TUM

TECHNISCHE UNIVERSITÄT MÜNCHEN
INSTITUT FÜR INFORMATIK

Relational Abstract Interpretation for the Verification of 2-Hypersafety Properties (Proofs)

Máté Kovács

TUM-I1340

Relational Abstract Interpretation for the Verification of 2-Hypersafety Properties (Proofs)

Máté Kovács

This document contains the proofs of the theorems published in [1]. Therefore, this work should be seen as an extension of [1] and should be read together with it. In Section 1 we prove the theorems published in Section 2 of [1], and in Section 2 we prove the theorems published in Section 3 of [1]. The numbering of theorems in this document is consistent with that in [1].

1 Proofs for Section 2 in [1]

Theorem 1. *Consider a pair of sequences of labels $\pi_1, \pi_2 \in n_{in} \rightsquigarrow n_{fi}$ on the CFG $G = (N, E, n_{in}, n_{fi})$, and states $s_0, s, t_0, t \in S$, where $s = [\![\pi_1]\!]s_0$, $t = [\![\pi_2]\!]t_0$ and $(s_0, t_0) \in \gamma(d_0)$. In this case $d \sqsupseteq MTC(G, d_0)$ implies $(s, t) \in \gamma(d)$.*

Proof. Lemma 2 below entails that if $d' \sqsupseteq \bigsqcap_{\omega \in A(\pi_1,\pi_2)} [\![\omega]\!]^\sharp d_0$ then $(s, t) \in \gamma(d')$. Since $\pi_1, \pi_2 \in n_{in} \rightsquigarrow n_{fi}$, $\mathrm{MTC}(G, d_0) \sqsupseteq d'$ holds. □

Theorem 2. *Given the CFG $G = (N, E, n_{in}, n_{fi})$ and a self-composition of it $GG = (N', E', n'_{in}, n'_{fi})$, the following holds for all d_0:*

$$\bigsqcup_{\omega \in n'_{in} \rightsquigarrow n'_{fi}} [\![\omega]\!]^\sharp d_0 \sqsupseteq MTC(G, d_0)$$

Proof. According to Definition 3 in [1] for all $\pi_1, \pi_2 \in n_{in} \rightsquigarrow n_{fi}$ there is an $\omega_{\pi_1,\pi_2} \in n'_{in} \rightsquigarrow n'_{fi}$ so that $\omega_{\pi_1,\pi_2} \in A(\pi_1, \pi_2)$. Therefore:

$$\mathrm{MTC}(G, d_0) = \bigsqcup_{\substack{\pi_1 \in n_{in} \rightsquigarrow n_{fi} \\ \pi_2 \in n_{in} \rightsquigarrow n_{fi}}} \bigsqcap_{\omega \in A(\pi_1,\pi_2)} [\![\omega]\!]^\sharp d_0 \sqsubseteq$$
$$\bigsqcup_{\substack{\pi_1 \in n_{in} \rightsquigarrow n_{fi} \\ \pi_2 \in n_{in} \rightsquigarrow n_{fi}}} [\![\omega_{\pi_1,\pi_2}]\!]^\sharp d_0 \sqsubseteq \bigsqcup_{\omega_{\pi_1,\pi_2} \in n'_{in} \rightsquigarrow n'_{fi}} [\![\omega_{\pi_1,\pi_2}]\!]^\sharp d_0$$

□

Definition 4. *The partially ordered sets $(\mathbb{A}, \sqsubseteq_{\mathbb{A}})$ and $(\mathbb{B}, \sqsubseteq_{\mathbb{B}})$ together with the functions $\alpha : \mathbb{A} \to \mathbb{B}$ and $\gamma : \mathbb{B} \to \mathbb{A}$ form a Galois connection $(\mathbb{A}, \alpha, \gamma, \mathbb{B})$, if for all $a \in \mathbb{A}$ and $b \in \mathbb{B}$ the following holds:*

$$\alpha(a) \sqsubseteq_{\mathbb{B}} b \Leftrightarrow a \sqsubseteq_{\mathbb{A}} \gamma(b)$$

Lemma 1. *If $(\mathbb{A}, \alpha, \gamma, \mathbb{B})$ is a Galois connection then the following holds for any arbitrary set $B \subseteq \mathbb{B}$:*

$$a \sqsubseteq_{\mathbb{A}} \bigsqcap_{b \in B} \gamma(b) \Rightarrow a \sqsubseteq_{\mathbb{A}} \gamma\Big(\bigsqcap_{b \in B} b\Big)$$

Proof. From the precondition follows the following conjunction:

$$\bigwedge_{b \in B} \Big[a \sqsubseteq_{\mathbb{A}} \gamma(b)\Big]$$

The properties of Galois connections according to Definition 4 entail that:

$$\bigwedge_{b \in B} \Big[\alpha(a) \sqsubseteq_{\mathbb{B}} b\Big]$$

Therefore, we have that:

$$\alpha(a) \sqsubseteq_{\mathbb{B}} \bigsqcap_{b \in B} b$$

From the properties of Galois connections follows that:

$$a \sqsubseteq_{\mathbb{A}} \gamma\Big(\bigsqcap_{b \in B} b\Big)$$

□

Lemma 2. *Let us regard two computations: π_1 and π_2. From $[\![\pi_1]\!]s_0 = s$, $[\![\pi_2]\!]t_0 = t$, $(s_0, d_0) \in \gamma(d_0)$ and $d \sqsupseteq \bigsqcap_{\omega \in A(\pi_1, \pi_2)} [\![\omega]\!]^\sharp d_0$ follows that $(s, t) \in \gamma(d)$, given that $(\mathcal{P}(S \times S), \alpha, \gamma, \mathbb{D})$ forms a Galois connection.*

