$
 $\text{then Some } (\text{if } x \in \{\} \wedge A \neq \{\}$
 $\text{then if } v \models a \ (\subseteq X)$
 $\text{then } (\{s(x := \text{aval } a \ s) \mid s. s \in A\}, \text{insert } x \ X) \text{ else } (A, X - \{x\})$
 $\text{else } (A, \text{Univ?? } A \ X))$
 $\text{else None} = \text{Some } (B, Y)$
 $(\text{is } (\text{if } (- \longrightarrow ?P) \wedge ?Q \text{ then } - \text{ else } -) = -) \text{ and}$
 $B: s \in A \text{ and}$
 $C: \text{finite } (\text{levels } U)$

shows $\text{Max } (\text{levels } U) \vdash x ::= a$

proof –

have $?P \wedge ?Q$

using A **and** B **by** (*auto simp: univ-states-if-def split: if-split-asm*)

moreover from this have $\text{Max } (\text{levels } U) \leq \text{sec } x$

using C **by** (*subst Max-le-iff, auto simp: levels-def, blast*)

ultimately show $\text{Max } (\text{levels } U) \vdash x ::= a$

by (*auto intro: Assign simp: avars-ub*)

qed

lemma *ctyping2-sec-type-seq*:

assumes

$A: \bigwedge B' s. B = B' \implies s \in A \implies \text{Max } (\text{levels } U) \vdash c_1 \text{ and}$
 $B: \bigwedge B' B'' C Z s'. B = B' \implies B'' = B' \implies$
 $(U, v) \models c_2 (\subseteq B', Y) = \text{Some } (C, Z) \implies$
 $s' \in B' \implies \text{Max } (\text{levels } U) \vdash c_2 \text{ and}$
 $C: (U, v) \models c_1 (\subseteq A, X) = \text{Some } (B, Y) \text{ and}$
 $D: (U, v) \models c_2 (\subseteq B, Y) = \text{Some } (C, Z) \text{ and}$
 $E: s \in A \text{ and}$
 $F: \text{cgood } c_1 \text{ and}$
 $G: \text{csimp } c_1 = c_1$

shows $\text{Max } (\text{levels } U) \vdash c_1;; c_2$

proof –

have $\text{Max } (\text{levels } U) \vdash c_1$

using A **and** E **by** *simp*

moreover from C and E and F and G have $B \neq \{\}$

by (*erule-tac csimp-ctyping2, blast*)

hence $\text{Max } (\text{levels } U) \vdash c_2$

using B **and** D **by** *blast*

ultimately show $?thesis ..$

qed

lemma *ctyping2-sec-type-if*:

assumes

$A: \bigwedge U' B C s. U' = \text{insert } (\text{Univ? } A X, \text{bvars } b) U \implies$
 $B = B_1 \implies C_1 = C \implies s \in B_1 \implies$
 $\text{finite } (\text{levels } (\text{insert } (\text{Univ? } A X, \text{bvars } b) U)) \implies$
 $\text{Max } (\text{levels } (\text{insert } (\text{Univ? } A X, \text{bvars } b) U)) \vdash c_1$
 $(\text{is } \bigwedge - - - -. - = ?U' \implies - \implies - \implies - \implies -)$
assumes
 $B: \bigwedge U' B C s. U' = ?U' \implies B = B_1 \implies C_2 = C \implies s \in B_2 \implies$
 $\text{finite } (\text{levels } ?U') \implies \text{Max } (\text{levels } ?U') \vdash c_2$ **and**
 $C: \models b (\subseteq A, X) = (B_1, B_2)$ **and**
 $D: s \in A$ **and**
 $E: \text{bsimp } b = b$ **and**
 $F: \forall v. b \neq Bc v$ **and**
 $G: \text{finite } (\text{levels } U)$
shows $\text{Max } (\text{levels } U) \vdash \text{IF } b \text{ THEN } c_1 \text{ ELSE } c_2$
proof –
from D **and** G **have** $H: \text{finite } (\text{levels } ?U') \wedge$
 $\text{Max } (\text{levels } ?U') = \text{max } (\text{sec } b) (\text{Max } (\text{levels } U))$
using levels-insert **by** $(\text{auto simp: univ-states-if-def})$
moreover have $I: \models b (\subseteq A, X) = (A, A)$
using E **and** F **by** $(\text{rule bsimp-btyping2})$
hence $\text{Max } (\text{levels } ?U') \vdash c_1$
using A **and** C **and** D **and** H **by** auto
moreover have $\text{Max } (\text{levels } ?U') \vdash c_2$
using B **and** C **and** D **and** H **and** I **by** auto
ultimately show $?thesis$
by (auto intro: If)
qed

