

# Information Flow Control via Dependency Tracking

Benedikt Nordhoff

November 24, 2021

## **Abstract**

We provide a characterisation of how information is propagated by program executions based on the tracking data and control dependencies within executions themselves. The characterisation might be used for deriving approximative safety properties to be targeted by static analyses or checked at runtime. We utilise a simple yet versatile control flow graph model as a program representation. As our model is not assumed to be finite it can be instantiated for a broad class of programs. The targeted security property is indistinguishable security where executions produce sequences of observations and only non-terminating executions are allowed to drop a tail of those.

A very crude approximation of our characterisation is slicing based on program dependence graphs, which we use as a minimal example and derive a corresponding soundness result.

For further details and applications refer to the authors upcoming dissertation.

# Contents

<b>1</b>	<b>Definitions</b>	<b>3</b>
1.1	Program Model . . . . .	3
1.1.1	Executions . . . . .	4
1.1.2	Well-formed Programs . . . . .	4
1.2	Security . . . . .	4
1.2.1	Observations . . . . .	4
1.2.2	Low equivalence of input states . . . . .	5
1.2.3	Termination . . . . .	5
1.2.4	Security Property . . . . .	5
1.3	Characterisation of Information Flows . . . . .	5
1.3.1	Post Dominance . . . . .	6
1.3.2	Control Dependence . . . . .	6
1.3.3	Control Slice . . . . .	6
1.3.4	Data Dependence . . . . .	7
1.3.5	Characterisation via Critical Paths . . . . .	7
1.3.6	Approximation via Single Critical Paths . . . . .	8
1.3.7	Further Definitions . . . . .	8
<b>2</b>	<b>Proofs</b>	<b>8</b>
2.1	Miscellaneous Facts . . . . .	8
2.2	Facts about Paths . . . . .	10
2.3	Facts about Post Dominators . . . . .	11
2.4	Facts about Control Dependencies . . . . .	12
2.5	Facts about Control Slices . . . . .	15
2.6	Facts about Observations . . . . .	19
2.7	Facts about Data . . . . .	19
2.8	Facts about Contradicting Paths . . . . .	20
2.9	Facts about Critical Observable Paths . . . . .	20
2.10	Correctness of the Characterisation . . . . .	21
2.11	Correctness of the Single Path Approximation . . . . .	21
<b>3</b>	<b>Example: Program Dependence Graphs</b>	<b>22</b>

# 1 Definitions

This section contains all necessary definitions of this development. Section 1.1 contains the structural definition of our program model which includes the security specification as well as abstractions of control flow and data. Executions of our program model are defined in section 1.1.1. Additional well-formedness properties are defined in section 1.1.2. Our security property is defined in section 1.2. Our characterisation of how information is propagated by executions of our program model is defined in section 1.3.5, for which the correctness result can be found in section 2.10. Section 1.3.6 contains an additional approximation of this characterisation whose correctness result can be found in section 2.11.

```
theory IFC
  imports Main
begin
```

## 1.1 Program Model

Our program model contains all necessary components for the remaining development and consists of:

```
record ⟨'n, 'var, 'val, 'obs⟩ ifc-problem =
— A set of nodes representing program locations:
  nodes :: ⟨'n set⟩
— An initial node where all executions start:
  entry :: ⟨'n⟩
— A final node where executions can terminate:
  return :: ⟨'n⟩
— An abstraction of control flow in the form of an edge relation:
  edges :: ⟨('n × 'n) set⟩
— An abstraction of variables written at program locations:
  writes :: ⟨'n ⇒ 'var set⟩
— An abstraction of variables read at program locations:
  reads :: ⟨'n ⇒ 'var set⟩
— A set of variables containing the confidential information in the initial state:
  hvars :: ⟨'var set⟩
— A step function on location state pairs:
  step :: ⟨('n × ('var ⇒ 'val)) ⇒ ('n × ('var ⇒ 'val))⟩
— An attacker model producing observations based on the reached state at certain locations:
  att :: ⟨'n → (('var ⇒ 'val) ⇒ 'obs)⟩
```

We fix a program in the following in order to define the central concepts. The necessary well-formedness assumptions will be made in section 1.1.2.

```
locale IFC-def =
fixes prob :: ⟨('n, 'var, 'val, 'obs) ifc-problem⟩
begin
```

Some short hands to the components of the program which we will utilise exclusively in the following.

```
definition nodes where ⟨nodes = ifc-problem.nodes prob⟩
definition entry where ⟨entry = ifc-problem.entry prob⟩
definition return where ⟨return = ifc-problem.return prob⟩
definition edges where ⟨edges = ifc-problem.edges prob⟩
definition writes where ⟨writes = ifc-problem.writes prob⟩
definition reads where ⟨reads = ifc-problem.reads prob⟩
definition hvars where ⟨hvars = ifc-problem.hvars prob⟩
definition step where ⟨step = ifc-problem.step prob⟩
definition att where ⟨att = ifc-problem.att prob⟩
```

The components of the step function for convenience.

**definition** *suc* **where**  $\langle \text{suc } n \ \sigma = \text{fst } (\text{step } (n, \sigma)) \rangle$

**definition** *sem* **where**  $\langle \text{sem } n \ \sigma = \text{snd } (\text{step } (n, \sigma)) \rangle$

**lemma** *step-suc-sem*:  $\langle \text{step } (n, \sigma) = (\text{suc } n \ \sigma, \text{sem } n \ \sigma) \rangle$  *<proof>*

### 1.1.1 Executions

In order to define what it means for a program to be well-formed, we first require concepts of executions and program paths.

The sequence of nodes visited by the execution corresponding to an input state.

**definition** *path* **where**

$\langle \text{path } \sigma \ k = \text{fst } ((\text{step} \sim^k) (\text{entry}, \sigma)) \rangle$

The sequence of states visited by the execution corresponding to an input state.

**definition** *kth-state* ( $\langle \cdot \rangle$  [111,111] 110) **where**

$\langle \sigma^k = \text{snd } ((\text{step} \sim^k) (\text{entry}, \sigma)) \rangle$

A predicate asserting that a sequence of nodes is a valid program path according to the control flow graph.

**definition** *is-path* **where**

$\langle \text{is-path } \pi = (\forall n. (\pi \ n, \pi \ (\text{Suc } n)) \in \text{edges}) \rangle$

**end**

### 1.1.2 Well-formed Programs

The following assumptions define our notion of valid programs.

**locale** *IFC* = *IFC-def*  $\langle \text{prob} \rangle$  **for** *prob*:  $\langle ('n, 'var, 'val, 'out) \text{ ifc-problem} \rangle +$

**assumes** *ret-is-node*[*simp, intro*]:  $\langle \text{return} \in \text{nodes} \rangle$

**and** *entry-is-node*[*simp, intro*]:  $\langle \text{entry} \in \text{nodes} \rangle$

**and** *writes*:  $\langle \bigwedge v \ n. (\exists \sigma. \sigma \ v \neq \text{sem } n \ \sigma \ v) \implies v \in \text{writes } n \rangle$

**and** *writes-return*:  $\langle \text{writes } \text{return} = \{\} \rangle$

**and** *uses-writes*:  $\langle \bigwedge n \ \sigma \ \sigma'. (\forall v \in \text{reads } n. \sigma \ v = \sigma' \ v) \implies \forall v \in \text{writes } n. \text{sem } n \ \sigma \ v = \text{sem } n \ \sigma' \ v \rangle$

**and** *uses-suc*:  $\langle \bigwedge n \ \sigma \ \sigma'. (\forall v \in \text{reads } n. \sigma \ v = \sigma' \ v) \implies \text{suc } n \ \sigma = \text{suc } n \ \sigma' \rangle$

**and** *uses-att*:  $\langle \bigwedge n \ f \ \sigma \ \sigma'. \text{att } n = \text{Some } f \implies (\forall v \in \text{reads } n. \sigma \ v = \sigma' \ v) \implies f \ \sigma = f \ \sigma' \rangle$

**and** *edges-complete*[*intro, simp*]:  $\langle \bigwedge m \ \sigma. m \in \text{nodes} \implies (m, \text{suc } m \ \sigma) \in \text{edges} \rangle$

**and** *edges-return*:  $\langle \bigwedge x. (\text{return}, x) \in \text{edges} \implies x = \text{return} \rangle$

**and** *edges-nodes*:  $\langle \text{edges} \subseteq \text{nodes} \times \text{nodes} \rangle$

**and** *reaching-ret*:  $\langle \bigwedge x. x \in \text{nodes} \implies \exists \pi \ n. \text{is-path } \pi \wedge \pi \ 0 = x \wedge \pi \ n = \text{return} \rangle$

## 1.2 Security

We define our notion of security, which corresponds to what Bohannon et al. [1] refer to as indistinguishable security. In order to do so we require notions of observations made by the attacker, termination and equivalence of input states.

**context** *IFC-def*

**begin**

### 1.2.1 Observations

The observation made at a given index within an execution.

**definition** *obsp* **where**

$\langle \text{obsp } \sigma \ k = (\text{case } \text{att}(\text{path } \sigma \ k) \text{ of } \text{Some } f \Rightarrow \text{Some } (f (\sigma^k)) \mid \text{None} \Rightarrow \text{None}) \rangle$

The indices within a path where an observation is made.

**definition** *obs-ids* ::  $\langle (\text{nat} \Rightarrow 'n) \Rightarrow \text{nat set} \rangle$  **where**  
 $\langle \text{obs-ids } \pi = \{k. \text{att } (\pi \ k) \neq \text{None}\} \rangle$

A predicate relating an observable index to the number of observations made before.

**definition** *is-kth-obs* ::  $\langle (\text{nat} \Rightarrow 'n) \Rightarrow \text{nat} \Rightarrow \text{nat} \Rightarrow \text{bool} \rangle$  **where**  
 $\langle \text{is-kth-obs } \pi \ k \ i = (\text{card } (\text{obs-ids } \pi \cap \{..<i\}) = k \wedge \text{att } (\pi \ i) \neq \text{None}) \rangle$

The final sequence of observations made for an execution.

**definition** *obs* **where**  
 $\langle \text{obs } \sigma \ k = (\text{if } (\exists i. \text{is-kth-obs } (\text{path } \sigma) \ k \ i) \text{ then } \text{obsp } \sigma \ (\text{THE } i. \text{is-kth-obs } (\text{path } \sigma) \ k \ i) \text{ else } \text{None}) \rangle$

Comparability of observations.

**definition** *obs-prefix* ::  $\langle (\text{nat} \Rightarrow 'obs \text{ option}) \Rightarrow (\text{nat} \Rightarrow 'obs \text{ option}) \Rightarrow \text{bool} \rangle$  (**infix**  $\langle \lesssim \rangle$  50) **where**  
 $\langle a \lesssim b \equiv \forall i. a \ i \neq \text{None} \longrightarrow a \ i = b \ i \rangle$

**definition** *obs-comp* (**infix**  $\langle \approx \rangle$  50) **where**  
 $\langle a \approx b \equiv a \lesssim b \vee b \lesssim a \rangle$

### 1.2.2 Low equivalence of input states

**definition** *restrict* (**infix**  $\langle | \rangle$  100) **where**  
 $\langle f|U = (\lambda n. \text{if } n \in U \text{ then } f \ n \text{ else } \text{undefined}) \rangle$

Two input states are low equivalent if they coincide on the non high variables.

**definition** *loweq* (**infix**  $\langle =_L \rangle$  50)  
**where**  $\langle \sigma =_L \sigma' = (\sigma|(-\text{hvars}) = \sigma'|(-\text{hvars})) \rangle$

### 1.2.3 Termination

An execution terminates iff it reaches the terminal node at any point.

**definition** *terminates* **where**  
 $\langle \text{terminates } \sigma \equiv \exists i. \text{path } \sigma \ i = \text{return} \rangle$

### 1.2.4 Security Property

The fixed program is secure if and only if for all pairs of low equivalent inputs the observation sequences are comparable and if the execution for an input state terminates then the observation sequence is not missing any observations.

**definition** *secure* **where**  
 $\langle \text{secure} \equiv \forall \sigma \ \sigma'. \sigma =_L \sigma' \longrightarrow (\text{obs } \sigma \approx \text{obs } \sigma' \wedge (\text{terminates } \sigma \longrightarrow \text{obs } \sigma' \lesssim \text{obs } \sigma)) \rangle$

## 1.3 Characterisation of Information Flows

We now define our characterisation of information flows which tracks data and control dependencies within executions. To do so we first require some additional concepts.

### 1.3.1 Post Dominance

We utilise the post dominance relation in order to define control dependence.

The basic post dominance relation.

**definition** *is-pd* (**infix**  $\langle pd \rightarrow \rangle$  50) **where**

$\langle y \text{ pd} \rightarrow x \iff x \in \text{nodes} \wedge (\forall \pi n. \text{is-path } \pi \wedge \pi (0::\text{nat}) = x \wedge \pi n = \text{return} \longrightarrow (\exists k \leq n. \pi k = y)) \rangle$

The immediate post dominance relation.

**definition** *is-ipd* (**infix**  $\langle ipd \rightarrow \rangle$  50) **where**

$\langle y \text{ ipd} \rightarrow x \iff x \neq y \wedge y \text{ pd} \rightarrow x \wedge (\forall z. z \neq x \wedge z \text{ pd} \rightarrow x \longrightarrow z \text{ pd} \rightarrow y) \rangle$

**definition** *ipd* **where**

$\langle \text{ipd } x = (\text{THE } y. y \text{ ipd} \rightarrow x) \rangle$

The post dominance tree.