Proof. Let us regard a specific $\omega \in A(\pi_1, \pi_2)$, where $\omega = (f_1^\omega, g_1^\omega), ..., (f_{n_\omega}^\omega, g_{n_\omega}^\omega)$. Let $d_i^\omega = [\![f_i^\omega, g_i^\omega]\!]^\sharp d_{i-1}^\omega$ for all i , where $d_0^\omega = d_0$. Furthermore, let us suppose that $s_i = [\![f_1^\omega, ..., f_i^\omega]\!]s_0$ and $t_i = [\![g_1^\omega, ..., g_i^\omega]\!]t_0$. We prove inductively on the length of ω that $(s_i^\omega, t_i^\omega) \in \gamma(d_i^\omega)$ using (1) in [1]. The inductive assumption is that $(s_i^\omega, t_i^\omega) \in \gamma(d_i^\omega)$, which holds on d_0, s_0 and t_0, because of the assumptions of the lemma. Based on the abstract semantics of pairs of labels according to (1) in [1] we know now that $(s_{i+1}^\omega, t_{i+1}^\omega) \in \gamma([\![f_{i+1}^\omega, g_{i+1}^\omega]\!]^\sharp d_i^\omega)$.

We know that $[\![f_1^\omega ... f_{n_\omega}^\omega]\!] = [\![\pi_1]\!]$ and $[\![g_1^\omega ... g_{n_\omega}^\omega]\!] = [\![\pi_2]\!]$, because inserting `skip` operations in a sequence of instructions according to (2) in [1] does not alter the result of a computation. It follows then that $(s, t) = (s_n^\omega, t_n^\omega) \in \gamma([\![\omega]\!]^\sharp d_0)$. Therefore, for each $\omega \in A(\pi_1, \pi_2)$ we know that $(s, t) \in \gamma([\![\omega]\!]^\sharp d_0)$. It follows then that $(s, t) \in \bigcap_{\omega \in A(\pi_1, \pi_2)} \gamma([\![\omega]\!]^\sharp d_0)$. Otherwise put it we have $\{(s, t)\} \subseteq \bigcap_{\omega \in A(\pi_1, \pi_2)} \gamma([\![\omega]\!]^\sharp d_0)$. According to Lemma 1 we have $\{(s, t)\} \subseteq \gamma(\bigsqcap_{\omega \in A(\pi_1, \pi_2)} [\![\omega]\!]^\sharp d_0)$. From the properties of Galois connections according to Definition 4, it follows that $\alpha(\{(s, t)\}) \sqsubseteq \bigsqcap_{\omega \in A(\pi_1, \pi_2)} [\![\omega]\!]^\sharp d_0$. Accordingly, if $\bigsqcap_{\omega \in A(\pi_1, \pi_2)} [\![\omega]\!]^\sharp d_0 \sqsubseteq d$ then $\alpha(\{(s, t)\}) \sqsubseteq d$ too. Therefore, from properties of Galois connections follows that $\{(s, t)\} \subseteq \gamma(d)$. □

2 Proofs for Section 3 in [1]

Here we modify the notation of the original paper [1] to some extent. From now on, we denote pairs of labels f and g with $\begin{bmatrix} f \\ g \end{bmatrix}$ instead of (f, g). Furthermore, we use a grammar to generate the set of possible alignments of two sequences. We use here the notation $\Delta\begin{bmatrix} \pi_1 \\ \pi_2 \end{bmatrix}$ for a nonterminal generating the possible alignments of sequences π_1 and π_2 according to the rules below in (18). The set of all possible alignments that can be generated from nonterminal $\Delta\begin{bmatrix} \pi_1 \\ \pi_2 \end{bmatrix}$ using rules (18) is then denoted by $L(\Delta\begin{bmatrix} \pi_1 \\ \pi_2 \end{bmatrix})$. The grammar is as follows:

$$\begin{array}{lcl}
\Delta\begin{bmatrix} \varepsilon \\ \varepsilon \end{bmatrix} & \xrightarrow{1} & \varepsilon \\
\Delta\begin{bmatrix} \varepsilon \\ \varepsilon \end{bmatrix} & \xrightarrow{2} & \begin{bmatrix} \texttt{skip} \\ \texttt{skip} \end{bmatrix}\Delta\begin{bmatrix} \varepsilon \\ \varepsilon \end{bmatrix} \\
\Delta\begin{bmatrix} \varepsilon \\ g\pi \end{bmatrix} & \xrightarrow{3} & \begin{bmatrix} \texttt{skip} \\ g \end{bmatrix}\Delta\begin{bmatrix} \varepsilon \\ \pi \end{bmatrix} \\
\Delta\begin{bmatrix} \varepsilon \\ g\pi \end{bmatrix} & \xrightarrow{4} & \begin{bmatrix} \texttt{skip} \\ \texttt{skip} \end{bmatrix}\Delta\begin{bmatrix} \varepsilon \\ g\pi \end{bmatrix} \\
\Delta\begin{bmatrix} f\pi \\ \varepsilon \end{bmatrix} & \xrightarrow{5} & \begin{bmatrix} f \\ \texttt{skip} \end{bmatrix}\Delta\begin{bmatrix} \pi \\ \varepsilon \end{bmatrix} \\
\Delta\begin{bmatrix} f\pi \\ \varepsilon \end{bmatrix} & \xrightarrow{6} & \begin{bmatrix} \texttt{skip} \\ \texttt{skip} \end{bmatrix}\Delta\begin{bmatrix} f\pi \\ \varepsilon \end{bmatrix} \\
\Delta\begin{bmatrix} f\pi_1 \\ g\pi_2 \end{bmatrix} & \xrightarrow{7} & \begin{bmatrix} \texttt{skip} \\ g \end{bmatrix}\Delta\begin{bmatrix} f\pi_1 \\ \pi_2 \end{bmatrix} \\
\Delta\begin{bmatrix} f\pi_1 \\ g\pi_2 \end{bmatrix} & \xrightarrow{8} & \begin{bmatrix} f \\ \texttt{skip} \end{bmatrix}\Delta\begin{bmatrix} \pi_1 \\ g\pi_2 \end{bmatrix} \\
\Delta\begin{bmatrix} f\pi_1 \\ g\pi_2 \end{bmatrix} & \xrightarrow{9} & \begin{bmatrix} f \\ g \end{bmatrix}\Delta\begin{bmatrix} \pi_1 \\ \pi_2 \end{bmatrix} \\
\Delta\begin{bmatrix} f\pi_1 \\ g\pi_2 \end{bmatrix} & \xrightarrow{10} & \begin{bmatrix} \texttt{skip} \\ \texttt{skip} \end{bmatrix}\Delta\begin{bmatrix} f\pi_1 \\ g\pi_2 \end{bmatrix}
\end{array} \tag{18}$$

By comparing the rules of (18) with the rules of (2) in [1], we can see that there is a rule of the form $\Delta\begin{bmatrix} \pi_1 \\ \pi_2 \end{bmatrix} \xrightarrow{x} \begin{bmatrix} f \\ g \end{bmatrix}\Delta\begin{bmatrix} \pi_1' \\ \pi_2' \end{bmatrix}$ in (18), if and only if there is a corresponding member $\{\begin{bmatrix} f \\ g \end{bmatrix}\omega' \mid \omega' \in A(\pi_1', \pi_2')\}$ in the union of the equation defining $A(\pi_1, \pi_2)$ in (2) of [1]. In particular, for the rule $\Delta\begin{bmatrix} \varepsilon \\ \varepsilon \end{bmatrix} \xrightarrow{1} \varepsilon$ of (18) there is the corresponding equation $A(\varepsilon, \varepsilon) = \varepsilon \cup ...$ in (2) of [1]. Therefore, $\omega \in L(\Delta\begin{bmatrix} \pi_1 \\ \pi_2 \end{bmatrix})$ for an arbitrary ω, π_1 and π_2, if and only if $\omega \in A(\pi_1, \pi_2)$.

Theorem 3. *Consider a program p together with its CFG G constructed by the function $\mathsf{p2cfg}(p, n_{in}, n_{fi})$. In this case, the resulting CFG of the function $\mathsf{pp2cfg}(p, p, n_{in}', n_{fi}')$ is a self-composition of G according to Definition 3 in [1].*

Proof. The statement of the theorem directly follows from Lemma 7 below. □

Lemma 3. *The following holds for any pair of sequences of sequences $\pi_{1,1}...\pi_{1,n}$ and $\pi_{2,1}...\pi_{2,n}$:*

$$L\Big(\Delta\begin{bmatrix} \pi_{1,1}...\pi_{1,n} \\ \pi_{2,1}...\pi_{2,n} \end{bmatrix}\Big) \supseteq L\Big(\Delta\begin{bmatrix} \pi_{1,1} \\ \pi_{2,1} \end{bmatrix}...\Delta\begin{bmatrix} \pi_{1,n} \\ \pi_{2,n} \end{bmatrix}\Big)$$

Note, that any $\pi_{i,j}$ above may equal to ε, which is the empty sequence.

Proof. Let us denote the configurations of the derivation starting with the series of nonterminals $\Delta\begin{bmatrix}\pi_{1,1}\\ \pi_{2,1}\end{bmatrix}...\Delta\begin{bmatrix}\pi_{1,n}\\ \pi_{2,n}\end{bmatrix}$ using $\langle\omega_1\Delta\begin{bmatrix}\pi^k_{1,i}\\ \pi^l_{2,i}\end{bmatrix}...\Delta\begin{bmatrix}\pi_{1,n}\\ \pi_{1,n}\end{bmatrix}\rangle_1$, and similarly, denote the configurations of the derivation starting with $\Delta\begin{bmatrix}\pi_{1,1}...\pi_{1,n}\\ \pi_{2,1}...\pi_{2,n}\end{bmatrix}$ using $\langle\omega_2\Delta\begin{bmatrix}\pi^k_{1,i}...\pi_{1,n}\\ \pi^l_{2,i}...\pi_{2,n}\end{bmatrix}\rangle_2$, where ω_1 and ω_2 are the sequences of pairs that have been generated, and $\pi^k_{1,i}$ and $\pi^l_{2.i}$ are the postfixes of $\pi_{1,i}$ and $\pi_{2.i}$ where k and l indicate the length of the prefixes of $\pi_{1,i}$ and $\pi_{2.i}$ that have been processed already.