lemma *ctyping2-sec-type-while*:

assumes
 $A: \bigwedge B C' B' D' s. B = B_1 \implies C' = C \implies B' = B_1' \implies$
 $(\exists s. s \in \text{Univ? } A X \vee s \in \text{Univ? } C Y) \longrightarrow$
 $(\forall x \in \text{bvars } b. \text{All } ((\leq) (\text{sec } x)))) \wedge$
 $(\forall p \in U. \text{case } p \text{ of } (B, W) \Rightarrow (\exists s. s \in B) \longrightarrow$
 $(\forall x \in W. \text{All } ((\leq) (\text{sec } x)))) \implies$
 $D = D' \implies s \in B_1 \implies \text{finite } (\text{levels } \{s\}) \implies \text{Max } (\text{levels } \{s\}) \vdash c$
 $(\text{is } \bigwedge - - - -. - \implies - \implies - \implies$
 $?P \wedge (\forall p \in -. \text{case } p \text{ of } (-, W) \Rightarrow - \longrightarrow ?Q W) \implies$
 $- \implies - \implies - \implies -)$
assumes
 $B: (\text{if } ?P \wedge (\forall p \in U. \forall B W. p = (B, W) \longrightarrow B = \{s\} \vee ?Q W)$
 $\text{then } \text{Some } (B_2 \cup B_2', \text{Univ? } B_2 X \cap Y) \text{ else None}) = \text{Some } (B, Z)$
 $(\text{is } (\text{if } ?R \text{ then } - \text{ else } -) = -)$ **and**
 $C: \models b (\subseteq A, X) = (B_1, B_2)$ **and**
 $D: s \in A$ **and**
 $E: \text{bsimp } b = b$ **and**
 $F: b \neq Bc \text{ False}$ **and**
 $G: b \neq Bc \text{ True}$ **and**
 $H: \text{finite } (\text{levels } U)$

shows $Max (levels U) \vdash WHILE\ b\ DO\ c$
proof –
 have $?R$
 using B by (*simp split: if-split-asm*)
 hence $sec\ b \leq 0$
 using D by (*subst bvars-ub, auto simp: univ-states-if-def, fastforce*)
 moreover have $\models b (\subseteq A, X) = (A, A)$
 using E and F and G by (*blast intro: bsimp-btyping2*)
 hence $0 \vdash c$
 using A and C and D and $\langle ?R \rangle$ by (*fastforce simp: levels-def*)
 moreover have $Max (levels U) = 0$
proof (*rule Max-eqI [OF H]*)
 fix l
 assume $l \in levels\ U$
 thus $l \leq 0$
 using $\langle ?R \rangle$ by (*fastforce simp: levels-def*)
next
 show $0 \in levels\ U$
 by (*simp add: levels-def*)
qed
 ultimately show $?thesis$
 by (*auto intro: While*)
qed