**definition** *pdt* **where**

$\langle \text{pdt} = \{(x,y). x \neq y \wedge y \text{ pd} \rightarrow x\} \rangle$

### 1.3.2 Control Dependence

An index on an execution path is control dependent upon another if the path does not visit the immediate post domiator of the node reached by the smaller index.

**definition** *is-cdi* ( $\langle - \text{ cd} \rightarrow - \rangle$  [51,51,51]50) **where**

$\langle i \text{ cd} \rightarrow k \iff \text{is-path } \pi \wedge k < i \wedge \pi i \neq \text{return} \wedge (\forall j \in \{k..i\}. \pi j \neq \text{ipd } (\pi k)) \rangle$

The largest control dependency of an index is the immediate control dependency.

**definition** *is-icdi* ( $\langle - \text{ icd} \rightarrow - \rangle$  [51,51,51]50) **where**

$\langle n \text{ icd} \rightarrow n' \iff \text{is-path } \pi \wedge n \text{ cd} \rightarrow n' \wedge (\forall m \in \{n' < .. < n\}. \neg n \text{ cd} \rightarrow m) \rangle$

For the definition of the control slice, which we will define next, we require the uniqueness of the immediate control dependency.

**lemma** *icd-uniq*: **assumes**  $\langle m \text{ icd} \rightarrow n \rangle \langle m \text{ icd} \rightarrow n' \rangle$  **shows**  $\langle n = n' \rangle$

$\langle \text{proof} \rangle$

### 1.3.3 Control Slice

We utilise the control slice, that is the sequence of nodes visited by the control dependencies of an index, to match indices between executions.

**function** *cs*:  $\langle (\text{nat} \Rightarrow 'n) \Rightarrow \text{nat} \Rightarrow 'n \text{ list} \rangle$  ( $\langle \text{cs} \rightarrow \rangle$  [51,70] 71) **where**

$\langle \text{cs}^\pi n = (\text{if } (\exists m. n \text{ icd} \rightarrow m) \text{ then } (\text{cs } \pi (\text{THE } m. n \text{ icd} \rightarrow m)) @ [\pi n] \text{ else } [\pi n]) \rangle$

$\langle \text{proof} \rangle$

**termination**  $\langle \text{cs} \rangle \langle \text{proof} \rangle$

**inductive** *cs-less* (**infix**  $\langle < \rangle$  50) **where**

$\langle \text{length } xs < \text{length } ys \implies \text{take } (\text{length } xs) \text{ } ys = xs \implies xs < ys \rangle$

**definition** *cs-select* (**infix**  $\langle \downarrow \rangle$  50) **where**

$\langle \pi \downarrow xs = (\text{THE } k. \text{cs}^\pi k = xs) \rangle$

### 1.3.4 Data Dependence

Data dependence is defined straight forward. An index is data dependent upon another, if the index reads a variable written by the earlier index and the variable in question has not been written by any index in between.

**definition** *is-ddi* ( $\langle - \text{dd}^{\cdot, v} \rightarrow - \rangle [51, 51, 51, 51] 50$ ) **where**

$\langle n \text{dd}^{\pi, v} \rightarrow m \iff \text{is-path } \pi \wedge m < n \wedge v \in \text{reads}(\pi \ n) \cap (\text{writes}(\pi \ m)) \wedge (\forall l \in \{m < .. < n\}. v \notin \text{writes}(\pi \ l)) \rangle$

### 1.3.5 Characterisation via Critical Paths

With the above we define the set of critical paths which as we will prove characterise the matching points in executions where diverging data is read.

**inductive-set** *cp* **where**

— Any pair of low equivalent input states and indices where a diverging high variable is first read is critical.

$\langle \llbracket \sigma =_L \sigma';$   
 $\text{cs}^{\text{path}} \sigma \ n = \text{cs}^{\text{path}} \sigma' \ n';$   
 $h \in \text{reads}(\text{path } \sigma \ n);$   
 $(\sigma^n) \ h \neq (\sigma'^n) \ h;$   
 $\forall k < n. h \notin \text{writes}(\text{path } \sigma \ k);$   
 $\forall k' < n'. h \notin \text{writes}(\text{path } \sigma' \ k')$   
 $\rrbracket \implies ((\sigma, n), (\sigma', n')) \in \text{cp} \rangle \mid$

— If from a pair of critical indices in two executions there exist data dependencies from both indices to a pair of matching indices where the variable diverges, the later pair of indices is critical.

$\langle \llbracket ((\sigma, k), (\sigma', k')) \in \text{cp};$   
 $n \text{dd}^{\text{path}} \sigma, v \rightarrow k;$   
 $n' \text{dd}^{\text{path}} \sigma', v \rightarrow k';$   
 $\text{cs}^{\text{path}} \sigma \ n = \text{cs}^{\text{path}} \sigma' \ n';$   
 $(\sigma^n) \ v \neq (\sigma'^n) \ v$   
 $\rrbracket \implies ((\sigma, n), (\sigma', n')) \in \text{cp} \rangle \mid$

— If from a pair of critical indices the executions take different branches and one of the critical indices is a control dependency of an index that is data dependency of a matched index where diverging data is read and the variable in question is not written by the other execution after the executions first reached matching indices again, then the later matching pair of indices is critical.

$\langle \llbracket ((\sigma, k), (\sigma', k')) \in \text{cp};$   
 $n \text{dd}^{\text{path}} \sigma, v \rightarrow l;$   
 $l \text{cd}^{\text{path}} \sigma \rightarrow k;$   
 $\text{cs}^{\text{path}} \sigma \ n = \text{cs}^{\text{path}} \sigma' \ n';$   
 $\text{path } \sigma \ (\text{Suc } k) \neq \text{path } \sigma' \ (\text{Suc } k');$   
 $(\sigma^n) \ v \neq (\sigma'^n) \ v;$   
 $\forall j' \in \{(\text{LEAST } i'. k' < i' \wedge (\exists i. \text{cs}^{\text{path}} \sigma \ i = \text{cs}^{\text{path}} \sigma' \ i')) .. < n'\}. v \notin \text{writes}(\text{path } \sigma' \ j')$   
 $\rrbracket \implies ((\sigma, n), (\sigma', n')) \in \text{cp} \rangle \mid$

— The relation is symmetric.

$\langle \llbracket ((\sigma, k), (\sigma', k')) \in \text{cp} \rrbracket \implies ((\sigma', k'), (\sigma, k)) \in \text{cp} \rangle$

Based on the set of critical paths, the critical observable paths are those that either directly reach observable nodes or are diverging control dependencies of an observable index.

**inductive-set** *cop* **where**

$\langle \llbracket ((\sigma, n), (\sigma', n')) \in cp; \text{path } \sigma \ n \in \text{dom att} \rrbracket \implies ((\sigma, n), (\sigma', n')) \in cop \rangle \mid$

$\langle \llbracket ((\sigma, k), (\sigma', k')) \in cp; n \text{ cd}^{\text{path } \sigma} \rightarrow k; \text{path } \sigma \ (\text{Suc } k) \neq \text{path } \sigma' \ (\text{Suc } k'); \text{path } \sigma \ n \in \text{dom att} \rrbracket \implies ((\sigma, n), (\sigma', k')) \in cop \rangle$

### 1.3.6 Approximation via Single Critical Paths

For applications we also define a single execution approximation.

**definition** *is-dcdi-via* ( $\langle \text{- dcd}^{\cdot, \cdot} \rightarrow \cdot \text{ via } \cdot \rightarrow [51, 51, 51, 51, 51, 51] \ 50 \rangle$ ) **where**

$\langle n \text{ dcd}^{\pi, v} \rightarrow m \text{ via } \pi' \ m' = (\text{is-path } \pi \wedge m < n \wedge (\exists l' \ n'. \text{cs}^{\pi} \ m = \text{cs}^{\pi'} \ m' \wedge \text{cs}^{\pi} \ n = \text{cs}^{\pi'} \ n' \wedge n' \text{ dd}^{\pi', v} \rightarrow l' \wedge l' \text{ cd}^{\pi'} \rightarrow m')) \wedge (\forall l \in \{m..<n\}. v \notin \text{writes}(\pi \ l)) \rangle$

**inductive-set** *scp* **where**

$\langle \llbracket h \in \text{hvars}; h \in \text{reads}(\text{path } \sigma \ n); (\forall k < n. h \notin \text{writes}(\text{path } \sigma \ k)) \rrbracket \implies (\text{path } \sigma, n) \in scp \rangle \mid$   
 $\langle \llbracket (\pi, m) \in scp; n \text{ cd}^{\pi} \rightarrow m \rrbracket \implies (\pi, n) \in scp \rangle \mid$   
 $\langle \llbracket (\pi, m) \in scp; n \text{ dd}^{\pi, v} \rightarrow m \rrbracket \implies (\pi, n) \in scp \rangle \mid$   
 $\langle \llbracket (\pi, m) \in scp; (\pi', m') \in scp; n \text{ dcd}^{\pi, v} \rightarrow m \text{ via } \pi' \ m' \rrbracket \implies (\pi, n) \in scp \rangle$

**inductive-set** *scop* **where**

$\langle \llbracket (\pi, n) \in scp; \pi \ n \in \text{dom att} \rrbracket \implies (\pi, n) \in scop \rangle$

### 1.3.7 Further Definitions

The following concepts are utilised by the proofs.

**inductive** *contradicts* (**infix**  $\langle \mathbf{c} \rangle \ 50$ ) **where**

$\langle \llbracket \text{cs}^{\pi'} \ k' \prec \text{cs}^{\pi} \ k; \pi = \text{path } \sigma; \pi' = \text{path } \sigma'; \pi \ (\text{Suc} \ (\pi \ \text{cs}^{\pi'} \ k')) \neq \pi' \ (\text{Suc} \ k') \rrbracket \implies (\sigma', k') \ \mathbf{c} \ (\sigma, k) \rangle \mid$   
 $\langle \llbracket \text{cs}^{\pi'} \ k' = \text{cs}^{\pi} \ k; \pi = \text{path } \sigma; \pi' = \text{path } \sigma'; \sigma^k \ \uparrow \ (\text{reads} \ (\pi \ k)) \neq \sigma'^{k'} \ \uparrow \ (\text{reads} \ (\pi \ k)) \rrbracket \implies (\sigma', k') \ \mathbf{c} \ (\sigma, k) \rangle$

**definition** *path-shift* (**infixl**  $\langle \ll \rangle \ 51$ ) **where**

$\llbracket \text{simp} \rrbracket: \langle \pi \ll m = (\lambda \ n. \ \pi \ (m+n)) \rangle$

**definition** *path-append*  $:: \langle (\text{nat} \Rightarrow 'n) \Rightarrow \text{nat} \Rightarrow (\text{nat} \Rightarrow 'n) \Rightarrow (\text{nat} \Rightarrow 'n) \rangle$  ( $\langle \text{- } @^{\cdot} \rightarrow [0, 0, 999] \ 51 \rangle$ ) **where**

$\llbracket \text{simp} \rrbracket: \langle \pi \ @^m \ \pi' = (\lambda \ n. (\text{if } n \leq m \text{ then } \pi \ n \text{ else } \pi' \ (n-m))) \rangle$

**definition** *eq-up-to*  $:: \langle (\text{nat} \Rightarrow 'n) \Rightarrow \text{nat} \Rightarrow (\text{nat} \Rightarrow 'n) \Rightarrow \text{bool} \rangle$  ( $\langle \text{- } =_{\cdot} \rightarrow [55, 55, 55] \ 50 \rangle$ ) **where**

$\langle \pi =_k \ \pi' = (\forall \ i \leq k. \ \pi \ i = \pi' \ i) \rangle$

**end**

## 2 Proofs

### 2.1 Miscellaneous Facts

**lemma** *option-neq-cases*: **assumes**  $\langle x \neq y \rangle$  **obtains** (*none1*)  $a$  **where**  $\langle x = \text{None} \rangle \langle y = \text{Some } a \rangle \mid$  (*none2*)  $a$  **where**  $\langle x = \text{Some } a \rangle \langle y = \text{None} \rangle \mid$  (*some*)  $a \ b$  **where**  $\langle x = \text{Some } a \rangle \langle y = \text{Some } b \rangle \langle a \neq b \rangle$  *\langle proof \rangle*



**lemmas** *nat-sym-cases*[*case-names less sym eq*] = *linorder-less-wlog*

**lemma** *mod-bound-instance*: **assumes**  $\langle j < (i::nat) \rangle$  **obtains**  $j'$  **where**  $\langle k < j' \rangle$  **and**  $\langle j' \bmod i = j \rangle$  *<proof>*

**lemma** *list-neq-prefix-cases*: **assumes**  $\langle ls \neq ls' \rangle$  **and**  $\langle ls \neq Nil \rangle$  **and**  $\langle ls' \neq Nil \rangle$   
**obtains** (*diverge*)  $xs\ x\ x'\ ys\ ys'$  **where**  $\langle ls = xs@[x]@ys \rangle$   $\langle ls' = xs@[x']@ys' \rangle$   $\langle x \neq x' \rangle$  |  
(*prefix1*)  $xs$  **where**  $\langle ls = ls'@xs \rangle$  **and**  $\langle xs \neq Nil \rangle$  |  
(*prefix2*)  $xs$  **where**  $\langle ls@xs = ls' \rangle$  **and**  $\langle xs \neq Nil \rangle$   
*<proof>*

**lemma** *three-cases*: **assumes**  $\langle A \vee B \vee C \rangle$  **obtains**  $\langle A \rangle$  |  $\langle B \rangle$  |  $\langle C \rangle$  *<proof>*