Now we prove inductively on the length of the derivations that whenever there is an κ and an ω such that

$$\langle\Delta\begin{bmatrix}\pi_{1,1}\\ \pi_{2,1}\end{bmatrix}...\Delta\begin{bmatrix}\pi_{1,n}\\ \pi_{1,n}\end{bmatrix}\rangle_1 \xrightarrow{\kappa}{}^{*} \langle\omega\Delta\begin{bmatrix}\pi^k_{1,i}\\ \pi^l_{2,i}\end{bmatrix}...\Delta\begin{bmatrix}\pi_{1,n}\\ \pi_{1,n}\end{bmatrix}\rangle_1,$$

then there is a χ such that

$$\langle\Delta\begin{bmatrix}\pi_{1,1}...\pi_{1,n}\\ \pi_{2,1}...\pi_{2,n}\end{bmatrix}\rangle_2 \xrightarrow{\chi}{}^{*} \langle\omega\Delta\begin{bmatrix}\pi^k_{1,i}...\pi_{1,n}\\ \pi^l_{2,i}...\pi_{2,n}\end{bmatrix}\rangle_2$$

holds. Above, $\kappa, \chi \in \{1, ..., 10\}^*$ denote sequences of numbers indicating the order of the application of the rules of the grammar in (18). The rules corresponding to κ are always applied to the left-most nonterminal of the configuration cfg_1. The inductive assumption is that the configurations of the two derivations are in relation $\mathit{cfg}_1 \sim \mathit{cfg}_2$. $\mathit{cfg}_1 \sim \mathit{cfg}_2$ holds if cfg_1 and cfg_2 are of the form:

$$\mathit{cfg}_1 = \langle\omega\Delta\begin{bmatrix}\pi^k_{1,i}\\ \pi^l_{2,i}\end{bmatrix}...\Delta\begin{bmatrix}\pi_{1,n}\\ \pi_{1,n}\end{bmatrix}\rangle_1 \sim \langle\omega\Delta\begin{bmatrix}\pi^k_{1,i}...\pi_{1,n}\\ \pi^l_{2,i}...\pi_{2,n}\end{bmatrix}\rangle_2 = \mathit{cfg}_2$$

In each step we apply one rule on

$$\mathit{cfg}_1 = \langle\omega\Delta\begin{bmatrix}\pi^k_{1,i}\\ \pi^l_{2,i}\end{bmatrix}...\Delta\begin{bmatrix}\pi_{1,n}\\ \pi_{1,n}\end{bmatrix}\rangle_1$$

and show what to do with

$$\mathit{cfg}_2 = \langle\omega\Delta\begin{bmatrix}\pi^k_{1,i}...\pi_{1,n}\\ \pi^l_{2,i}...\pi_{2,n}\end{bmatrix}\rangle_2$$

in order to preserve the inductive assumption. During the application of the rules on cfg_1, we always expand the leftmost nonterminal. In the initial case when $\omega = \varepsilon$ and no rules have been applied yet, the statement trivially holds.

Now we make a case distinction, based on the form of cfg_1.

1) $\pi^k_{1,i} \neq \varepsilon$ and $\pi^l_{2,i} \neq \varepsilon$. In this case we apply the same rule x on both of the configurations cfg_1 and cfg_2:

$$\begin{aligned}
\langle \omega \Delta \begin{bmatrix} \pi^k_{1,i} \\ \pi^l_{2,i} \end{bmatrix} ... \Delta \begin{bmatrix} \pi_{1,n} \\ \pi_{1,n} \end{bmatrix} \rangle_1 &\xrightarrow{x} \langle \omega \begin{bmatrix} f \\ g \end{bmatrix} \Delta \begin{bmatrix} \pi^{k'}_{1,i} \\ \pi^{l'}_{2,i} \end{bmatrix} ... \Delta \begin{bmatrix} \pi_{1,n} \\ \pi_{1,n} \end{bmatrix} \rangle_1 \\
\langle \omega \Delta \begin{bmatrix} \pi^k_{1,i} ... \pi_{1,n} \\ \pi^l_{2,i} ... \pi_{2,n} \end{bmatrix} \rangle_2 &\xrightarrow{x} \langle \omega \begin{bmatrix} f \\ g \end{bmatrix} \Delta \begin{bmatrix} \pi^{k'}_{1,i} ... \pi_{1,n} \\ \pi^{l'}_{2,i} ... \pi_{2,n} \end{bmatrix} \rangle_2
\end{aligned}$$

The inductive assumption holds on the resulting configurations.

2) $\pi^k_{1,i} = \varepsilon$ and $\pi^l_{2,i} \neq \varepsilon$, but $\pi^k_{1,i} ... \pi_{1,n} \neq \varepsilon$. If rule 3 is applied on cfg_1 then rule 7 is applied on cfg_2:

$$\begin{aligned}
\langle \omega \Delta \begin{bmatrix} \varepsilon \\ \pi^l_{2,i} \end{bmatrix} \Delta \begin{bmatrix} \pi^0_{1,i+1} \\ \pi^0_{2,i+1} \end{bmatrix} ... \Delta \begin{bmatrix} \pi_{1,n} \\ \pi_{1,n} \end{bmatrix} \rangle_1 &\xrightarrow{3} \\
\langle \omega \begin{bmatrix} \texttt{skip} \\ g \end{bmatrix} \Delta \begin{bmatrix} \varepsilon \\ \pi^{l+1}_{2,i} \end{bmatrix} \Delta \begin{bmatrix} \pi^0_{1,i+1} \\ \pi^0_{2,i+1} \end{bmatrix} ... \Delta \begin{bmatrix} \pi_{1,n} \\ \pi_{1,n} \end{bmatrix} \rangle_1 & \\
\langle \omega \Delta \begin{bmatrix} \pi^0_{1,i+1} ... \pi_{1,n} \\ \pi^l_{2,i} ... \pi_{2,n} \end{bmatrix} \rangle_2 &\xrightarrow{7} \langle \omega \begin{bmatrix} \texttt{skip} \\ g \end{bmatrix} \Delta \begin{bmatrix} \pi^0_{1,i+1} ... \pi_{1,n} \\ \pi^{l+1}_{2,i} ... \pi_{2,n} \end{bmatrix} \rangle_2
\end{aligned}$$