theorem *ctyping2-sec-type*:
 $\llbracket (U, v) \models c (\subseteq A, X) = Some\ (B, Y);$
 $s \in A; cgood\ c; csimp\ c = c; finite\ (levels\ U) \rrbracket \implies$
 $Max\ (levels\ U) \vdash c$
proof (*induction (U, v) c A X arbitrary: B Y U v s rule: ctyping2.induct*)
 fix U
 show $Max\ (levels\ U) \vdash SKIP$
 by (*rule Skip*)
next
 fix $A\ X\ C\ Z\ U\ v\ c_1\ c_2\ s$
 show
 $\llbracket \bigwedge B\ Y\ s. (U, v) \models c_1 (\subseteq A, X) = Some\ (B, Y) \implies$
 $s \in A \implies cgood\ c_1 \implies csimp\ c_1 = c_1 \implies finite\ (levels\ U) \implies$
 $Max\ (levels\ U) \vdash c_1;$
 $\bigwedge p\ B\ Y\ C\ Z\ s. (U, v) \models c_1 (\subseteq A, X) = Some\ p \implies$
 $(B, Y) = p \implies (U, v) \models c_2 (\subseteq B, Y) = Some\ (C, Z) \implies$
 $s \in B \implies cgood\ c_2 \implies csimp\ c_2 = c_2 \implies finite\ (levels\ U) \implies$
 $Max\ (levels\ U) \vdash c_2;$
 $(U, v) \models c_1;; c_2 (\subseteq A, X) = Some\ (C, Z);$
 $s \in A; cgood\ (c_1;; c_2);$
 $csimp\ (c_1;; c_2) = c_1;; c_2;$
 $finite\ (levels\ U) \rrbracket \implies$
 $Max\ (levels\ U) \vdash c_1;; c_2$
 by (*auto split: option.split-asm, rule ctyping2-sec-type-seq*)

```

next
  fix A X B Y U v b c1 c2 s
  show
     $\llbracket \bigwedge U' p B_1 B_2 C Y s.$ 
       $(U', p) = (\text{insert } (Univ? A X, \text{bvars } b) U, \models b (\subseteq A, X)) \implies$ 
       $(B_1, B_2) = p \implies (U', v) \models c_1 (\subseteq B_1, X) = \text{Some } (C, Y) \implies$ 
       $s \in B_1 \implies \text{cgood } c_1 \implies \text{csimp } c_1 = c_1 \implies \text{finite } (\text{levels } U') \implies$ 
       $\text{Max } (\text{levels } U') \vdash c_1;$ 
     $\bigwedge U' p B_1 B_2 C Y s.$ 
       $(U', p) = (\text{insert } (Univ? A X, \text{bvars } b) U, \models b (\subseteq A, X)) \implies$ 
       $(B_1, B_2) = p \implies (U', v) \models c_2 (\subseteq B_2, X) = \text{Some } (C, Y) \implies$ 
       $s \in B_2 \implies \text{cgood } c_2 \implies \text{csimp } c_2 = c_2 \implies \text{finite } (\text{levels } U') \implies$ 
       $\text{Max } (\text{levels } U') \vdash c_2;$ 
       $(U, v) \models \text{IF } b \text{ THEN } c_1 \text{ ELSE } c_2 (\subseteq A, X) = \text{Some } (B, Y);$ 
       $s \in A; \text{cgood } (\text{IF } b \text{ THEN } c_1 \text{ ELSE } c_2);$ 
       $\text{csimp } (\text{IF } b \text{ THEN } c_1 \text{ ELSE } c_2) = \text{IF } b \text{ THEN } c_1 \text{ ELSE } c_2;$ 
       $\text{finite } (\text{levels } U) \rrbracket \implies$ 
       $\text{Max } (\text{levels } U) \vdash \text{IF } b \text{ THEN } c_1 \text{ ELSE } c_2$ 
    by (auto split: option.split-asm prod.split-asm,
      rule ctyping2-sec-type-if)
next
  fix A X B Z U v b c s
  show
     $\llbracket \bigwedge B_1 B_2 C Y B_1' B_2' D Z s.$ 
       $(B_1, B_2) = \models b (\subseteq A, X) \implies$ 
       $(C, Y) = \vdash c (\subseteq B_1, X) \implies$ 
       $(B_1', B_2') = \models b (\subseteq C, Y) \implies$ 
       $\forall (B, W) \in \text{insert } (Univ? A X \cup Univ? C Y, \text{bvars } b) U.$ 
       $B: \text{sec } ' W \rightsquigarrow UNIV \implies$ 
       $(\{\}, \text{False}) \models c (\subseteq B_1, X) = \text{Some } (D, Z) \implies$ 
       $s \in B_1 \implies \text{cgood } c \implies \text{csimp } c = c \implies \text{finite } (\text{levels } \{\}) \implies$ 
       $\text{Max } (\text{levels } \{\}) \vdash c;$ 
     $\bigwedge B_1 B_2 C Y B_1' B_2' D' Z' s.$ 
       $(B_1, B_2) = \models b (\subseteq A, X) \implies$ 
       $(C, Y) = \vdash c (\subseteq B_1, X) \implies$ 
       $(B_1', B_2') = \models b (\subseteq C, Y) \implies$ 
       $\forall (B, W) \in \text{insert } (Univ? A X \cup Univ? C Y, \text{bvars } b) U.$ 
       $B: \text{sec } ' W \rightsquigarrow UNIV \implies$ 
       $(\{\}, \text{False}) \models c (\subseteq B_1', Y) = \text{Some } (D', Z') \implies$ 
       $s \in B_1' \implies \text{cgood } c \implies \text{csimp } c = c \implies \text{finite } (\text{levels } \{\}) \implies$ 
       $\text{Max } (\text{levels } \{\}) \vdash c;$ 
       $(U, v) \models \text{WHILE } b \text{ DO } c (\subseteq A, X) = \text{Some } (B, Z);$ 
       $s \in A; \text{cgood } (\text{WHILE } b \text{ DO } c);$ 
       $\text{csimp } (\text{WHILE } b \text{ DO } c) = \text{WHILE } b \text{ DO } c;$ 
       $\text{finite } (\text{levels } U) \rrbracket \implies$ 
       $\text{Max } (\text{levels } U) \vdash \text{WHILE } b \text{ DO } c$ 
    by (auto split: option.split-asm prod.split-asm,
      rule ctyping2-sec-type-while)
qed (auto split: prod.split-asm)