**lemma** *insort-greater*:  $\langle \forall x \in set\ ls.\ x < y \implies insort\ y\ ls = ls@[y] \rangle$  *<proof>*

**lemma** *insort-append-first*: **assumes**  $\langle \forall y \in set\ ys.\ x \leq y \rangle$  **shows**  $\langle insort\ x\ (xs@ys) = insort\ x\ xs\ @\ ys \rangle$   
*<proof>*

**lemma** *sorted-list-of-set-append*: **assumes**  $\langle finite\ xs \rangle$   $\langle finite\ ys \rangle$   $\langle \forall x \in xs.\ \forall y \in ys.\ x < y \rangle$  **shows**  $\langle sorted-list-of-set\ (xs \cup ys) = sorted-list-of-set\ xs\ @\ (sorted-list-of-set\ ys) \rangle$   
*<proof>*

**lemma** *filter-insort*:  $\langle sorted\ xs \implies filter\ P\ (insort\ x\ xs) = (if\ P\ x\ then\ insort\ x\ (filter\ P\ xs)\ else\ filter\ P\ xs) \rangle$   
*<proof>*

**lemma** *filter-sorted-list-of-set*: **assumes**  $\langle finite\ xs \rangle$  **shows**  $\langle filter\ P\ (sorted-list-of-set\ xs) = sorted-list-of-set\ \{x \in xs.\ P\ x\} \rangle$  *<proof>*

**lemma** *unbounded-nat-set-infinite*: **assumes**  $\langle \forall (i::nat).\ \exists j \geq i.\ j \in A \rangle$  **shows**  $\langle \neg finite\ A \rangle$  *<proof>*

**lemma** *infinite-ascending*: **assumes**  $nf: \langle \neg finite\ (A::nat\ set) \rangle$  **obtains**  $f$  **where**  $\langle range\ f = A \rangle$   $\langle \forall i.\ f\ i < f\ (Suc\ i) \rangle$  *<proof>*

**lemma** *mono-ge-id*:  $\langle \forall i.\ f\ i < f\ (Suc\ i) \implies i \leq f\ i \rangle$   
*<proof>*

**lemma** *insort-map-mono*: **assumes** *mono*:  $\langle \forall n\ m.\ n < m \implies f\ n < f\ m \rangle$  **shows**  $\langle map\ f\ (insort\ n\ ns) = insort\ (f\ n)\ (map\ f\ ns) \rangle$   
*<proof>*

**lemma** *sorted-list-of-set-map-mono*: **assumes** *mono*:  $\langle \forall n\ m.\ n < m \implies f\ n < f\ m \rangle$  **and** *fin*:  $\langle finite\ A \rangle$   
**shows**  $\langle map\ f\ (sorted-list-of-set\ A) = sorted-list-of-set\ (f\ A) \rangle$   
*<proof>*

**lemma** *GreatestIB*:

**fixes**  $n :: \langle nat \rangle$  **and**  $P$

**assumes**  $a: \langle \exists k \leq n.\ P\ k \rangle$

**shows** *GreatestBI*:  $\langle P\ (GREATEST\ k.\ k \leq n \wedge P\ k) \rangle$  **and** *GreatestB*:  $\langle (GREATEST\ k.\ k \leq n \wedge P\ k) \leq n \rangle$   
*<proof>*

**lemma** *GreatestB-le*:

**fixes**  $n :: \langle nat \rangle$

**assumes**  $\langle x \leq n \rangle$  **and**  $\langle P\ x \rangle$

**shows**  $\langle x \leq (GREATEST\ k.\ k \leq n \wedge P\ k) \rangle$   
*<proof>*

**lemma** *LeastBI-ex*: **assumes**  $\langle \exists k \leq n. P k \rangle$  **shows**  $\langle P (LEAST k::'c::wellorder. P k) \rangle$  **and**  $\langle (LEAST k. P k) \leq n \rangle$   
 $\langle proof \rangle$

**lemma** *allB-atLeastLessThan-lower*: **assumes**  $\langle (i::nat) \leq j \rangle \langle \forall x \in \{i..<n\}. P x \rangle$  **shows**  $\langle \forall x \in \{j..<n\}. P x \rangle$   
 $\langle proof \rangle$

## 2.2 Facts about Paths

**context** *IFC*  
**begin**

**lemma** *path0*:  $\langle path \ \sigma \ 0 = entry \rangle$   $\langle proof \rangle$

**lemma** *path-in-nodes*[*intro*]:  $\langle path \ \sigma \ k \in nodes \rangle$   $\langle proof \rangle$

**lemma** *path-is-path*[*simp*]:  $\langle is-path \ (path \ \sigma) \rangle$   $\langle proof \rangle$

**lemma** *term-path-stable*: **assumes**  $\langle is-path \ \pi \rangle \langle \pi \ i = return \rangle$  **and** *le*:  $\langle i \leq j \rangle$  **shows**  $\langle \pi \ j = return \rangle$   
 $\langle proof \rangle$

**lemma** *path-path-shift*: **assumes**  $\langle is-path \ \pi \rangle$  **shows**  $\langle is-path \ (\pi \ll m) \rangle$   
 $\langle proof \rangle$

**lemma** *path-cons*: **assumes**  $\langle is-path \ \pi \rangle \langle is-path \ \pi' \rangle \langle \pi \ m = \pi' \ 0 \rangle$  **shows**  $\langle is-path \ (\pi \ @^m \ \pi') \rangle$   
 $\langle proof \rangle$

**lemma** *is-path-loop*: **assumes**  $\langle is-path \ \pi \rangle \langle 0 < i \rangle \langle \pi \ i = \pi \ 0 \rangle$  **shows**  $\langle is-path \ (\lambda n. \pi \ (n \bmod i)) \rangle$   $\langle proof \rangle$

**lemma** *path-nodes*:  $\langle is-path \ \pi \implies \pi \ k \in nodes \rangle$   $\langle proof \rangle$

**lemma** *direct-path-return'*: **assumes**  $\langle is-path \ \pi \rangle \langle \pi \ 0 = x \rangle \langle x \neq return \rangle \langle \pi \ n = return \rangle$   
**obtains**  $\pi' \ n'$  **where**  $\langle is-path \ \pi' \rangle \langle \pi' \ 0 = x \rangle \langle \pi' \ n' = return \rangle \langle \forall i > 0. \pi' \ i \neq x \rangle$   
 $\langle proof \rangle$

**lemma** *direct-path-return*: **assumes**  $\langle x \in nodes \rangle \langle x \neq return \rangle$   
**obtains**  $\pi \ n$  **where**  $\langle is-path \ \pi \rangle \langle \pi \ 0 = x \rangle \langle \pi \ n = return \rangle \langle \forall i > 0. \pi \ i \neq x \rangle$   
 $\langle proof \rangle$

**lemma** *path-append-eq-up-to*:  $\langle (\pi \ @^k \ \pi') =_k \ \pi \rangle$   $\langle proof \rangle$

**lemma** *eq-up-to-le*: **assumes**  $\langle k \leq n \rangle \langle \pi =_n \ \pi' \rangle$  **shows**  $\langle \pi =_k \ \pi' \rangle$   $\langle proof \rangle$

**lemma** *eq-up-to-refl*: **shows**  $\langle \pi =_k \ \pi \rangle$   $\langle proof \rangle$

**lemma** *eq-up-to-sym*: **assumes**  $\langle \pi =_k \ \pi' \rangle$  **shows**  $\langle \pi' =_k \ \pi \rangle$   $\langle proof \rangle$

**lemma** *eq-up-to-apply*: **assumes**  $\langle \pi =_k \ \pi' \rangle \langle j \leq k \rangle$  **shows**  $\langle \pi \ j = \pi' \ j \rangle$   $\langle proof \rangle$

**lemma** *path-swap-ret*: **assumes**  $\langle is-path \ \pi \rangle$  **obtains**  $\pi' \ n$  **where**  $\langle is-path \ \pi' \rangle \langle \pi =_k \ \pi' \rangle \langle \pi' \ n = return \rangle$   
 $\langle proof \rangle$

**lemma** *path-suc*:  $\langle path \ \sigma \ (Suc \ k) = fst \ (step \ (path \ \sigma \ k, \ \sigma^k)) \rangle$   $\langle proof \rangle$

**lemma** *kth-state-suc*:  $\langle \sigma^{Suc \ k} = snd \ (step \ (path \ \sigma \ k, \ \sigma^k)) \rangle$   $\langle proof \rangle$

## 2.3 Facts about Post Dominators

**lemma** *pd-trans*: **assumes**  $1: \langle y \text{ pd} \rightarrow x \rangle$  **and**  $2: \langle z \text{ pd} \rightarrow y \rangle$  **shows**  $\langle z \text{ pd} \rightarrow x \rangle$   
 $\langle \text{proof} \rangle$

**lemma** *pd-path*: **assumes**  $\langle y \text{ pd} \rightarrow x \rangle$   
**obtains**  $\pi \ n \ k$  **where**  $\langle \text{is-path } \pi \rangle$  **and**  $\langle \pi \ 0 = x \rangle$  **and**  $\langle \pi \ n = \text{return} \rangle$  **and**  $\langle \pi \ k = y \rangle$  **and**  $\langle k \leq n \rangle$   
 $\langle \text{proof} \rangle$

**lemma** *pd-antisym*: **assumes**  $x\text{pdy}: \langle x \text{ pd} \rightarrow y \rangle$  **and**  $y\text{pdx}: \langle y \text{ pd} \rightarrow x \rangle$  **shows**  $\langle x = y \rangle$   
 $\langle \text{proof} \rangle$

**lemma** *pd-refl[simp]*:  $\langle x \in \text{nodes} \implies x \text{ pd} \rightarrow x \rangle$   $\langle \text{proof} \rangle$

**lemma** *pdt-trans-in-pdt*:  $\langle (x,y) \in \text{pdt}^+ \implies (x,y) \in \text{pdt} \rangle$   
 $\langle \text{proof} \rangle$

**lemma** *pdt-trancl-pdt*:  $\langle \text{pdt}^+ = \text{pdt} \rangle$   $\langle \text{proof} \rangle$

**lemma** *trans-pdt*:  $\langle \text{trans } \text{pdt} \rangle$   $\langle \text{proof} \rangle$

**definition** *[simp]*:  $\langle \text{pdt-inv} = \text{pdt}^{-1} \rangle$

**lemma** *wf-pdt-inv*:  $\langle \text{wf } (\text{pdt-inv}) \rangle$   $\langle \text{proof} \rangle$

**lemma** *return-pd*: **assumes**  $\langle x \in \text{nodes} \rangle$  **shows**  $\langle \text{return } \text{pd} \rightarrow x \rangle$   $\langle \text{proof} \rangle$

**lemma** *pd-total*: **assumes**  $xz: \langle x \text{ pd} \rightarrow z \rangle$  **and**  $yz: \langle y \text{ pd} \rightarrow z \rangle$  **shows**  $\langle x \text{ pd} \rightarrow y \vee y \text{ pd} \rightarrow x \rangle$   
 $\langle \text{proof} \rangle$

**lemma** *pds-finite*:  $\langle \text{finite } \{y . (x,y) \in \text{pdt}\} \rangle$   $\langle \text{proof} \rangle$

**lemma** *ipd-exists*: **assumes**  $\text{node}: \langle x \in \text{nodes} \rangle$  **and**  $\text{not-ret}: \langle x \neq \text{return} \rangle$  **shows**  $\langle \exists y. y \text{ ipd} \rightarrow x \rangle$   
 $\langle \text{proof} \rangle$

**lemma** *ipd-unique*: **assumes**  $y\text{ipd}: \langle y \text{ ipd} \rightarrow x \rangle$  **and**  $y'\text{ipd}: \langle y' \text{ ipd} \rightarrow x \rangle$  **shows**  $\langle y = y' \rangle$   
 $\langle \text{proof} \rangle$

**lemma** *ipd-is-ipd*: **assumes**  $\langle x \in \text{nodes} \rangle$  **and**  $\langle x \neq \text{return} \rangle$  **shows**  $\langle \text{ipd } x \text{ ipd} \rightarrow x \rangle$   $\langle \text{proof} \rangle$

**lemma** *is-ipd-in-pdt*:  $\langle y \text{ ipd} \rightarrow x \implies (x,y) \in \text{pdt} \rangle$   $\langle \text{proof} \rangle$

**lemma** *ipd-in-pdt*:  $\langle x \in \text{nodes} \implies x \neq \text{return} \implies (x, \text{ipd } x) \in \text{pdt} \rangle$   $\langle \text{proof} \rangle$

**lemma** *no-pd-path*: **assumes**  $\langle x \in \text{nodes} \rangle$  **and**  $\langle \neg y \text{ pd} \rightarrow x \rangle$   
**obtains**  $\pi \ n$  **where**  $\langle \text{is-path } \pi \rangle$  **and**  $\langle \pi \ 0 = x \rangle$  **and**  $\langle \pi \ n = \text{return} \rangle$  **and**  $\langle \forall k \leq n. \pi \ k \neq y \rangle$   
 $\langle \text{proof} \rangle$

**lemma** *pd-pd-ipd*: **assumes**  $\langle x \in \text{nodes} \rangle$   $\langle x \neq \text{return} \rangle$   $\langle y \neq x \rangle$   $\langle y \text{ pd} \rightarrow x \rangle$  **shows**  $\langle y \text{ pd} \rightarrow \text{ipd } x \rangle$   
 $\langle \text{proof} \rangle$