If rule 4 is applied on cfg_1, then rule 10 is applied on cfg_2:

$$\begin{aligned}
\langle \omega \Delta \begin{bmatrix} \varepsilon \\ \pi^l_{2,i} \end{bmatrix} \Delta \begin{bmatrix} \pi^0_{1,i+1} \\ \pi^0_{2,i+1} \end{bmatrix} ... \Delta \begin{bmatrix} \pi_{1,n} \\ \pi_{1,n} \end{bmatrix} \rangle_1 &\xrightarrow{4} \\
\langle \omega \begin{bmatrix} \texttt{skip} \\ \texttt{skip} \end{bmatrix} \Delta \begin{bmatrix} \varepsilon \\ \pi^l_{2,i} \end{bmatrix} \Delta \begin{bmatrix} \pi^0_{1,i+1} \\ \pi^0_{2,i+1} \end{bmatrix} ... \Delta \begin{bmatrix} \pi_{1,n} \\ \pi_{1,n} \end{bmatrix} \rangle_1 & \\
\langle \omega \Delta \begin{bmatrix} \pi^0_{1,i+1} ... \pi_{1,n} \\ \pi^l_{2,i} ... \pi_{2,n} \end{bmatrix} \rangle_2 &\xrightarrow{10} \langle \omega \begin{bmatrix} \texttt{skip} \\ \texttt{skip} \end{bmatrix} \Delta \begin{bmatrix} \pi^0_{1,i+1} ... \pi_{1,n} \\ \pi^l_{2,i} ... \pi_{2,n} \end{bmatrix} \rangle_2
\end{aligned}$$

The application of these rules preserve the inductive assumption, furthermore, no other rules can be applied on the left-most nonterminal in cfg_1.

2a) The case when $\pi^k_{1,i} \neq \varepsilon$ and $\pi^l_{2,i} = \varepsilon$, but $\pi^k_{2,i} ... \pi_{2,n} \neq \varepsilon$ can be proved analogously to case 2). If rule 5 is applied on cfg_1 then rule 8 is applied on cfg_2, and if rule 6 is applied on cfg_1 then rule 10 is applied on cfg_2. No other rules can be applied on the left-most nonterminal in cfg_1.

3) $\pi^k_{1,i} = \varepsilon$ and $\pi^l_{2,i} \neq \varepsilon$ and $\pi^k_{1,i} ... \pi_{1,n} = \varepsilon$. Either rule 3 can be applied on cfg_1, and we apply the same rule on cfg_2:

$$\begin{aligned}
\langle \omega \Delta \begin{bmatrix} \varepsilon \\ \pi^l_{2,i} \end{bmatrix} \Delta \begin{bmatrix} \varepsilon \\ \pi^0_{2,i+1} \end{bmatrix} ... \Delta \begin{bmatrix} \varepsilon \\ \pi_{1,n} \end{bmatrix} \rangle_1 &\xrightarrow{3} \\
\langle \omega \begin{bmatrix} \texttt{skip} \\ g \end{bmatrix} \Delta \begin{bmatrix} \varepsilon \\ \pi^{l+1}_{2,i} \end{bmatrix} \Delta \begin{bmatrix} \varepsilon \\ \pi^0_{2,i+1} \end{bmatrix} ... \Delta \begin{bmatrix} \varepsilon \\ \pi_{1,n} \end{bmatrix} \rangle_1 & \\
\langle \omega \Delta \begin{bmatrix} \varepsilon \\ \pi^l_{2,i} ... \pi_{2,n} \end{bmatrix} \rangle_2 &\xrightarrow{3} \langle \omega \begin{bmatrix} \texttt{skip} \\ g \end{bmatrix} \Delta \begin{bmatrix} \varepsilon \\ \pi^{l+1}_{2,i} ... \pi_{2,n} \end{bmatrix} \rangle_2
\end{aligned}$$

Or we can apply rule 4 on both of the configurations:

$$\begin{aligned}
\langle \omega \Delta \begin{bmatrix} \varepsilon \\ \pi^l_{2,i} \end{bmatrix} \Delta \begin{bmatrix} \varepsilon \\ \pi^0_{2,i+1} \end{bmatrix} ... \Delta \begin{bmatrix} \varepsilon \\ \pi_{1,n} \end{bmatrix} \rangle_1 &\xrightarrow{4} \\
\langle \omega \begin{bmatrix} \texttt{skip} \\ \texttt{skip} \end{bmatrix} \Delta \begin{bmatrix} \varepsilon \\ \pi^1_{2,i} \end{bmatrix} \Delta \begin{bmatrix} \varepsilon \\ \pi^0_{2,i+1} \end{bmatrix} ... \Delta \begin{bmatrix} \varepsilon \\ \pi_{1,n} \end{bmatrix} \rangle_1 & \\
\langle \omega \Delta \begin{bmatrix} \varepsilon \\ \pi^l_{2,i} ... \pi_{2,n} \end{bmatrix} \rangle_2 &\xrightarrow{4} \langle \omega \begin{bmatrix} \texttt{skip} \\ \texttt{skip} \end{bmatrix} \Delta \begin{bmatrix} \varepsilon \\ \pi^l_{2,i} ... \pi_{2,n} \end{bmatrix} \rangle_2
\end{aligned}$$

There are no other rules that can be applied on the left-most nonterminal of configuration cfg_1, furthermore, the inductive assumption has been preserved by the application of the above rules.