```

lemma *sec-type-ctyping2-if*:

assumes

$A: \bigwedge U' B_1 B_2. U' = \text{insert } (\text{Univ? } A \ X, \text{ bvars } b) \ U \implies$
 $(B_1, B_2) = \models b (\subseteq A, X) \implies$
 $\text{Max } (\text{levels } (\text{insert } (\text{Univ? } A \ X, \text{ bvars } b) \ U)) \vdash c_1 \implies$
 $\text{finite } (\text{levels } (\text{insert } (\text{Univ? } A \ X, \text{ bvars } b) \ U)) \implies$
 $\exists C \ Y. (\text{insert } (\text{Univ? } A \ X, \text{ bvars } b) \ U, v) \models c_1 (\subseteq B_1, X) =$
 $\text{Some } (C, Y)$
 $(\text{is } \bigwedge - \ -. \ - = ?U' \implies - \implies - \implies - \implies -)$

assumes

$B: \bigwedge U' B_1 B_2. U' = ?U' \implies (B_1, B_2) = \models b (\subseteq A, X) \implies$
 $\text{Max } (\text{levels } ?U') \vdash c_2 \implies \text{finite } (\text{levels } ?U') \implies$
 $\exists C \ Y. (?U', v) \models c_2 (\subseteq B_2, X) = \text{Some } (C, Y) \text{ and}$
 $C: \text{finite } (\text{levels } U) \text{ and}$
 $D: \text{max } (\text{sec } b) (\text{Max } (\text{levels } U)) \vdash c_1 \text{ and}$
 $E: \text{max } (\text{sec } b) (\text{Max } (\text{levels } U)) \vdash c_2$
shows $\exists C \ Y. (U, v) \models \text{IF } b \ \text{THEN } c_1 \ \text{ELSE } c_2 (\subseteq A, X) = \text{Some } (C, Y)$