**lemma** *pd-nodes*: **assumes**  $\langle y \text{ pd} \rightarrow x \rangle$  **shows**  $\text{pd-node1}: \langle y \in \text{nodes} \rangle$  **and**  $\text{pd-node2}: \langle x \in \text{nodes} \rangle$   
 $\langle \text{proof} \rangle$

**lemma** *pd-ret-is-ret*:  $\langle x \text{ pd} \rightarrow \text{return} \implies x = \text{return} \rangle$   $\langle \text{proof} \rangle$

**lemma** *ret-path-none-pd*: **assumes**  $\langle x \in \text{nodes} \rangle \langle x \neq \text{return} \rangle$   
**obtains**  $\pi \ n$  **where**  $\langle \text{is-path } \pi \rangle \langle \pi \ 0 = x \rangle \langle \pi \ n = \text{return} \rangle \langle \forall i > 0. \neg x \text{ pd} \rightarrow \pi \ i \rangle$   
 $\langle \text{proof} \rangle$

**lemma** *path-pd-ipd0'*: **assumes**  $\langle \text{is-path } \pi \rangle$  **and**  $\langle \pi \ n \neq \text{return} \rangle \langle \pi \ n \neq \pi \ 0 \rangle$  **and**  $\langle \pi \ n \text{ pd} \rightarrow \pi \ 0 \rangle$   
**obtains**  $k$  **where**  $\langle k \leq n \rangle$  **and**  $\langle \pi \ k = \text{ipd}(\pi \ 0) \rangle$   
 $\langle \text{proof} \rangle$

**lemma** *path-pd-ipd0*: **assumes**  $\langle \text{is-path } \pi \rangle$  **and**  $\langle \pi \ 0 \neq \text{return} \rangle \langle \pi \ n \neq \pi \ 0 \rangle$  **and**  $\langle \pi \ n \text{ pd} \rightarrow \pi \ 0 \rangle$   
**obtains**  $k$  **where**  $\langle k \leq n \rangle$  **and**  $\langle \pi \ k = \text{ipd}(\pi \ 0) \rangle$   
 $\langle \text{proof} \rangle$

**lemma** *path-pd-ipd*: **assumes**  $\langle \text{is-path } \pi \rangle$  **and**  $\langle \pi \ k \neq \text{return} \rangle \langle \pi \ n \neq \pi \ k \rangle$  **and**  $\langle \pi \ n \text{ pd} \rightarrow \pi \ k \rangle$  **and**  $kn$ :  $\langle k < n \rangle$   
**obtains**  $l$  **where**  $\langle k < l \rangle$  **and**  $\langle l \leq n \rangle$  **and**  $\langle \pi \ l = \text{ipd}(\pi \ k) \rangle$   
 $\langle \text{proof} \rangle$

**lemma** *path-ret-ipd*: **assumes**  $\langle \text{is-path } \pi \rangle$  **and**  $\langle \pi \ k \neq \text{return} \rangle \langle \pi \ n = \text{return} \rangle$   
**obtains**  $l$  **where**  $\langle k < l \rangle$  **and**  $\langle l \leq n \rangle$  **and**  $\langle \pi \ l = \text{ipd}(\pi \ k) \rangle$   
 $\langle \text{proof} \rangle$

**lemma** *pd-intro*: **assumes**  $\langle l \text{ pd} \rightarrow k \rangle \langle \text{is-path } \pi \rangle \langle \pi \ 0 = k \rangle \langle \pi \ n = \text{return} \rangle$   
**obtains**  $i$  **where**  $\langle i \leq n \rangle \langle \pi \ i = l \rangle$   $\langle \text{proof} \rangle$

**lemma** *path-pd-pd0*: **assumes** *path*:  $\langle \text{is-path } \pi \rangle$  **and** *lpdn*:  $\langle \pi \ l \text{ pd} \rightarrow n \rangle$  **and** *npd0*:  $\langle n \text{ pd} \rightarrow \pi \ 0 \rangle$   
**obtains**  $k$  **where**  $\langle k \leq l \rangle \langle \pi \ k = n \rangle$   
 $\langle \text{proof} \rangle$

## 2.4 Facts about Control Dependencies

**lemma** *icd-imp-cd*:  $\langle n \text{ icd}^\pi \rightarrow k \implies n \text{ cd}^\pi \rightarrow k \rangle$   $\langle \text{proof} \rangle$

**lemma** *ipd-impl-not-cd*: **assumes**  $\langle j \in \{k..i\} \rangle$  **and**  $\langle \pi \ j = \text{ipd}(\pi \ k) \rangle$  **shows**  $\langle \neg i \text{ cd}^\pi \rightarrow k \rangle$   
 $\langle \text{proof} \rangle$

**lemma** *cd-not-ret*: **assumes**  $\langle i \text{ cd}^\pi \rightarrow k \rangle$  **shows**  $\langle \pi \ k \neq \text{return} \rangle$   $\langle \text{proof} \rangle$

**lemma** *cd-path-shift*: **assumes**  $\langle j \leq k \rangle \langle \text{is-path } \pi \rangle$  **shows**  $\langle (i \text{ cd}^\pi \rightarrow k) = (i - j \text{ cd}^{\pi \ll j} \rightarrow k - j) \rangle$   $\langle \text{proof} \rangle$

**lemma** *cd-path-shift0*: **assumes**  $\langle \text{is-path } \pi \rangle$  **shows**  $\langle (i \text{ cd}^\pi \rightarrow k) = (i - k \text{ cd}^{\pi \ll k} \rightarrow 0) \rangle$   
 $\langle \text{proof} \rangle$

**lemma** *icd-path-shift*: **assumes**  $\langle l \leq k \rangle \langle \text{is-path } \pi \rangle$  **shows**  $\langle (i \text{ icd}^\pi \rightarrow k) = (i - l \text{ icd}^{\pi \ll l} \rightarrow k - l) \rangle$   
 $\langle \text{proof} \rangle$

**lemma** *icd-path-shift0*: **assumes**  $\langle \text{is-path } \pi \rangle$  **shows**  $\langle (i \text{ icd}^\pi \rightarrow k) = (i - k \text{ icd}^{\pi \ll k} \rightarrow 0) \rangle$   
 $\langle \text{proof} \rangle$

**lemma** *cdi-path-swap*: **assumes**  $\langle \text{is-path } \pi' \rangle \langle j \text{ cd}^{\pi'} \rightarrow k \rangle \langle \pi =_j \pi' \rangle$  **shows**  $\langle j \text{ cd}^{\pi'} \rightarrow k \rangle$   $\langle \text{proof} \rangle$

**lemma** *cdi-path-swap-le*: **assumes**  $\langle \text{is-path } \pi' \rangle \langle j \text{ cd}^{\pi'} \rightarrow k \rangle \langle \pi =_n \pi' \rangle \langle j \leq n \rangle$  **shows**  $\langle j \text{ cd}^{\pi'} \rightarrow k \rangle$   $\langle \text{proof} \rangle$

**lemma** *not-cd-impl-ipd*: **assumes**  $\langle \text{is-path } \pi \rangle$  **and**  $\langle k < i \rangle$  **and**  $\langle \neg i \text{ cd}^\pi \rightarrow k \rangle$  **and**  $\langle \pi \ i \neq \text{return} \rangle$  **obtains**  $j$   
**where**  $\langle j \in \{k..i\} \rangle$  **and**  $\langle \pi \ j = \text{ipd}(\pi \ k) \rangle$   
 $\langle \text{proof} \rangle$

**lemma** *icd-is-the-icd*: **assumes**  $\langle i \text{ icd}^\pi \rightarrow k \rangle$  **shows**  $\langle k = (\text{THE } k. i \text{ icd}^\pi \rightarrow k) \rangle$   $\langle \text{proof} \rangle$

**lemma** *all-ipd-imp-ret*: **assumes**  $\langle \text{is-path } \pi \rangle$  **and**  $\langle \forall i. \pi i \neq \text{return} \longrightarrow (\exists j > i. \pi j = \text{ipd } (\pi i)) \rangle$  **shows**  $\langle \exists j. \pi j = \text{return} \rangle$   
 $\langle \text{proof} \rangle$

**lemma** *loop-has-cd*: **assumes**  $\langle \text{is-path } \pi \rangle$   $\langle 0 < i \rangle$   $\langle \pi i = \pi 0 \rangle$   $\langle \pi 0 \neq \text{return} \rangle$  **shows**  $\langle \exists k < i. i \text{ cd}^\pi \rightarrow k \rangle$   
 $\langle \text{proof} \rangle$

**lemma** *loop-has-cd'*: **assumes**  $\langle \text{is-path } \pi \rangle$   $\langle j < i \rangle$   $\langle \pi i = \pi j \rangle$   $\langle \pi j \neq \text{return} \rangle$  **shows**  $\langle \exists k \in \{j..<i\}. i \text{ cd}^\pi \rightarrow k \rangle$   
 $\langle \text{proof} \rangle$

**lemma** *claim''*: **assumes**  $\text{path}\pi: \langle \text{is-path } \pi \rangle$  **and**  $\text{path}\pi': \langle \text{is-path } \pi' \rangle$   
**and**  $\pi i: \langle \pi i = \pi' i' \rangle$  **and**  $\pi j: \langle \pi j = \pi' j' \rangle$   
**and** *not-cd*:  $\langle \forall k. \neg j \text{ cd}^\pi \rightarrow k \rangle$   $\langle \forall k. \neg i' \text{ cd}^{\pi'} \rightarrow k \rangle$   
**and** *nret*:  $\langle \pi i \neq \text{return} \rangle$   
**and** *ilj*:  $\langle i < j \rangle$   
**shows**  $\langle i' < j' \rangle$   $\langle \text{proof} \rangle$

**lemma** *other-claim'*: **assumes**  $\text{path}: \langle \text{is-path } \pi \rangle$  **and**  $\text{eq}: \langle \pi i = \pi j \rangle$  **and**  $\langle \pi i \neq \text{return} \rangle$   
**and** *icd*:  $\langle \forall k. \neg i \text{ cd}^\pi \rightarrow k \rangle$  **and**  $\langle \forall k. \neg j \text{ cd}^\pi \rightarrow k \rangle$  **shows**  $\langle i = j \rangle$   
 $\langle \text{proof} \rangle$

**lemma** *icd-no-cd-path-shift*: **assumes**  $\langle i \text{ icd}^\pi \rightarrow 0 \rangle$  **shows**  $\langle (\forall k. \neg i - 1 \text{ cd}^{\pi \ll 1} \rightarrow k) \rangle$   
 $\langle \text{proof} \rangle$

**lemma** *claim'*: **assumes**  $\text{path}\pi: \langle \text{is-path } \pi \rangle$  **and**  $\text{path}\pi': \langle \text{is-path } \pi' \rangle$  **and**  
 $\pi i: \langle \pi i = \pi' i' \rangle$  **and**  $\pi j: \langle \pi j = \pi' j' \rangle$  **and** *not-cd*:  
 $\langle i \text{ icd}^\pi \rightarrow 0 \rangle$   $\langle j \text{ icd}^\pi \rightarrow 0 \rangle$   
 $\langle i' \text{ icd}^{\pi'} \rightarrow 0 \rangle$   $\langle j' \text{ icd}^{\pi'} \rightarrow 0 \rangle$   
**and** *ilj*:  $\langle i < j \rangle$   
**and** *nret*:  $\langle \pi i \neq \text{return} \rangle$   
**shows**  $\langle i' < j' \rangle$   
 $\langle \text{proof} \rangle$

**lemma** *other-claim*: **assumes**  $\text{path}: \langle \text{is-path } \pi \rangle$  **and**  $\text{eq}: \langle \pi i = \pi j \rangle$  **and**  $\langle \pi i \neq \text{return} \rangle$   
**and** *icd*:  $\langle i \text{ icd}^\pi \rightarrow 0 \rangle$  **and**  $\langle j \text{ icd}^\pi \rightarrow 0 \rangle$  **shows**  $\langle i = j \rangle$   $\langle \text{proof} \rangle$

**lemma** *cd-trans0*: **assumes**  $\langle j \text{ cd}^\pi \rightarrow 0 \rangle$  **and**  $\langle k \text{ cd}^\pi \rightarrow j \rangle$  **shows**  $\langle k \text{ cd}^\pi \rightarrow 0 \rangle$   $\langle \text{proof} \rangle$

**lemma** *cd-trans*: **assumes**  $\langle j \text{ cd}^\pi \rightarrow i \rangle$  **and**  $\langle k \text{ cd}^\pi \rightarrow j \rangle$  **shows**  $\langle k \text{ cd}^\pi \rightarrow i \rangle$   $\langle \text{proof} \rangle$

**lemma** *excd-impl-exicd*: **assumes**  $\langle \exists k. i \text{ cd}^\pi \rightarrow k \rangle$  **shows**  $\langle \exists k. i \text{ icd}^\pi \rightarrow k \rangle$   
 $\langle \text{proof} \rangle$

**lemma** *cd-split*: **assumes**  $\langle i \text{ cd}^\pi \rightarrow k \rangle$  **and**  $\langle \neg i \text{ icd}^\pi \rightarrow k \rangle$  **obtains**  $m$  **where**  $\langle i \text{ icd}^\pi \rightarrow m \rangle$  **and**  $\langle m \text{ cd}^\pi \rightarrow k \rangle$   
 $\langle \text{proof} \rangle$