3a) The case when $\pi^k_{1,i} \neq \varepsilon$ and $\pi^l_{2,i} = \varepsilon$ and $\pi^k_{2,i}...\pi_{2,n} = \varepsilon$ can be proved similarly to the case 3). Either rule 5 or rule 6 is applied on the left-most nonterminal of both of the configurations, which preserves the inductive assumption.

4) $\pi^k_{1,i} = \varepsilon$, $\pi^l_{2,i} = \varepsilon$, $\pi^k_{1,i}...\pi_{1,n} = \varepsilon$, but $\pi^l_{2,i}...\pi_{2,n} \neq \varepsilon$. In this case one of the rules 1 and 2 may be applied on the left-most nonterminal of configuration cfg_1. If rule 1 is applied on cfg_1 then we do not apply anything on cfg_2:

$$\begin{array}{rcl}
\langle \omega \Delta \begin{bmatrix} \varepsilon \\ \varepsilon \end{bmatrix} \Delta \begin{bmatrix} \varepsilon \\ \pi^0_{2,i+1} \end{bmatrix} ... \Delta \begin{bmatrix} \varepsilon \\ \pi_{1,n} \end{bmatrix} \rangle_1 & \xrightarrow{1} & \langle \omega \Delta \begin{bmatrix} \varepsilon \\ \pi^0_{2,i+1} \end{bmatrix} ... \Delta \begin{bmatrix} \varepsilon \\ \pi_{1,n} \end{bmatrix} \rangle_1 \\
\langle \omega \Delta \begin{bmatrix} \varepsilon \\ \pi^0_{2,i+1} ... \pi_{2,n} \end{bmatrix} \rangle_2 & & \langle \omega \Delta \begin{bmatrix} \varepsilon \\ \pi^0_{2,i+1} ... \pi_{2,n} \end{bmatrix} \rangle_2
\end{array}$$

If rule 2 is applied on cfg_1 then rule 4 is applied on cfg_2:

$$\begin{array}{rcl}
\langle \omega \Delta \begin{bmatrix} \varepsilon \\ \varepsilon \end{bmatrix} \Delta \begin{bmatrix} \varepsilon \\ \pi^0_{2,i+1} \end{bmatrix} ... \Delta \begin{bmatrix} \varepsilon \\ \pi_{1,n} \end{bmatrix} \rangle_1 & \xrightarrow{2} & \langle \omega \begin{bmatrix} \texttt{skip} \\ \texttt{skip} \end{bmatrix} \Delta \begin{bmatrix} \varepsilon \\ \varepsilon \end{bmatrix} \Delta \begin{bmatrix} \varepsilon \\ \pi^0_{2,i+1} \end{bmatrix} ... \Delta \begin{bmatrix} \varepsilon \\ \pi_{1,n} \end{bmatrix} \rangle_1 \\
\langle \omega \Delta \begin{bmatrix} \varepsilon \\ \pi^0_{2,i+1} ... \pi_{2,n} \end{bmatrix} \rangle_2 & \xrightarrow{4} & \langle \omega \begin{bmatrix} \texttt{skip} \\ \texttt{skip} \end{bmatrix} \Delta \begin{bmatrix} \varepsilon \\ \pi^0_{2,i+1} ... \pi_{2,n} \end{bmatrix} \rangle_2
\end{array}$$

The application of these rules preserves the inductive assumption, furthermore, no other rules can be applied on the left-most nonterminal of cfg_1.

4a) The case when $\pi^k_{1,i} = \varepsilon$, $\pi^l_{2,i} = \varepsilon$, $\pi^k_{1,i}...\pi_{1,n} \neq \varepsilon$, but $\pi^l_{2,i}...\pi_{2,n} = \varepsilon$ can be proved similarly to case 4). Whenever rule 1 is applied on cfg_1 then cfg_2 is not modified. And whenever rule 2 is applied on cfg_1, then rule 6 is applied on cfg_2.

5) $\pi^k_{1,i} = \varepsilon$, $\pi^l_{2,i} = \varepsilon$, $\pi^k_{1,i}...\pi_{1,n} = \varepsilon$, and $\pi^l_{2,i}...\pi_{2,n} = \varepsilon$. In this case one of the rules 1 and 2 may be applied on the configuration cfg_1. If rule 2 is applied on cfg_1 then this rule is also applied on cfg_2:

$$\begin{array}{rcl}
\langle \omega \Delta \begin{bmatrix} \varepsilon \\ \varepsilon \end{bmatrix} \Delta \begin{bmatrix} \varepsilon \\ \varepsilon \end{bmatrix} ... \Delta \begin{bmatrix} \varepsilon \\ \varepsilon \end{bmatrix} \rangle_1 & \xrightarrow{2} & \langle \omega \begin{bmatrix} \texttt{skip} \\ \texttt{skip} \end{bmatrix} \Delta \begin{bmatrix} \varepsilon \\ \varepsilon \end{bmatrix} \Delta \begin{bmatrix} \varepsilon \\ \varepsilon \end{bmatrix} ... \Delta \begin{bmatrix} \varepsilon \\ \varepsilon \end{bmatrix} \rangle_1 \\
\langle \omega \Delta \begin{bmatrix} \varepsilon \\ \varepsilon \end{bmatrix} \rangle_2 & \xrightarrow{2} & \langle \omega \begin{bmatrix} \texttt{skip} \\ \texttt{skip} \end{bmatrix} \Delta \begin{bmatrix} \varepsilon \\ \varepsilon \end{bmatrix} \rangle_2
\end{array}$$