proof –

obtain $B_1 B_2$ **where** $F: (B_1, B_2) = \models b (\subseteq A, X)$
by $(\text{cases } \models b (\subseteq A, X), \text{ simp})$
moreover have $\exists C_1 C_2 Y_1 Y_2. (?U', v) \models c_1 (\subseteq B_1, X) = \text{Some } (C_1, Y_1) \wedge$
 $(?U', v) \models c_2 (\subseteq B_2, X) = \text{Some } (C_2, Y_2)$
proof $(\text{cases } A = \{\})$
case *True*
hence $\text{levels } ?U' = \text{levels } U$
by $(\text{auto simp: levels-def univ-states-if-def})$
moreover have $\text{Max } (\text{levels } U) \vdash c_1$
using D **by** $(\text{auto intro: anti-mono})$
moreover have $\text{Max } (\text{levels } U) \vdash c_2$
using E **by** $(\text{auto intro: anti-mono})$
ultimately show $?thesis$
using A **and** B **and** C **and** F **by** simp
next
case *False*
with C **have** $\text{finite } (\text{levels } ?U') \wedge$
 $\text{Max } (\text{levels } ?U') = \text{max } (\text{sec } b) (\text{Max } (\text{levels } U))$
by $(\text{simp add: levels-insert univ-states-if-def})$
thus $?thesis$
using A **and** B **and** D **and** E **and** F **by** simp
qed
ultimately show $?thesis$
by $(\text{auto split: prod.split})$
qed

lemma *sec-type-ctyping2-while*:

assumes

$A: \bigwedge B_1 B_2 C \ Y \ B_1' B_2'. (B_1, B_2) = \models b (\subseteq A, X) \implies$

$(C, Y) = \vdash c (\subseteq B_1, X) \implies (B_1', B_2') = \models b (\subseteq C, Y) \implies$
 $((\exists s. s \in Univ? A X \vee s \in Univ? C Y) \longrightarrow$
 $(\forall x \in bvars b. All ((\leq) (sec x)))) \wedge$
 $(\forall p \in U. case p of (B, W) \Rightarrow (\exists s. s \in B) \longrightarrow$
 $(\forall x \in W. All ((\leq) (sec x)))) \implies$
 $Max (levels \{ \}) \vdash c \implies finite (levels \{ \}) \implies$
 $\exists D Z. (\{ \}, False) \models c (\subseteq B_1, X) = Some (D, Z)$
 $(is \bigwedge - - C Y - - . - \implies - \implies - \implies ?P C Y \implies - \implies - \implies -)$
assumes
 $B: \bigwedge B_1 B_2 C Y B_1' B_2'. (B_1, B_2) = \models b (\subseteq A, X) \implies$
 $(C, Y) = \vdash c (\subseteq B_1, X) \implies (B_1', B_2') = \models b (\subseteq C, Y) \implies$
 $?P C Y \implies Max (levels \{ \}) \vdash c \implies finite (levels \{ \}) \implies$
 $\exists D Z. (\{ \}, False) \models c (\subseteq B_1', Y) = Some (D, Z) \text{ and}$
 $C: finite (levels U) \text{ and}$
 $D: Max (levels U) = 0 \text{ and}$
 $E: sec b = 0 \text{ and}$
 $F: 0 \vdash c$
shows $\exists B Y. (U, v) \models WHILE b DO c (\subseteq A, X) = Some (B, Y)$
proof –
obtain $B_1 B_2$ **where** $G: (B_1, B_2) = \models b (\subseteq A, X)$
by $(cases \models b (\subseteq A, X), simp)$
moreover obtain $C Y$ **where** $H: (C, Y) = \vdash c (\subseteq B_1, X)$
by $(cases \vdash c (\subseteq B_1, X), simp)$
moreover obtain $B_1' B_2'$ **where** $I: (B_1', B_2') = \models b (\subseteq C, Y)$
by $(cases \models b (\subseteq C, Y), simp)$
moreover {
fix $l x s B W$
assume $J: (B, W) \in U$ **and** $K: x \in W$ **and** $L: s \in B$
have $sec x \leq l$
proof $(rule le-trans, rule Max-ge [OF C])$
show $sec x \in levels U$
using J **and** K **and** L **by** $(fastforce simp: levels-def)$
next
show $Max (levels U) \leq l$
using D **by** $simp$
qed
}
hence $J: ?P C Y$
using E **by** $(auto dest: bvars-sec)$
ultimately have $\exists D D' Z Z'. (\{ \}, False) \models c (\subseteq B_1, X) = Some (D, Z) \wedge$
 $(\{ \}, False) \models c (\subseteq B_1', Y) = Some (D', Z')$
using A **and** B **and** F **by** $(force simp: levels-def)$
thus $?thesis$
using G **and** H **and** I **and** J **by** $(auto split: prod.split)$
qed