**lemma** *cd-induct*[*consumes 1, case-names base IS*]: **assumes**  $\text{prem}: \langle i \text{ cd}^\pi \rightarrow k \rangle$  **and**  $\text{base}: \langle \bigwedge i. i \text{ icd}^\pi \rightarrow k \implies P i \rangle$   
**and** *IH*:  $\langle \bigwedge k' i'. k' \text{ cd}^\pi \rightarrow k \implies P k' \implies i' \text{ icd}^\pi \rightarrow k' \implies P i' \rangle$  **shows**  $\langle P i \rangle$   
 $\langle \text{proof} \rangle$

**lemma** *cdi-prefix*:  $\langle n \text{ cd}^\pi \rightarrow m \implies m < n' \implies n' \leq n \implies n' \text{ cd}^\pi \rightarrow m \rangle$   $\langle \text{proof} \rangle$

**lemma cr-wn'**: assumes  $1: \langle n \text{ cd}^\pi \rightarrow m \rangle$  and  $nc: \langle \neg m' \text{ cd}^\pi \rightarrow m \rangle$  and  $3: \langle m < m' \rangle$  shows  $\langle n < m' \rangle$   
 ⟨proof⟩

**lemma cr-wn''**: assumes  $\langle i \text{ cd}^\pi \rightarrow m \rangle$  and  $\langle j \text{ cd}^\pi \rightarrow n \rangle$  and  $\langle \neg m \text{ cd}^\pi \rightarrow n \rangle$  and  $\langle i \leq j \rangle$  shows  $\langle m \leq n \rangle$   
 ⟨proof⟩

**lemma ret-no-cd**: assumes  $\langle \pi n = \text{return} \rangle$  shows  $\langle \neg n \text{ cd}^\pi \rightarrow k \rangle$  ⟨proof⟩

**lemma ipd-not-self**: assumes  $\langle x \in \text{nodes} \rangle$   $\langle x \neq \text{return} \rangle$  shows  $\langle x \neq \text{ipd } x \rangle$  ⟨proof⟩

**lemma icd-cs**: assumes  $\langle l \text{ icd}^\pi \rightarrow k \rangle$  shows  $\langle \text{cs}^\pi l = \text{cs}^\pi k @ [\pi l] \rangle$   
 ⟨proof⟩

**lemma cd-not-pd**: assumes  $\langle l \text{ cd}^\pi \rightarrow k \rangle$   $\langle \pi l \neq \pi k \rangle$  shows  $\langle \neg \pi l \text{ pd} \rightarrow \pi k \rangle$  ⟨proof⟩

**lemma cd-ipd-is-cd**: assumes  $\langle k < m \rangle$   $\langle \pi m = \text{ipd } (\pi k) \rangle$   $\langle \forall n \in \{k..<m\}. \pi n \neq \text{ipd } (\pi k) \rangle$  and  $\text{mcdj}: \langle m \text{ cd}^\pi \rightarrow j \rangle$  shows  $\langle k \text{ cd}^\pi \rightarrow j \rangle$  ⟨proof⟩

**lemma ipd-pd-cd0**: assumes  $\text{lcd}: \langle n \text{ cd}^\pi \rightarrow 0 \rangle$  shows  $\langle \text{ipd } (\pi 0) \text{ pd} \rightarrow (\pi n) \rangle$   
 ⟨proof⟩

**lemma ipd-pd-cd**: assumes  $\text{lcd}: \langle l \text{ cd}^\pi \rightarrow k \rangle$  shows  $\langle \text{ipd } (\pi k) \text{ pd} \rightarrow (\pi l) \rangle$   
 ⟨proof⟩

**lemma cd-is-cd-ipd**: assumes  $\text{km}: \langle k < m \rangle$  and  $\text{ipd}: \langle \pi m = \text{ipd } (\pi k) \rangle$   $\langle \forall n \in \{k..<m\}. \pi n \neq \text{ipd } (\pi k) \rangle$  and  $\text{cdj}: \langle k \text{ cd}^\pi \rightarrow j \rangle$  and  $\text{nipdj}: \langle \text{ipd } (\pi j) \neq \pi m \rangle$  shows  $\langle m \text{ cd}^\pi \rightarrow j \rangle$  ⟨proof⟩

**lemma ipd-icd-greatest-cd-not-ipd**: assumes  $\text{ipd}: \langle \pi m = \text{ipd } (\pi k) \rangle$   $\langle \forall n \in \{k..<m\}. \pi n \neq \text{ipd } (\pi k) \rangle$  and  $\text{km}: \langle k < m \rangle$  and  $\text{icdj}: \langle m \text{ icd}^\pi \rightarrow j \rangle$  shows  $\langle j = (\text{GREATEST } j. k \text{ cd}^\pi \rightarrow j \wedge \text{ipd } (\pi j) \neq \pi m) \rangle$   
 ⟨proof⟩

**lemma cd-impl-icd-cd**: assumes  $\langle i \text{ cd}^\pi \rightarrow l \rangle$  and  $\langle i \text{ icd}^\pi \rightarrow k \rangle$  and  $\langle \neg i \text{ icd}^\pi \rightarrow l \rangle$  shows  $\langle k \text{ cd}^\pi \rightarrow l \rangle$   
 ⟨proof⟩

**lemma cdi-is-cd-icdi**: assumes  $\langle k \text{ icd}^\pi \rightarrow j \rangle$  shows  $\langle k \text{ cd}^\pi \rightarrow i \iff j \text{ cd}^\pi \rightarrow i \vee i = j \rangle$   
 ⟨proof⟩

**lemma same-ipd-stable**: assumes  $\langle k \text{ cd}^\pi \rightarrow i \rangle$   $\langle k \text{ cd}^\pi \rightarrow j \rangle$   $\langle i < j \rangle$   $\langle \text{ipd } (\pi i) = \text{ipd } (\pi k) \rangle$  shows  $\langle \text{ipd } (\pi j) = \text{ipd } (\pi k) \rangle$   
 ⟨proof⟩

**lemma icd-pd-intermediate'**: assumes  $\text{icd}: \langle i \text{ icd}^\pi \rightarrow k \rangle$  and  $j: \langle k < j \rangle$   $\langle j < i \rangle$  shows  $\langle \pi i \text{ pd} \rightarrow (\pi j) \rangle$   
 ⟨proof⟩

**lemma icd-pd-intermediate**: assumes  $\text{icd}: \langle i \text{ icd}^\pi \rightarrow k \rangle$  and  $j: \langle k < j \rangle$   $\langle j \leq i \rangle$  shows  $\langle \pi i \text{ pd} \rightarrow (\pi j) \rangle$   
 ⟨proof⟩

**lemma no-icd-pd**: assumes  $\text{path}: \langle \text{is-path } \pi \rangle$  and  $\text{noicd}: \langle \forall l \geq n. \neg k \text{ icd}^\pi \rightarrow l \rangle$  and  $\text{nk}: \langle n \leq k \rangle$  shows  $\langle \pi k \text{ pd} \rightarrow \pi n \rangle$   
 ⟨proof⟩

**lemma first-pd-no-cd**: assumes  $\text{path}: \langle \text{is-path } \pi \rangle$  and  $\text{pd}: \langle \pi n \text{ pd} \rightarrow \pi 0 \rangle$  and  $\text{first}: \langle \forall l < n. \pi l \neq \pi n \rangle$  shows  $\langle \forall l. \neg n \text{ cd}^\pi \rightarrow l \rangle$   
 ⟨proof⟩

**lemma** *first-pd-no-icd*: **assumes**  $\langle is\text{-}path\ \pi \rangle$  **and**  $\langle pd:\ \langle \pi\ n\ pd \rightarrow \pi\ 0 \rangle$  **and**  $\langle first:\ \langle \forall\ l < n.\ \pi\ l \neq \pi\ n \rangle$   
**shows**  $\langle \forall\ l.\ \neg\ n\ icd^\pi \rightarrow l \rangle$   
 $\langle proof \rangle$

**lemma** *path-nret-ex-nipd*: **assumes**  $\langle is\text{-}path\ \pi \rangle$   $\langle \forall\ i.\ \pi\ i \neq return \rangle$  **shows**  $\langle \forall\ i.\ (\exists\ j \geq i.\ (\forall\ k > j.\ \pi\ k \neq ipd\ (\pi\ j))) \rangle$   $\langle proof \rangle$

**lemma** *path-nret-ex-all-cd*: **assumes**  $\langle is\text{-}path\ \pi \rangle$   $\langle \forall\ i.\ \pi\ i \neq return \rangle$  **shows**  $\langle \forall\ i.\ (\exists\ j \geq i.\ (\forall\ k > j.\ k\ cd^\pi \rightarrow j)) \rangle$   
 $\langle proof \rangle$

**lemma** *path-nret-inf-all-cd*: **assumes**  $\langle is\text{-}path\ \pi \rangle$   $\langle \forall\ i.\ \pi\ i \neq return \rangle$  **shows**  $\langle \neg\ finite\ \{j.\ \forall\ k > j.\ k\ cd^\pi \rightarrow j\} \rangle$   
 $\langle proof \rangle$

**lemma** *path-nret-inf-icd-seq*: **assumes**  $\langle is\text{-}path\ \pi \rangle$  **and**  $\langle nret:\ \langle \forall\ i.\ \pi\ i \neq return \rangle$   
**obtains**  $f$  **where**  $\langle \forall\ i.\ f\ (Suc\ i)\ icd^\pi \rightarrow f\ i \rangle$   $\langle range\ f = \{i.\ \forall\ j > i.\ j\ cd^\pi \rightarrow i\} \rangle$   $\langle \neg\ (\exists\ i.\ f\ 0\ cd^\pi \rightarrow i) \rangle$   
 $\langle proof \rangle$

**lemma** *cdi-iff-no-strict-pd*:  $\langle i\ cd^\pi \rightarrow k \iff is\text{-}path\ \pi \wedge k < i \wedge \pi\ i \neq return \wedge (\forall\ j \in \{k..i\}.\ \neg\ (\pi\ k,\ \pi\ j) \in pdt) \rangle$   
 $\langle proof \rangle$

## 2.5 Facts about Control Slices

**lemma** *last-cs*:  $\langle last\ (cs^\pi\ i) = \pi\ i \rangle$   $\langle proof \rangle$

**lemma** *cs-not-nil*:  $\langle cs^\pi\ n \neq [] \rangle$   $\langle proof \rangle$

**lemma** *cs-return*: **assumes**  $\langle \pi\ n = return \rangle$  **shows**  $\langle cs^\pi\ n = [\pi\ n] \rangle$   $\langle proof \rangle$

**lemma** *cs-0[simp]*:  $\langle cs^\pi\ 0 = [\pi\ 0] \rangle$   $\langle proof \rangle$

**lemma** *cs-inj*: **assumes**  $\langle is\text{-}path\ \pi \rangle$   $\langle \pi\ n \neq return \rangle$   $\langle cs^\pi\ n = cs^\pi\ n' \rangle$  **shows**  $\langle n = n' \rangle$   
 $\langle proof \rangle$

**lemma** *cs-cases*: **fixes**  $\pi\ i$   
**obtains**  $(base)\ \langle cs^\pi\ i = [\pi\ i] \rangle$  **and**  $\langle \forall\ k.\ \neg\ i\ cd^\pi \rightarrow k \rangle$  |  
 $(depend)\ k$  **where**  $\langle cs^\pi\ i = (cs^\pi\ k)@[\pi\ i] \rangle$  **and**  $\langle i\ icd^\pi \rightarrow k \rangle$   
 $\langle proof \rangle$

**lemma** *cs-length-one*: **assumes**  $\langle length\ (cs^\pi\ i) = 1 \rangle$  **shows**  $\langle cs^\pi\ i = [\pi\ i] \rangle$  **and**  $\langle \forall\ k.\ \neg\ i\ cd^\pi \rightarrow k \rangle$   
 $\langle proof \rangle$

**lemma** *cs-length-g-one*: **assumes**  $\langle length\ (cs^\pi\ i) \neq 1 \rangle$  **obtains**  $k$  **where**  $\langle cs^\pi\ i = (cs^\pi\ k)@[\pi\ i] \rangle$  **and**  $\langle i\ icd^\pi \rightarrow k \rangle$   
 $\langle proof \rangle$

**lemma** *claim*: **assumes**  $\langle is\text{-}path\ \pi \rangle$   $\langle is\text{-}path\ \pi' \rangle$  **and**  $ii:\ \langle cs^\pi\ i = cs^{\pi'}\ i' \rangle$  **and**  $jj:\ \langle cs^\pi\ j = cs^{\pi'}\ j' \rangle$   
**and**  $bl:\ \langle butlast\ (cs^\pi\ i) = butlast\ (cs^{\pi'}\ j) \rangle$  **and**  $nret:\ \langle \pi\ i \neq return \rangle$  **and**  $ilj:\ \langle i < j \rangle$   
**shows**  $\langle i' < j' \rangle$   
 $\langle proof \rangle$

**lemma** *cs-split'*: **assumes**  $\langle cs^\pi\ i = xs@[x,x']@ys \rangle$  **shows**  $\langle \exists\ m.\ cs^\pi\ m = xs@[x] \wedge i\ cd^\pi \rightarrow m \rangle$   
 $\langle proof \rangle$

**lemma cs-split:** **assumes**  $\langle cs^\pi i = xs@[x]@ys@[\pi i] \rangle$  **shows**  $\langle \exists m. cs^\pi m = xs@[x] \wedge i cd^\pi \rightarrow m \rangle$   $\langle proof \rangle$

**lemma cs-less-split:** **assumes**  $\langle xs \prec ys \rangle$  **obtains**  $a$  **as where**  $\langle ys = xs@a\#as \rangle$   
 $\langle proof \rangle$

**lemma cs-select-is-cs:** **assumes**  $\langle is-path \pi \rangle$   $\langle xs \neq Nil \rangle$   $\langle xs \prec cs^\pi k \rangle$  **shows**  $\langle cs^\pi (\pi \downarrow xs) = xs \rangle$   $\langle k cd^\pi \rightarrow (\pi \downarrow xs) \rangle$   $\langle proof \rangle$

**lemma cd-in-cs:** **assumes**  $\langle n cd^\pi \rightarrow m \rangle$  **shows**  $\langle \exists ns. cs^\pi n = (cs^\pi m) @ ns @ [\pi n] \rangle$   
 $\langle proof \rangle$

**lemma butlast-cs-not-cd:** **assumes**  $\langle butlast (cs^\pi m) = butlast (cs^\pi n) \rangle$  **shows**  $\langle \neg m cd^\pi \rightarrow n \rangle$   
 $\langle proof \rangle$

**lemma wn-cs-butlast:** **assumes**  $\langle butlast (cs^\pi m) = butlast (cs^\pi n) \rangle$   $\langle i cd^\pi \rightarrow m \rangle$   $\langle j cd^\pi \rightarrow n \rangle$   $\langle m < n \rangle$  **shows**  
 $\langle i < j \rangle$   
 $\langle proof \rangle$

This is the central theorem making the control slice suitable for matching indices between executions.