However, if rule 1 is applied on cfg_1 then this rule is only applied on cfg_2 if $cfg_1 = \langle \omega \Delta \begin{bmatrix} \varepsilon \\ \varepsilon \end{bmatrix} \rangle_1$:

$$\begin{array}{rcl}
\langle \omega \Delta \begin{bmatrix} \varepsilon \\ \varepsilon \end{bmatrix} \rangle_1 & \xrightarrow{1} & \langle \omega \rangle_1 \\
\langle \omega \Delta \begin{bmatrix} \varepsilon \\ \varepsilon \end{bmatrix} \rangle_2 & \xrightarrow{1} & \langle \omega \rangle_2
\end{array}$$

Otherwise no rule is applied on cfg_2:

$$\begin{array}{rcl}
\langle \omega \Delta \begin{bmatrix} \varepsilon \\ \varepsilon \end{bmatrix} \Delta \begin{bmatrix} \varepsilon \\ \varepsilon \end{bmatrix} ... \Delta \begin{bmatrix} \varepsilon \\ \varepsilon \end{bmatrix} \rangle_1 & \xrightarrow{1} & \langle \omega \Delta \begin{bmatrix} \varepsilon \\ \varepsilon \end{bmatrix} ... \Delta \begin{bmatrix} \varepsilon \\ \varepsilon \end{bmatrix} \rangle_1 \\
\langle \omega \Delta \begin{bmatrix} \varepsilon \\ \varepsilon \end{bmatrix} \rangle_2 & & \langle \omega \Delta \begin{bmatrix} \varepsilon \\ \varepsilon \end{bmatrix} \rangle_2
\end{array}$$

These rule applications preserve the inductive assumption. Furthermore, no other rules can be applied on the left-most nonterminal of cfg_1.

6) $\pi^k_{1,i} = \varepsilon$, $\pi^l_{2,i} = \varepsilon$, but $\pi^k_{1,i}...\pi_{1,n} \neq \varepsilon$ and $\pi^l_{2,i}...\pi_{2,n} \neq \varepsilon$. Now rules 1 and 2 can be applied on the left-most nonterminal of cfg_1. If rule 1 is applied, then we do not modify cfg_2:

$$\begin{array}{ccc} \langle\omega\Delta\begin{bmatrix}\varepsilon\\ \varepsilon\end{bmatrix}\Delta\begin{bmatrix}\pi^0_{1,i+1}\\ \pi^0_{2,i+1}\end{bmatrix}...\Delta\begin{bmatrix}\pi_{1,n}\\ \pi_{1,n}\end{bmatrix}\rangle_1 & \xrightarrow{1} & \langle\omega\Delta\begin{bmatrix}\pi^0_{1,i+1}\\ \pi^0_{2,i+1}\end{bmatrix}...\Delta\begin{bmatrix}\pi_{1,n}\\ \pi_{1,n}\end{bmatrix}\rangle_1 \\ \langle\omega\Delta\begin{bmatrix}\pi^0_{1,i+1}\cdots\pi_{1,n}\\ \pi^0_{2,i+1}\cdots\pi_{2,n}\end{bmatrix}\rangle_2 & & \langle\omega\Delta\begin{bmatrix}\pi^0_{1,i+1}\cdots\pi_{1,n}\\ \pi^0_{2,i+1}\cdots\pi_{2,n}\end{bmatrix}\rangle_2 \end{array}$$

If rule 2 is applied on cfg_1 then rule 10 is applied on cfg_2:

$$\begin{array}{ccc} \langle\omega\Delta\begin{bmatrix}\varepsilon\\ \varepsilon\end{bmatrix}\Delta\begin{bmatrix}\pi^0_{1,i+1}\\ \pi^0_{2,i+1}\end{bmatrix}...\Delta\begin{bmatrix}\pi_{1,n}\\ \pi_{1,n}\end{bmatrix}\rangle_1 & \xrightarrow{2} & \langle\omega\begin{bmatrix}\texttt{skip}\\ \texttt{skip}\end{bmatrix}\Delta\begin{bmatrix}\varepsilon\\ \varepsilon\end{bmatrix}\Delta\begin{bmatrix}\pi^0_{1,i+1}\\ \pi^0_{2,i+1}\end{bmatrix}...\Delta\begin{bmatrix}\pi_{1,n}\\ \pi_{1,n}\end{bmatrix}\rangle_1 \\ \langle\omega\Delta\begin{bmatrix}\pi^0_{1,i+1}\cdots\pi_{1,n}\\ \pi^0_{2,i+1}\cdots\pi_{2,n}\end{bmatrix}\rangle_2 & \xrightarrow{10} & \langle\omega\begin{bmatrix}\texttt{skip}\\ \texttt{skip}\end{bmatrix}\Delta\begin{bmatrix}\pi^{k'}_{1,i}\cdots\pi_{1,n}\\ \pi^{l'}_{2,i}\cdots\pi_{2,n}\end{bmatrix}\rangle_2 \end{array}$$

The application of these rules preserves the inductive assumption.