theorem *sec-type-ctyping2*:
 $\llbracket Max (levels U) \vdash c; finite (levels U) \rrbracket \implies$

```

     $\exists B Y. (U, v) \models c (\subseteq A, X) = \text{Some } (B, Y)$ 
proof (induction  $(U, v) \vdash c \ A \ X$  arbitrary: U v rule: ctyping2.induct)
  fix  $A \ X \ U \ v \ x \ a$ 
  show  $\text{Max } (\text{levels } U) \vdash x ::= a \implies \text{finite } (\text{levels } U) \implies$ 
     $\exists B Y. (U, v) \models x ::= a (\subseteq A, X) = \text{Some } (B, Y)$ 
    by (fastforce dest: avars-sec simp: levels-def)
next
  fix  $A \ X \ U \ v \ b \ c_1 \ c_2$ 
  show
     $\llbracket \bigwedge U' p B_1 B_2. (U', p) = (\text{insert } (\text{Univ? } A \ X, \text{bvars } b) \ U, \models b (\subseteq A, X)) \implies$ 
       $(B_1, B_2) = p \implies \text{Max } (\text{levels } U') \vdash c_1 \implies \text{finite } (\text{levels } U') \implies$ 
       $\exists B Y. (U', v) \models c_1 (\subseteq B_1, X) = \text{Some } (B, Y);$ 
       $\bigwedge U' p B_1 B_2. (U', p) = (\text{insert } (\text{Univ? } A \ X, \text{bvars } b) \ U, \models b (\subseteq A, X)) \implies$ 
       $(B_1, B_2) = p \implies \text{Max } (\text{levels } U') \vdash c_2 \implies \text{finite } (\text{levels } U') \implies$ 
       $\exists B Y. (U', v) \models c_2 (\subseteq B_2, X) = \text{Some } (B, Y);$ 
       $\text{Max } (\text{levels } U) \vdash \text{IF } b \ \text{THEN } c_1 \ \text{ELSE } c_2; \text{finite } (\text{levels } U) \rrbracket \implies$ 
       $\exists B Y. (U, v) \models \text{IF } b \ \text{THEN } c_1 \ \text{ELSE } c_2 (\subseteq A, X) = \text{Some } (B, Y)$ 
    by (auto simp del: ctyping2.simps(4), rule sec-type-ctyping2-if)
next
  fix  $A \ X \ U \ v \ b \ c$ 
  show
     $\llbracket \bigwedge B_1 B_2 C Y B_1' B_2'. (B_1, B_2) = \models b (\subseteq A, X) \implies$ 
       $(C, Y) = \vdash c (\subseteq B_1, X) \implies$ 
       $(B_1', B_2') = \models b (\subseteq C, Y) \implies$ 
       $\forall (B, W) \in \text{insert } (\text{Univ? } A \ X \cup \text{Univ? } C \ Y, \text{bvars } b) \ U.$ 
       $B: \text{sec } 'W \rightsquigarrow \text{UNIV} \implies$ 
       $\text{Max } (\text{levels } \{\}) \vdash c \implies \text{finite } (\text{levels } \{\}) \implies$ 
       $\exists B Z. (\{\}, \text{False}) \models c (\subseteq B_1, X) = \text{Some } (B, Z);$ 
       $\bigwedge B_1 B_2 C Y B_1' B_2'. (B_1, B_2) = \models b (\subseteq A, X) \implies$ 
       $(C, Y) = \vdash c (\subseteq B_1, X) \implies$ 
       $(B_1', B_2') = \models b (\subseteq C, Y) \implies$ 
       $\forall (B, W) \in \text{insert } (\text{Univ? } A \ X \cup \text{Univ? } C \ Y, \text{bvars } b) \ U.$ 
       $B: \text{sec } 'W \rightsquigarrow \text{UNIV} \implies$ 
       $\text{Max } (\text{levels } \{\}) \vdash c \implies \text{finite } (\text{levels } \{\}) \implies$ 
       $\exists B Z. (\{\}, \text{False}) \models c (\subseteq B_1', Y) = \text{Some } (B, Z);$ 
       $\text{Max } (\text{levels } U) \vdash \text{WHILE } b \ \text{DO } c; \text{finite } (\text{levels } U) \rrbracket \implies$ 
       $\exists B Z. (U, v) \models \text{WHILE } b \ \text{DO } c (\subseteq A, X) = \text{Some } (B, Z)$ 
    by (auto simp del: ctyping2.simps(5), rule sec-type-ctyping2-while)
qed auto

end

end