**theorem cs-order:** **assumes**  $path: \langle is-path \pi \rangle$   $\langle is-path \pi' \rangle$  **and**  $csi: \langle cs^\pi i = cs^{\pi'} i' \rangle$   
**and**  $csj: \langle cs^\pi j = cs^{\pi'} j' \rangle$  **and**  $nret: \langle \pi i \neq return \rangle$  **and**  $ilj: \langle i < j \rangle$   
**shows**  $\langle i' < j' \rangle$   
 $\langle proof \rangle$

**lemma cs-order-le:** **assumes**  $path: \langle is-path \pi \rangle$   $\langle is-path \pi' \rangle$  **and**  $csi: \langle cs^\pi i = cs^{\pi'} i' \rangle$   
**and**  $csj: \langle cs^\pi j = cs^{\pi'} j' \rangle$  **and**  $nret: \langle \pi i \neq return \rangle$  **and**  $ilj: \langle i \leq j \rangle$   
**shows**  $\langle i' \leq j' \rangle$   $\langle proof \rangle$

**lemmas cs-induct** $[case-names cs] = cs.induct$

**lemma icdi-path-swap:** **assumes**  $\langle is-path \pi' \rangle$   $\langle j icd^\pi \rightarrow k \rangle$   $\langle \pi =_j \pi' \rangle$  **shows**  $\langle j icd^{\pi'} \rightarrow k \rangle$   $\langle proof \rangle$

**lemma icdi-path-swap-le:** **assumes**  $\langle is-path \pi' \rangle$   $\langle j icd^\pi \rightarrow k \rangle$   $\langle \pi =_n \pi' \rangle$   $\langle j \leq n \rangle$  **shows**  $\langle j icd^{\pi'} \rightarrow k \rangle$   $\langle proof \rangle$

**lemma cs-path-swap:** **assumes**  $\langle is-path \pi \rangle$   $\langle is-path \pi' \rangle$   $\langle \pi =_k \pi' \rangle$  **shows**  $\langle cs^\pi k = cs^{\pi'} k \rangle$   $\langle proof \rangle$

**lemma cs-path-swap-le:** **assumes**  $\langle is-path \pi \rangle$   $\langle is-path \pi' \rangle$   $\langle \pi =_n \pi' \rangle$   $\langle k \leq n \rangle$  **shows**  $\langle cs^\pi k = cs^{\pi'} k \rangle$   $\langle proof \rangle$

**lemma cs-path-swap-cd:** **assumes**  $\langle is-path \pi \rangle$  **and**  $\langle is-path \pi' \rangle$  **and**  $\langle cs^\pi n = cs^{\pi'} n' \rangle$  **and**  $\langle n cd^\pi \rightarrow k \rangle$   
**obtains**  $k'$  **where**  $\langle n' cd^{\pi'} \rightarrow k' \rangle$  **and**  $\langle cs^\pi k = cs^{\pi'} k' \rangle$   
 $\langle proof \rangle$

**lemma path-ipd-swap:** **assumes**  $\langle is-path \pi \rangle$   $\langle \pi k \neq return \rangle$   $\langle k < n \rangle$   
**obtains**  $\pi' m$  **where**  $\langle is-path \pi' \rangle$   $\langle \pi =_n \pi' \rangle$   $\langle k < m \rangle$   $\langle \pi' m = ipd (\pi' k) \rangle$   $\langle \forall l \in \{k..<m\}. \pi' l \neq ipd (\pi' k) \rangle$   
 $\langle proof \rangle$

**lemma cs-sorted-list-of-cd':**  $\langle cs^\pi k = map \pi (sorted-list-of-set \{ i . k cd^\pi \rightarrow i \}) @ [\pi k] \rangle$   
 $\langle proof \rangle$

**lemma cs-sorted-list-of-cd:**  $\langle cs^\pi k = map \pi (sorted-list-of-set (\{ i . k cd^\pi \rightarrow i \} \cup \{k\})) \rangle$   $\langle proof \rangle$

**lemma cs-not-ipd:** **assumes**  $\langle k cd^\pi \rightarrow j \wedge ipd (\pi j) \neq ipd (\pi k) \rangle$  **(is**  $\langle ?Q j \rangle$   
**shows**  $\langle cs^\pi (GREATEST j. k cd^\pi \rightarrow j \wedge ipd (\pi j) \neq ipd (\pi k)) = [n \leftarrow cs^\pi k . ipd n \neq ipd (\pi k)] \rangle$   
**(is**  $\langle cs^\pi ?j = filter ?P \rightarrow \rangle$   
 $\langle proof \rangle$



**lemma cs-ipd:** **assumes**  $ipd: \langle \pi m = ipd (\pi k) \rangle \langle \forall n \in \{k..<m\}. \pi n \neq ipd (\pi k) \rangle$   
**and km:**  $\langle k < m \rangle$  **shows**  $\langle cs^\pi m = [n \leftarrow cs^\pi k . ipd n \neq \pi m] @ [\pi m] \rangle$   
 $\langle proof \rangle$

**lemma converged-ipd-same-icd:** **assumes**  $path: \langle is-path \pi \rangle \langle is-path \pi' \rangle$  **and**  $converge: \langle l < m \rangle \langle cs^\pi m = cs^{\pi'} m' \rangle$   
**and csk:**  $\langle cs^\pi k = cs^{\pi'} k' \rangle$  **and**  $icd: \langle l icd^\pi \rightarrow k \rangle$  **and**  $suc: \langle \pi (Suc k) = \pi' (Suc k') \rangle$   
**and ipd:**  $\langle \pi' m' = ipd (\pi k) \rangle \langle \forall n \in \{k'..<m'\}. \pi' n \neq ipd (\pi k) \rangle$   
**shows**  $\langle \exists l'. cs^\pi l = cs^{\pi'} l' \rangle$   
 $\langle proof \rangle$

**lemma converged-same-icd:** **assumes**  $path: \langle is-path \pi \rangle \langle is-path \pi' \rangle$  **and**  $converge: \langle l < n \rangle \langle cs^\pi n = cs^{\pi'} n' \rangle$   
**and csk:**  $\langle cs^\pi k = cs^{\pi'} k' \rangle$  **and**  $icd: \langle l icd^\pi \rightarrow k \rangle$  **and**  $suc: \langle \pi (Suc k) = \pi' (Suc k') \rangle$   
**shows**  $\langle \exists l'. cs^\pi l = cs^{\pi'} l' \rangle$   $\langle proof \rangle$

**lemma cd-is-cs-less:** **assumes**  $\langle l cd^\pi \rightarrow k \rangle$  **shows**  $\langle cs^\pi k \prec cs^\pi l \rangle$   $\langle proof \rangle$

**lemma cs-select-id:** **assumes**  $\langle is-path \pi \rangle \langle \pi k \neq return \rangle$  **shows**  $\langle \pi | cs^\pi k = k \rangle$  **(is**  $\langle ?k = k \rangle$ )  $\langle proof \rangle$

**lemma cs-single-nocd:** **assumes**  $\langle cs^\pi i = [x] \rangle$  **shows**  $\langle \forall k. \neg i cd^\pi \rightarrow k \rangle$   $\langle proof \rangle$

**lemma cs-single-pd-intermed:** **assumes**  $\langle is-path \pi \rangle \langle cs^\pi n = [\pi n] \rangle \langle k \leq n \rangle$  **shows**  $\langle \pi n pd \rightarrow \pi k \rangle$   $\langle proof \rangle$

**lemma cs-first-pd:** **assumes**  $path: \langle is-path \pi \rangle$  **and**  $pd: \langle \pi n pd \rightarrow \pi 0 \rangle$  **and**  $first: \langle \forall l < n. \pi l \neq \pi n \rangle$  **shows**  
 $\langle cs^\pi n = [\pi n] \rangle$   
 $\langle proof \rangle$

**lemma converged-pd-cs-single:** **assumes**  $path: \langle is-path \pi \rangle \langle is-path \pi' \rangle$  **and**  $converge: \langle l < m \rangle \langle cs^\pi m = cs^{\pi'} m' \rangle$   
**and**  $\pi 0: \langle \pi 0 = \pi' 0 \rangle$  **and**  $mpdl: \langle \pi m pd \rightarrow \pi l \rangle$  **and**  $csl: \langle cs^\pi l = [\pi l] \rangle$   
**shows**  $\langle \exists l'. cs^\pi l = cs^{\pi'} l' \rangle$   $\langle proof \rangle$

**lemma converged-cs-single:** **assumes**  $path: \langle is-path \pi \rangle \langle is-path \pi' \rangle$  **and**  $converge: \langle l < m \rangle \langle cs^\pi m = cs^{\pi'} m' \rangle$   
**and**  $\pi 0: \langle \pi 0 = \pi' 0 \rangle$  **and**  $csl: \langle cs^\pi l = [\pi l] \rangle$   
**shows**  $\langle \exists l'. cs^\pi l = cs^{\pi'} l' \rangle$   $\langle proof \rangle$

**lemma converged-cd-same-suc:** **assumes**  $path: \langle is-path \pi \rangle \langle is-path \pi' \rangle$  **and**  $init: \langle \pi 0 = \pi' 0 \rangle$   
**and**  $cd-suc: \langle \forall k k'. cs^\pi k = cs^{\pi'} k' \wedge l cd^\pi \rightarrow k \longrightarrow \pi (Suc k) = \pi' (Suc k') \rangle$  **and**  $converge: \langle l < m \rangle \langle cs^\pi m = cs^{\pi'} m' \rangle$   
**shows**  $\langle \exists l'. cs^\pi l = cs^{\pi'} l' \rangle$   
 $\langle proof \rangle$

**lemma converged-cd-diverge:**  
**assumes**  $path: \langle is-path \pi \rangle \langle is-path \pi' \rangle$  **and**  $init: \langle \pi 0 = \pi' 0 \rangle$  **and**  $notin: \langle \neg (\exists l'. cs^\pi l = cs^{\pi'} l') \rangle$  **and**  
 $converge: \langle l < m \rangle \langle cs^\pi m = cs^{\pi'} m' \rangle$   
**obtains**  $k k'$  **where**  $\langle cs^\pi k = cs^{\pi'} k' \rangle \langle l cd^\pi \rightarrow k \rangle \langle \pi (Suc k) \neq \pi' (Suc k') \rangle$   
 $\langle proof \rangle$

**lemma converged-cd-same-suc-return:** **assumes**  $path: \langle is-path \pi \rangle \langle is-path \pi' \rangle$  **and**  $\pi 0: \langle \pi 0 = \pi' 0 \rangle$

**and cd-suc:**  $\langle \forall k k'. cs^\pi k = cs^{\pi'} k' \wedge l cd^\pi \rightarrow k \longrightarrow \pi (Suc k) = \pi' (Suc k') \rangle$  **and ret:**  $\langle \pi' n' = return \rangle$   
**shows**  $\langle \exists l'. cs^\pi l = cs^{\pi'} l' \rangle \langle proof \rangle$

**lemma converged-cd-diverge-return:** **assumes path:**  $\langle is-path \pi \rangle \langle is-path \pi' \rangle$  **and init:**  $\langle \pi 0 = \pi' 0 \rangle$   
**and notin:**  $\langle \neg (\exists l'. cs^\pi l = cs^{\pi'} l') \rangle$  **and ret:**  $\langle \pi' m' = return \rangle$   
**obtains**  $k k'$  **where**  $\langle cs^\pi k = cs^{\pi'} k' \rangle \langle l cd^\pi \rightarrow k \rangle \langle \pi (Suc k) \neq \pi' (Suc k') \rangle \langle proof \rangle$

**lemma returned-missing-cd-or-loop:** **assumes path:**  $\langle is-path \pi \rangle \langle is-path \pi' \rangle$  **and  $\pi 0$ :**  $\langle \pi 0 = \pi' 0 \rangle$   
**and notin':**  $\langle \neg (\exists k'. cs^\pi k = cs^{\pi'} k') \rangle$  **and nret:**  $\langle \forall n'. \pi' n' \neq return \rangle$  **and ret:**  $\langle \pi n = return \rangle$   
**obtains**  $i i'$  **where**  $\langle i < k \rangle \langle cs^\pi i = cs^{\pi'} i' \rangle \langle \pi (Suc i) \neq \pi' (Suc i') \rangle \langle k cd^\pi \rightarrow i \vee (\forall j' > i'. j' cd^{\pi'} \rightarrow i') \rangle$   
 $\langle proof \rangle$

