Supplementary Proofs

A Chain Containment

Here we provide the proof for a key claim from the paper that we used while proving the uni-dummy relation. Let us first introduce useful notation before restating the claim:

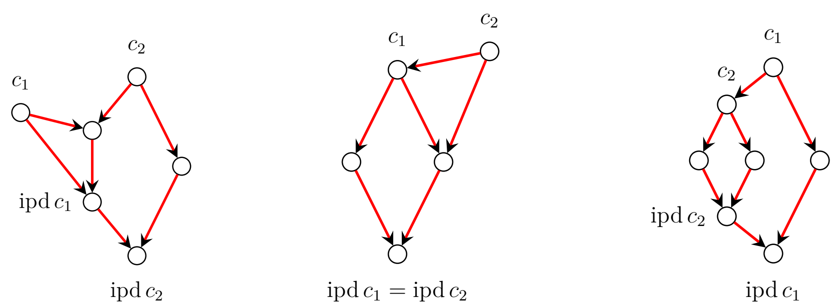
$$c_1 \preceq c_2 := \text{ipd}\, c1 \in ir^+(c2)$$
$$c_1 \prec c_2 := \text{ipd}\, c1 \in ir(c2)$$

▷ Claim 1 (Chain Containment). If $c_1 \cap \cdots \cap c_k$ and $\text{ipd}\, c_1 <_{idx} \text{ipd}\, c_k$, then $\exists i, c_1 \prec c_i$.

Intersection of two influence regions makes them comparable as illustrated in Figure 1:

▶ **Lemma 2.** $c_1 \cap c_2 \implies c_1 \prec c_2 \;\vee\; c_1 \succeq c_2$.

Proof. If $\text{ipd}\, c_1 = \text{ipd}\, c_2$ we have $c_1 \succeq c_2$. Otherwise, let $x \in ir^+(c_1)$ and $x \in ir^+(c_2)$. From $x \rhd \text{ipd}\, c_1 \;\wedge\; x \rhd \text{ipd}\, c_2$ it follows $\text{ipd}\, c_1 \rhd \text{ipd}\, c_2 \;\vee\; \text{ipd}\, c_2 \rhd \text{ipd}\, c_1$. In the first case we have $c_1 \to^* x \rhd \text{ipd}\, c_1 \rhd \text{ipd}\, c_2$ and therefore $\text{ipd}\, c_1 \in ir(c_2)$ and the second case is analogous. ◀



(a) $c_1 \prec c_2$ **(b)** $c_1 \preceq c_2 \preceq c_1$ **(c)** $c_1 \succ c_2$

Figure 1 Possible ways of how the ipd's of two intersecting influence regions relate.

For proving the claim, we need the following slightly stronger induction hypothesis:

▶ **Lemma 3.**

$$\begin{aligned} \forall\; c_1 \cap \cdots \cap c_k,\; & c_1 \prec c_2 \\ & \vee\; c_1 \succeq \cdots \succeq c_k \\ & \vee\; c_1 \cap \tilde{c}_2 \cap \cdots \cap \tilde{c}_l \cap c_k \textit{ with } l < k-1 \textit{ and } \tilde{c}_i \in \{c_2, \ldots, c_{k-1}\} \textit{ for all } i. \end{aligned}$$

Proof. We do an induction on the chain length. If $k = 2$ then $c_1 \cap c_2$ and Lemma 2 gives $c_1 \prec c_2 \;\vee\; c_1 \succeq c_2$.

Otherwise, consider $c_1 \cap c_2 \cap \cdots \cap c_k$. Again by Lemma 2 we get $c_1 \prec c_2 \;\vee\; c_1 \succeq c_2$. In the first case the proof is done. If $c_1 \succeq c_2$, we apply the induction hypothesis to $c_2 \cap \cdots \cap c_k$ which yields one of:

- $c_2 \prec c_3$. From $c_1 \succeq c_2 \prec c_3$ we can conclude $c_1 \cap c_3$ because $\text{ipd}\, c_2$ is contained in both $ir^+(c_1)$ and $ir^+(c_3)$. This gives us a shorter chain $c_1 \cap c_3 \cap \cdots \cap c_k$ as required.
- $c_2 \succeq \cdots \succeq c_k$, from which we conclude $c_1 \succeq c_2 \succeq \cdots \succeq c_k$.
- A shorter chain $c_2 \cap \cdots \cap c_k$, from which we construct a shorter chain $c_1 \cap c_2 \cap \cdots \cap c_k$. ◀

Proof of Claim 1. Let $c_1 \cap \cdots \cap c_k$ and $\operatorname{ipd} c_1 <_{idx} \operatorname{ipd} c_k$. We do a strong induction on the chain length. Applying Lemma 3, we get one of these options:

- $c_1 \prec c_2$, which is the required result.
- $c_1 \succeq \cdots \succeq c_k$. As $c_i \succeq c_{i+1}$ implies $\operatorname{ipd} c_{i+1} \triangleright \operatorname{ipd} c_i$, we get $\operatorname{ipd} c_k \triangleright \operatorname{ipd} c_1$, contradicting $\operatorname{ipd} c_1 <_{idx} \operatorname{ipd} c_k$.
- A shorter intersection chain $c_1 \cap \cdots \cap c_k$ from which we conclude by strong induction. ◀

In our development, Claim 1 is found as `Theorem chain_containment`.

B Equivalence of *uni* Notions

Here we prove the equivalence of our *uni-dummy relation* to Theorem 4.1 from Hack and Moll by proving that our notion of *uni* coincides with theirs.

Therefore we restate their recursive definition of uni_{cdep} and our definition of *uni*, all of which refer to g_{orig}:

▶ **Definition 4.** $\forall c\ v\ w \in V$, let

$$c \to w \in cdep(v) := c \to w \ \wedge\ w \triangleright v \ \wedge\ c \not\triangleright v.$$

$$uni_{cdep}\ v := \forall c \to w \in cdep(v), uni_{cdep}\ c \ \wedge\ \neg secret\_cond\ c.$$

$$uni\ v := \forall c \in V, v \in ir(c) \implies \neg secret\_cond\ c.$$

The following two lemmata relate the notion of influence regions and control dependence:

▶ **Lemma 5.** $c \to w \in cdep(v) \implies v \in ir(c)$.

Proof. We have $c \to w \triangleright v$. As $w \in ir(c)$ it is $w \triangleright \operatorname{ipd} c$. It follows $v \triangleright \operatorname{ipd} c \ \vee\ \operatorname{ipd} c \triangleright v$, but the latter is contradictory because $c \triangleright \operatorname{ipd} c$, but $c \not\triangleright v$ per assumption.

Therefore we get $c \to^* v \triangleright \operatorname{ipd} c$ and because $v \neq \operatorname{ipd} c$ (else $c \triangleright v$), we have $v \in ir(c)$. ◀

▶ **Lemma 6.** $v \in ir(c) \implies \exists \tilde{c} \to w \in cdep(v)$ *with* $\tilde{c} \in (ir(c) \cup \{c\})$.

Proof. Consider the set $P_v := \{x \in ir(c) \mid x \triangleright v\}$. It is nonempty as $v \in P_v$, so let $w := \min_{<_{idx}} P_v$. Now take any predecessor $\tilde{c} \in (ir(c) \cup \{c\})$ of w, which exists because $w \in ir(c)$.

It is $\tilde{c} \not\triangleright v$, otherwise w would not be the $<_{idx}$-minimum of P_v (if $\tilde{c} = c$, $\tilde{c} \not\triangleright v$ because $v \in ir(c)$). Together with $\tilde{c} \to w \triangleright v$ we get $\tilde{c} \to w \in cdep(v)$. ◀

▶ **Theorem 7.** $\forall v \in V, uni\ v \iff uni_{cdep}\ v$.

Proof.

$\implies$: Via induction on idx (i.e. assume the statement is shown for all $w <_{idx} v$). Let $c \to w \in cdep(v)$. By Lemma 5, $v \in ir(c)$ and so by $uni\ v$, $\neg secret\_cond\ c$.

We still need to show $uni_{cdep}\ c$, which we do by showing $uni\ c$ and applying induction. Therefore, let $c \in ir(\tilde{c})$. From $v \in ir(c)$ it follows that also $v \in ir(\tilde{c})$ (containment of influence regions) and therefore, by $uni\ v$, $\neg secret\_cond\ \tilde{c}$ which concludes.

$\impliedby$: Again via induction on idx. Let $v \in ir(c)$. By Lemma 6, $\exists\ \tilde{c} \to w \in cdep(v)$ with $\tilde{c} \in (ir(c) \cup \{c\})$. By $uni_{cdep}\ v$ we have $uni_{cdep}\ \tilde{c} \ \wedge\ \neg secret\_cond\ \tilde{c}$.

If $c = \tilde{c}$, we are done. Otherwise we have $\tilde{c} \in ir(c)$ and we use induction to get $uni\ \tilde{c}$ from which then follows $\neg secret\_cond\ c$. ◀

While it is not required for proving semantic preservation nor control-flow security, we provided a proof of `Theorem uni_cdep_equivalent` in our development.