```

References

- [1] C. Ballarin. *Tutorial to Locales and Locale Interpretation*. <https://isabelle.in.tum.de/website-Isabelle2023/dist/Isabelle2023/doc/locales.pdf>.
- [2] A. Krauss. *Defining Recursive Functions in Isabelle/HOL*. <https://isabelle.in.tum.de/website-Isabelle2023/dist/Isabelle2023/doc/functions.pdf>.
- [3] T. Nipkow. *A Tutorial Introduction to Structured Isar Proofs*. <https://isabelle.in.tum.de/website-Isabelle2011/dist/Isabelle2011/doc/isar-overview.pdf>.
- [4] T. Nipkow. *Programming and Proving in Isabelle/HOL*, Sept. 2023. <https://isabelle.in.tum.de/website-Isabelle2023/dist/Isabelle2023/doc/prog-prove.pdf>.
- [5] T. Nipkow and G. Klein. Theory HOL-IMP.Sec_Type_Expr (included in the Isabelle2023 distribution). https://isabelle.in.tum.de/website-Isabelle2023/dist/library/HOL/HOL-IMP/Sec_Type_Expr.html.
- [6] T. Nipkow and G. Klein. Theory HOL-IMP.Sec_TypingT (included in the Isabelle2023 distribution). https://isabelle.in.tum.de/website-Isabelle2023/dist/library/HOL/HOL-IMP/Sec_TypingT.html.
- [7] T. Nipkow and G. Klein. *Concrete Semantics with Isabelle/HOL*. Springer-Verlag, Feb. 2023. (Current version: <http://www.concrete-semantics.org/concrete-semantics.pdf>).
- [8] T. Nipkow, L. C. Paulson, and M. Wenzel. *Isabelle/HOL – A Proof Assistant for Higher-Order Logic*, Sept. 2023. <https://isabelle.in.tum.de/website-Isabelle2023/dist/Isabelle2023/doc/tutorial.pdf>.
- [9] J. Rushby. Noninterference, Transitivity, and Channel-Control Security Policies. Technical report, SRI International, Dec. 1992.
- [10] D. Volpano and G. Smith. Eliminating Covert Flows with Minimum Typings. In *Proc. 10th IEEE Computer Security Foundations Workshop*, June 1997.
- [11] D. Volpano, G. Smith, and C. Irvine. A Sound Type System for Secure Flow Analysis. *Journal of Computer Security*, Jan. 1996.