**lemma missing-cd-or-loop:** **assumes path:**  $\langle is-path \pi \rangle \langle is-path \pi' \rangle$  **and  $\pi 0$ :**  $\langle \pi 0 = \pi' 0 \rangle$  **and notin':**  $\langle \neg (\exists k'. cs^\pi k = cs^{\pi'} k') \rangle$   
**obtains**  $i i'$  **where**  $\langle i < k \rangle \langle cs^\pi i = cs^{\pi'} i' \rangle \langle \pi (Suc i) \neq \pi' (Suc i') \rangle \langle k cd^\pi \rightarrow i \vee (\forall j' > i'. j' cd^{\pi'} \rightarrow i') \rangle$   
 $\langle proof \rangle$

**lemma path-shift-set-cd:** **assumes**  $\langle is-path \pi \rangle$  **shows**  $\langle \{k + j \mid j . n cd^{\pi \ll k} \rightarrow j\} = \{i. (k+n) cd^\pi \rightarrow i \wedge k \leq i\} \rangle$   
 $\langle proof \rangle$

**lemma cs-path-shift-set-cd:** **assumes path:**  $\langle is-path \pi \rangle$  **shows**  $\langle cs^{\pi \ll k} n = map \pi (sorted-list-of-set \{i. k+n cd^\pi \rightarrow i \wedge k \leq i\}) @ [\pi (k+n)] \rangle$   
 $\langle proof \rangle$

**lemma cs-split-shift-cd:** **assumes**  $\langle n cd^\pi \rightarrow j \rangle$  **and**  $\langle j < k \rangle$  **and**  $\langle k < n \rangle$  **and**  $\langle \forall j' < k. n cd^\pi \rightarrow j' \longrightarrow j' \leq j \rangle$   
**shows**  $\langle cs^\pi n = cs^\pi j @ cs^{\pi \ll k} (n-k) \rangle$   
 $\langle proof \rangle$

**lemma cs-split-shift-nocd:** **assumes**  $\langle is-path \pi \rangle$  **and**  $\langle k < n \rangle$  **and**  $\langle \forall j. n cd^\pi \rightarrow j \longrightarrow k \leq j \rangle$  **shows**  $\langle cs^\pi n = cs^{\pi \ll k} (n-k) \rangle$   
 $\langle proof \rangle$

**lemma shifted-cs-eq-is-eq:** **assumes**  $\langle is-path \pi \rangle$  **and**  $\langle is-path \pi' \rangle$  **and**  $\langle cs^\pi k = cs^{\pi'} k' \rangle$  **and**  $\langle cs^{\pi \ll k} n = cs^{\pi' \ll k'} n' \rangle$  **shows**  $\langle cs^\pi (k+n) = cs^{\pi'} (k'+n') \rangle$   
 $\langle proof \rangle$

**lemma cs-eq-is-eq-shifted:** **assumes**  $\langle is-path \pi \rangle$  **and**  $\langle is-path \pi' \rangle$  **and**  $\langle cs^\pi k = cs^{\pi'} k' \rangle$  **and**  $\langle cs^\pi (k+n) = cs^{\pi'} (k'+n') \rangle$  **shows**  $\langle cs^{\pi \ll k} n = cs^{\pi' \ll k'} n' \rangle$   
 $\langle proof \rangle$

**lemma converged-cd-diverge-cs:** **assumes**  $\langle is-path \pi \rangle$  **and**  $\langle is-path \pi' \rangle$  **and**  $\langle cs^\pi j = cs^{\pi'} j' \rangle$  **and**  $\langle j < l \rangle$  **and**  
 $\langle \neg (\exists l'. cs^\pi l = cs^{\pi'} l') \rangle$  **and**  $\langle l < m \rangle$  **and**  $\langle cs^\pi m = cs^{\pi'} m' \rangle$   
**obtains**  $k k'$  **where**  $\langle j \leq k \rangle \langle cs^\pi k = cs^{\pi'} k' \rangle$  **and**  $\langle l cd^\pi \rightarrow k \rangle$  **and**  $\langle \pi (Suc k) \neq \pi' (Suc k') \rangle$   
 $\langle proof \rangle$

**lemma cs-ipd-conv:** **assumes**  $csk: \langle cs^\pi k = cs^{\pi'} k' \rangle$  **and**  $ipd: \langle \pi l = ipd (\pi k) \rangle \langle \pi' l' = ipd (\pi' k') \rangle$   
**and**  $nipd: \langle \forall n \in \{k..<l\}. \pi n \neq ipd (\pi k) \rangle \langle \forall n' \in \{k'..<l'\}. \pi' n' \neq ipd (\pi' k') \rangle$  **and**  $kl: \langle k < l \rangle \langle k' < l' \rangle$   
**shows**  $\langle cs^\pi l = cs^{\pi'} l' \rangle \langle proof \rangle$

**lemma cp-eq-cs:** **assumes**  $\langle ((\sigma, k), (\sigma', k')) \in cp \rangle$  **shows**  $\langle cs^{path} \sigma k = cs^{path} \sigma' k' \rangle$   
 $\langle proof \rangle$

**lemma** *cd-cs-swap*: **assumes**  $\langle l \text{ cd}^\pi \rightarrow k \rangle \langle \text{cs}^\pi l = \text{cs}^{\pi'} l' \rangle \langle \text{cs}^\pi k = \text{cs}^{\pi'} k' \rangle$  **shows**  $\langle l' \text{ cd}^{\pi'} \rightarrow k' \rangle$   $\langle \text{proof} \rangle$

## 2.6 Facts about Observations

**lemma** *kth-obs-not-none*: **assumes**  $\langle \text{is-kth-obs} (\text{path } \sigma) k i \rangle$  **obtains a where**  $\langle \text{obs } \sigma i = \text{Some } a \rangle$   $\langle \text{proof} \rangle$

**lemma** *kth-obs-unique*:  $\langle \text{is-kth-obs } \pi k i \implies \text{is-kth-obs } \pi k j \implies i = j \rangle$   $\langle \text{proof} \rangle$

**lemma** *obs-none-no-kth-obs*: **assumes**  $\langle \text{obs } \sigma k = \text{None} \rangle$  **shows**  $\langle \neg (\exists i. \text{is-kth-obs} (\text{path } \sigma) k i) \rangle$   $\langle \text{proof} \rangle$

**lemma** *obs-some-kth-obs* : **assumes**  $\langle \text{obs } \sigma k \neq \text{None} \rangle$  **obtains i where**  $\langle \text{is-kth-obs} (\text{path } \sigma) k i \rangle$   $\langle \text{proof} \rangle$

**lemma** *not-none-is-obs*: **assumes**  $\langle \text{att}(\pi i) \neq \text{None} \rangle$  **shows**  $\langle \text{is-kth-obs } \pi (\text{card} (\text{obs-ids } \pi \cap \{..<i\})) i \rangle$   $\langle \text{proof} \rangle$

**lemma** *in-obs-ids-is-kth-obs*: **assumes**  $\langle i \in \text{obs-ids } \pi \rangle$  **obtains k where**  $\langle \text{is-kth-obs } \pi k i \rangle$   $\langle \text{proof} \rangle$

**lemma** *kth-obs-stable*: **assumes**  $\langle \text{is-kth-obs } \pi l j \rangle \langle k < l \rangle$  **shows**  $\langle \exists i. \text{is-kth-obs } \pi k i \rangle$   $\langle \text{proof} \rangle$

**lemma** *kth-obs-mono*: **assumes**  $\langle \text{is-kth-obs } \pi k i \rangle \langle \text{is-kth-obs } \pi l j \rangle \langle k < l \rangle$  **shows**  $\langle i < j \rangle$   $\langle \text{proof} \rangle$

**lemma** *kth-obs-le-iff*: **assumes**  $\langle \text{is-kth-obs } \pi k i \rangle \langle \text{is-kth-obs } \pi l j \rangle$  **shows**  $\langle k < l \iff i < j \rangle$   $\langle \text{proof} \rangle$

**lemma** *ret-obs-all-obs*: **assumes** *path*:  $\langle \text{is-path } \pi \rangle$  **and** *iki*:  $\langle \text{is-kth-obs } \pi k i \rangle$  **and** *ret*:  $\langle \pi i = \text{return} \rangle$  **and** *kl*:  $\langle k < l \rangle$  **obtains j where**  $\langle \text{is-kth-obs } \pi l j \rangle$   $\langle \text{proof} \rangle$

**lemma** *no-kth-obs-missing-cs*: **assumes** *path*:  $\langle \text{is-path } \pi \rangle \langle \text{is-path } \pi' \rangle$  **and** *iki*:  $\langle \text{is-kth-obs } \pi k i \rangle$  **and** *not-in- $\pi'$* :  $\langle \neg (\exists i'. \text{is-kth-obs } \pi' k i') \rangle$  **obtains l j where**  $\langle \text{is-kth-obs } \pi l j \rangle \langle \neg (\exists j'. \text{cs}^\pi j = \text{cs}^{\pi'} j') \rangle$   $\langle \text{proof} \rangle$

**lemma** *kth-obs-cs-missing-cs*: **assumes** *path*:  $\langle \text{is-path } \pi \rangle \langle \text{is-path } \pi' \rangle$  **and** *iki*:  $\langle \text{is-kth-obs } \pi k i \rangle$  **and** *iki'*:  $\langle \text{is-kth-obs } \pi' k i' \rangle$  **and** *csi*:  $\langle \text{cs}^\pi i \neq \text{cs}^{\pi'} i' \rangle$  **obtains l j where**  $\langle j \leq i \rangle \langle \text{is-kth-obs } \pi l j \rangle \langle \neg (\exists j'. \text{cs}^\pi j = \text{cs}^{\pi'} j') \rangle \mid l' j' \text{ where } \langle j' \leq i' \rangle \langle \text{is-kth-obs } \pi' l' j' \rangle \langle \neg (\exists j. \text{cs}^\pi j = \text{cs}^{\pi'} j') \rangle$   $\langle \text{proof} \rangle$

## 2.7 Facts about Data

**lemma** *reads-restrict1*:  $\langle \sigma \upharpoonright (\text{reads } n) = \sigma' \upharpoonright (\text{reads } n) \implies \forall x \in \text{reads } n. \sigma x = \sigma' x \rangle$   $\langle \text{proof} \rangle$

**lemma** *reads-restrict2*:  $\langle \forall x \in \text{reads } n. \sigma x = \sigma' x \implies \sigma \upharpoonright (\text{reads } n) = \sigma' \upharpoonright (\text{reads } n) \rangle$   $\langle \text{proof} \rangle$

**lemma** *reads-restrict*:  $\langle (\sigma \upharpoonright (\text{reads } n) = \sigma' \upharpoonright (\text{reads } n)) = (\forall x \in \text{reads } n. \sigma x = \sigma' x) \rangle$   $\langle \text{proof} \rangle$

**lemma** *reads-restr-suc*:  $\langle \sigma \upharpoonright (\text{reads } n) = \sigma' \upharpoonright (\text{reads } n) \implies \text{suc } n \sigma = \text{suc } n \sigma' \rangle$   $\langle \text{proof} \rangle$

**lemma** *reads-restr-sem*:  $\langle \sigma \upharpoonright (\text{reads } n) = \sigma' \upharpoonright (\text{reads } n) \implies \forall v \in \text{writes } n. \text{sem } n \sigma v = \text{sem } n \sigma' v \rangle$   $\langle \text{proof} \rangle$

**lemma** *reads-obsp*: **assumes**  $\langle \text{path } \sigma k = \text{path } \sigma' k' \rangle \langle \sigma^k \upharpoonright (\text{reads } (\text{path } \sigma k)) = \sigma'^{k'} \upharpoonright (\text{reads } (\text{path } \sigma k)) \rangle$  **shows**  $\langle \text{obsp } \sigma k = \text{obsp } \sigma' k' \rangle$   $\langle \text{proof} \rangle$

**lemma** *no-writes-unchanged0*: **assumes**  $\langle \forall l < k. v \notin \text{writes}(\text{path } \sigma l) \rangle$  **shows**  $\langle (\sigma^k) v = \sigma v \rangle$   $\langle \text{proof} \rangle$

**lemma** *written-read-dd*: **assumes**  $\langle is\text{-}path\ \pi \rangle \langle v \in reads\ (\pi\ k) \rangle \langle v \in writes\ (\pi\ j) \rangle \langle j < k \rangle$  **obtains**  $l$  **where**  $\langle k\ dd^{\pi, v} \rightarrow l \rangle$

$\langle proof \rangle$

**lemma** *no-writes-unchanged*: **assumes**  $\langle k \leq l \rangle \langle \forall j \in \{k..<l\}. v \notin writes(path\ \sigma\ j) \rangle$  **shows**  $\langle (\sigma^l)\ v = (\sigma^k)\ v \rangle$

$\langle proof \rangle$

**lemma** *ddi-value*: **assumes**  $\langle l\ dd^{(path\ \sigma), v} \rightarrow k \rangle$  **shows**  $\langle (\sigma^l)\ v = (\sigma^{Suc\ k})\ v \rangle$

$\langle proof \rangle$

**lemma** *written-value*: **assumes**  $\langle path\ \sigma\ l = path\ \sigma'\ l' \rangle \langle \sigma^l \upharpoonright reads\ (path\ \sigma\ l) = \sigma'^{l'} \upharpoonright reads\ (path\ \sigma'\ l') \rangle \langle v \in writes\ (path\ \sigma\ l) \rangle$

**shows**  $\langle (\sigma^{Suc\ l})\ v = (\sigma'^{Suc\ l'})\ v \rangle$

$\langle proof \rangle$

## 2.8 Facts about Contradicting Paths

**lemma** *obsp-contradict*: **assumes**  $csk: \langle cs^{path\ \sigma}\ k = cs^{path\ \sigma'}\ k' \rangle$  **and**  $obs: \langle obsp\ \sigma\ k \neq obsp\ \sigma'\ k' \rangle$  **shows**  $\langle (\sigma', k')\ c\ (\sigma, k) \rangle$

$\langle proof \rangle$

**lemma** *missing-cs-contradicts*: **assumes**  $notin: \langle \neg(\exists k'. cs^{path\ \sigma}\ k = cs^{path\ \sigma'}\ k') \rangle$  **and**  $converge: \langle k < n \rangle \langle cs^{path\ \sigma}\ n = cs^{path\ \sigma'}\ n' \rangle$  **shows**  $\langle \exists j'. (\sigma', j')\ c\ (\sigma, k) \rangle$

$\langle proof \rangle$

**theorem** *obs-neq-contradicts-term*: **fixes**  $\sigma\ \sigma'$  **defines**  $\pi: \langle \pi \equiv path\ \sigma \rangle$  **and**  $\pi': \langle \pi' \equiv path\ \sigma' \rangle$  **assumes**  $ret: \langle \pi\ n = return \rangle \langle \pi'\ n' = return \rangle$  **and**  $obsne: \langle obs\ \sigma \neq obs\ \sigma' \rangle$

**shows**  $\langle \exists k\ k'. ((\sigma', k')\ c\ (\sigma, k) \wedge \pi\ k \in dom\ (att)) \vee ((\sigma, k)\ c\ (\sigma', k') \wedge \pi'\ k' \in dom\ (att)) \rangle$

$\langle proof \rangle$

**lemma** *obs-neq-some-contradicts'*: **fixes**  $\sigma\ \sigma'$  **defines**  $\pi: \langle \pi \equiv path\ \sigma \rangle$  **and**  $\pi': \langle \pi' \equiv path\ \sigma' \rangle$

**assumes**  $obsnecs: \langle obsp\ \sigma\ i \neq obsp\ \sigma'\ i' \vee cs^{\pi}\ i \neq cs^{\pi'}\ i' \rangle$

**and**  $iki: \langle is\text{-}kth\text{-}obs\ \pi\ k\ i \rangle$  **and**  $iki': \langle is\text{-}kth\text{-}obs\ \pi'\ k'\ i' \rangle$

**shows**  $\langle \exists k\ k'. ((\sigma', k')\ c\ (\sigma, k) \wedge \pi\ k \in dom\ (att)) \vee ((\sigma, k)\ c\ (\sigma', k') \wedge \pi'\ k' \in dom\ (att)) \rangle$

$\langle proof \rangle$

**theorem** *obs-neq-some-contradicts*: **fixes**  $\sigma\ \sigma'$  **defines**  $\pi: \langle \pi \equiv path\ \sigma \rangle$  **and**  $\pi': \langle \pi' \equiv path\ \sigma' \rangle$

**assumes**  $obsne: \langle obs\ \sigma\ k \neq obs\ \sigma'\ k \rangle$  **and**  $not\ none: \langle obs\ \sigma\ k \neq None \rangle \langle obs\ \sigma'\ k \neq None \rangle$

**shows**  $\langle \exists k\ k'. ((\sigma', k')\ c\ (\sigma, k) \wedge \pi\ k \in dom\ (att)) \vee ((\sigma, k)\ c\ (\sigma', k') \wedge \pi'\ k' \in dom\ (att)) \rangle$

$\langle proof \rangle$

**theorem** *obs-neq-ret-contradicts*: **fixes**  $\sigma\ \sigma'$  **defines**  $\pi: \langle \pi \equiv path\ \sigma \rangle$  **and**  $\pi': \langle \pi' \equiv path\ \sigma' \rangle$

**assumes**  $ret: \langle \pi\ n = return \rangle$  **and**  $obsne: \langle obs\ \sigma'\ i \neq obs\ \sigma\ i \rangle$  **and**  $obs: \langle obs\ \sigma'\ i \neq None \rangle$

**shows**  $\langle \exists k\ k'. ((\sigma', k')\ c\ (\sigma, k) \wedge \pi\ k \in dom\ (att)) \vee ((\sigma, k)\ c\ (\sigma', k') \wedge \pi'\ k' \in dom\ (att)) \rangle$

$\langle proof \rangle$

## 2.9 Facts about Critical Observable Paths

**lemma** *contradicting-in-cp*: **assumes**  $leq: \langle \sigma =_L\ \sigma' \rangle$  **and**  $cseq: \langle cs^{path\ \sigma}\ k = cs^{path\ \sigma'}\ k' \rangle$

**and**  $readv: \langle v \in reads(path\ \sigma\ k) \rangle$  **and**  $vneq: \langle (\sigma^k)\ v \neq (\sigma'^{k'})\ v \rangle$  **shows**  $\langle ((\sigma, k), (\sigma', k')) \in cp \rangle$

$\langle proof \rangle$

**theorem** *contradicting-in-cop*: **assumes**  $\langle \sigma =_L\ \sigma' \rangle$  **and**  $\langle (\sigma', k')\ c\ (\sigma, k) \rangle$  **and**  $\langle path\ \sigma\ k \in dom\ (att) \rangle$

**shows**  $\langle ((\sigma, k), \sigma', k') \in cop \rangle$   $\langle proof \rangle$

**theorem** *cop-correct-term*: **fixes**  $\sigma \sigma'$  **defines**  $\pi: \langle \pi \equiv \text{path } \sigma \rangle$  **and**  $\pi': \langle \pi' \equiv \text{path } \sigma' \rangle$   
**assumes** *ret*:  $\langle \pi \text{ n} = \text{return} \rangle$   $\langle \pi' \text{ n}' = \text{return} \rangle$  **and** *obsne*:  $\langle \text{obs } \sigma \neq \text{obs } \sigma' \rangle$  **and** *leq*:  $\langle \sigma =_L \sigma' \rangle$   
**shows**  $\langle \exists k k'. ((\sigma, k), (\sigma', k')) \in \text{cop} \vee ((\sigma', k'), (\sigma, k)) \in \text{cop} \rangle$   
 $\langle \text{proof} \rangle$

**theorem** *cop-correct-ret*: **fixes**  $\sigma \sigma'$  **defines**  $\pi: \langle \pi \equiv \text{path } \sigma \rangle$  **and**  $\pi': \langle \pi' \equiv \text{path } \sigma' \rangle$   
**assumes** *ret*:  $\langle \pi \text{ n} = \text{return} \rangle$  **and** *obsne*:  $\langle \text{obs } \sigma \text{ i} \neq \text{obs } \sigma' \text{ i} \rangle$  **and** *obs*:  $\langle \text{obs } \sigma' \text{ i} \neq \text{None} \rangle$  **and** *leq*:  $\langle \sigma =_L \sigma' \rangle$   
**shows**  $\langle \exists k k'. ((\sigma, k), (\sigma', k')) \in \text{cop} \vee ((\sigma', k'), (\sigma, k)) \in \text{cop} \rangle$   
 $\langle \text{proof} \rangle$

**theorem** *cop-correct-nterm*: **assumes** *obsne*:  $\langle \text{obs } \sigma \text{ k} \neq \text{obs } \sigma' \text{ k} \rangle$   $\langle \text{obs } \sigma \text{ k} \neq \text{None} \rangle$   $\langle \text{obs } \sigma' \text{ k} \neq \text{None} \rangle$   
**and** *leq*:  $\langle \sigma =_L \sigma' \rangle$   
**shows**  $\langle \exists k k'. ((\sigma, k), (\sigma', k')) \in \text{cop} \vee ((\sigma', k'), (\sigma, k)) \in \text{cop} \rangle$   
 $\langle \text{proof} \rangle$

## 2.10 Correctness of the Characterisation

The following is our main correctness result. If there exist no critical observable paths, then the program is secure.

**theorem** *cop-correct*: **assumes**  $\langle \text{cop} = \text{empty} \rangle$  **shows**  $\langle \text{secure} \rangle$   $\langle \text{proof} \rangle$

Our characterisation is not only correct, it is also precise in the way that *cp* characterises exactly the matching indices in executions for low equivalent input states where diverging data is read. This follows easily as the inverse implication to lemma *contradicting-in-cp* can be shown by simple induction.

**theorem** *cp-iff-reads-contradict*:  $\langle ((\sigma, k), (\sigma', k')) \in \text{cp} \longleftrightarrow \sigma =_L \sigma' \wedge \text{cs}^{\text{path } \sigma} k = \text{cs}^{\text{path } \sigma'} k' \wedge (\exists v \in \text{reads}(\text{path } \sigma \text{ k}). (\sigma^k) v \neq (\sigma'^{k'}) v) \rangle$   
 $\langle \text{proof} \rangle$

In the same way the inverse implication to *contradicting-in-cop* follows easily such that we obtain the following characterisation of *cop*.

**theorem** *cop-iff-contradicting*:  $\langle ((\sigma, k), (\sigma', k')) \in \text{cop} \longleftrightarrow \sigma =_L \sigma' \wedge (\sigma', k') \text{ c } (\sigma, k) \wedge \text{path } \sigma \text{ k} \in \text{dom att} \rangle$   
 $\langle \text{proof} \rangle$

## 2.11 Correctness of the Single Path Approximation

**theorem** *cp-in-scp*: **assumes**  $\langle ((\sigma, k), (\sigma', k')) \in \text{cp} \rangle$  **shows**  $\langle (\text{path } \sigma, k) \in \text{scp} \wedge (\text{path } \sigma', k') \in \text{scp} \rangle$   
 $\langle \text{proof} \rangle$

**theorem** *cop-in-scop*: **assumes**  $\langle ((\sigma, k), (\sigma', k')) \in \text{cop} \rangle$  **shows**  $\langle (\text{path } \sigma, k) \in \text{scop} \wedge (\text{path } \sigma', k') \in \text{scop} \rangle$   
 $\langle \text{proof} \rangle$

The main correctness result for our single execution approximation follows directly.

**theorem** *scop-correct*: **assumes**  $\langle \text{scop} = \text{empty} \rangle$  **shows**  $\langle \text{secure} \rangle$   
 $\langle \text{proof} \rangle$

**end**

**end**

### 3 Example: Program Dependence Graphs

Program dependence graph (PDG) based slicing provides a very crude but direct approximation of our characterisation. As such we can easily derive a corresponding correctness result.

**theory** *PDG* **imports** *IFC*  
**begin**

**context** *IFC*  
**begin**

We utilise our established dependencies on program paths to define the PDG. Note that PDGs usually only contain immediate control dependencies instead of the transitive ones we use here. However as slicing is considering reachability questions this does not affect the result.

**inductive-set** *pdg* **where**  
 $\langle \llbracket i \text{ cd}^\pi \rightarrow k \rrbracket \implies (\pi \ k, \pi \ i) \in \text{pdg} \rangle \mid$   
 $\langle \llbracket i \text{ dd}^{\pi, v} \rightarrow k \rrbracket \implies (\pi \ k, \pi \ i) \in \text{pdg} \rangle$

The set of sources is the set of nodes reading high variables.

**inductive-set** *sources* **where**  
 $\langle n \in \text{nodes} \implies h \in \text{hvars} \implies h \in \text{reads } n \implies n \in \text{sources} \rangle$

The forward slice is the set of nodes reachable in the PDG from the set of sources. To ensure security slicing aims to prove that no observable node is contained in the

**inductive-set** *slice* **where**  
 $\langle n \in \text{sources} \implies n \in \text{slice} \rangle \mid$   
 $\langle m \in \text{slice} \implies (m, n) \in \text{pdg} \implies n \in \text{slice} \rangle$

As the PDG does not contain data control dependencies themselves we have to decompose these.

**lemma** *dcd-pdg*: **assumes**  $\langle n \text{ dcd}^{\pi, v} \rightarrow m \text{ via } \pi' \ m' \rangle$  **obtains** *l* **where**  $\langle (\pi \ m, l) \in \text{pdg} \rangle$  **and**  $\langle (l, \pi \ n) \in \text{pdg} \rangle$   
 $\langle \text{proof} \rangle$

By induction it directly follows that the slice is an approximation of the single critical paths.

**lemma** *scp-slice*:  $\langle (\pi, i) \in \text{scp} \implies \pi \ i \in \text{slice} \rangle$   
 $\langle \text{proof} \rangle$

**lemma** *scop-slice*:  $\langle (\pi, i) \in \text{scop} \implies \pi \ i \in \text{slice} \cap \text{dom}(\text{att}) \rangle$   $\langle \text{proof} \rangle$

The requirement targeted by slicing, that no observable node is contained in the slice, is thereby a sound criteria for security.

**lemma** *pdg-correct*: **assumes**  $\langle \text{slice} \cap \text{dom}(\text{att}) = \{\} \rangle$  **shows**  $\langle \text{secure} \rangle$   
 $\langle \text{proof} \rangle$

**end**

**end**

### References

- [1] A. Bohannon, B. C. Pierce, V. Sjöberg, S. Weirich, and S. Zdancewic. Reactive noninterference. In *Proceedings of the 16th ACM Conference on Computer and Communications Security, CCS '09*, pages 79–90, New York, NY, USA, 2009. ACM.