□

Lemma 4. *The following holds for all sequences π:*

$$\begin{array}{ccc} L\Big(\Delta\begin{bmatrix}\varepsilon\\ \pi\end{bmatrix}\Big) & \supseteq & L\Big(\Delta\begin{bmatrix}\mathit{skip}\\ \pi\end{bmatrix}\Big) \\ & \textit{and} & \\ L\Big(\Delta\begin{bmatrix}\pi\\ \varepsilon\end{bmatrix}\Big) & \supseteq & L\Big(\Delta\begin{bmatrix}\pi\\ \mathit{skip}\end{bmatrix}\Big) \end{array}$$

Proof. We prove now the first statement, the second can be proved analogously. We show that for all $\omega \in L\Big(\Delta\begin{bmatrix}\texttt{skip}\\ \pi\end{bmatrix}\Big)$, ω is an element of $L\Big(\Delta\begin{bmatrix}\varepsilon\\ \pi\end{bmatrix}\Big)$ too. We denote the configurations of the derivation of an arbitrary ω starting from $\Delta\begin{bmatrix}\texttt{skip}\\ \pi\end{bmatrix}$ with $\langle\omega^*\Delta\begin{bmatrix}\pi'_1\\ \pi'_2\end{bmatrix}\rangle_1$, where ω^* stands for a prefix of ω that has already been generated, and $\Delta\begin{bmatrix}\pi'_1\\ \pi'_2\end{bmatrix}$ is the nonterminal that has not been expanded yet. Similarly, tuples of the form $\langle\omega^*\Delta\begin{bmatrix}\pi'_1\\ \pi'_2\end{bmatrix}\rangle_2$ denote the configurations of the derivation starting from the nonterminal $\Delta\begin{bmatrix}\varepsilon\\ \pi\end{bmatrix}$.

The initial configurations of the derivations are $\langle\varepsilon\Delta\begin{bmatrix}\texttt{skip}\\ \pi\end{bmatrix}\rangle_1$ and $\langle\varepsilon\Delta\begin{bmatrix}\varepsilon\\ \pi\end{bmatrix}\rangle_2$ respectively. During the construction of $\omega \in L\Big(\Delta\begin{bmatrix}\texttt{skip}\\ \pi\end{bmatrix}\Big)$ there must be a step when the upper label of the nonterminal $\Delta\begin{bmatrix}\texttt{skip}\\ \pi\end{bmatrix}$, `skip`, is processed using one of the rules 5, 8 or 9. Therefore, we split ω into subsequences so that $\omega = \omega_1\begin{bmatrix}\texttt{skip}\\ g\end{bmatrix}\omega_2$. Accordingly, during the derivation of ω we need to have the following step:

$$\langle\omega_1\Delta\begin{bmatrix}\texttt{skip}\\ \pi'\end{bmatrix}\rangle_1 \rightarrow \langle\omega_1\begin{bmatrix}\texttt{skip}\\ g\end{bmatrix}\Delta\begin{bmatrix}\varepsilon\\ \pi''\end{bmatrix}\rangle_1$$

The following production rules in (18) are used for the generation of ω_1 by the two derivations:

$$\langle \varepsilon \Delta \begin{bmatrix} \texttt{skip} \\ \pi \end{bmatrix} \rangle_1 \xrightarrow{\kappa}{}^{*} \langle \omega_1 \Delta \begin{bmatrix} \texttt{skip} \\ \pi' \end{bmatrix} \rangle_1$$
$$\langle \varepsilon \Delta \begin{bmatrix} \varepsilon \\ \pi \end{bmatrix} \rangle_2 \xrightarrow{\chi}{}^{*} \langle \omega_1 \Delta \begin{bmatrix} \varepsilon \\ \pi' \end{bmatrix} \rangle_2$$

Above $\kappa, \chi \in \{1, ..., 10\}^*$ are strings identifying the sequences of production rules in (18) that have been used for the generation of ω_1, where we assume that always the left-most nonterminals are expanded in the configurations. Below we give a function $\eta : \{1, ..., 10\} \to \{1, ..., 10\}$ to construct χ from κ by applying η on the members of κ:

$$\eta(7) = 3$$
$$\eta(10) = 4$$

Other rules than 7 and 10 can not occur in κ without consuming the upper `skip` of the nonterminal $\Delta \begin{bmatrix} \texttt{skip} \\ \pi \end{bmatrix}$. Now we make a case distinction based on the rule, which is applied on $\langle \omega_1 \Delta \begin{bmatrix} \texttt{skip} \\ \pi' \end{bmatrix} \rangle_1$ after the prefix ω_1 has been generated:

- If $\pi' = \varepsilon$, then rule 5 can be applied:

  $$\langle \omega_1 \Delta \begin{bmatrix} \texttt{skip} \\ \pi' \end{bmatrix} \rangle_1 \xrightarrow{5} \langle \omega_1 \begin{bmatrix} \texttt{skip} \\ \texttt{skip} \end{bmatrix} \Delta \begin{bmatrix} \varepsilon \\ \varepsilon \end{bmatrix} \rangle_1$$

  In this case rule 2 must be applied on the other derivation:

  $$\langle \omega_1 \Delta \begin{bmatrix} \varepsilon \\ \pi' \end{bmatrix} \rangle_2 \xrightarrow{2} \langle \omega_1 \begin{bmatrix} \texttt{skip} \\ \texttt{skip} \end{bmatrix} \Delta \begin{bmatrix} \varepsilon \\ \varepsilon \end{bmatrix} \rangle_2$$

  After the steps above, rule 2 is applied on both of the configurations an equal number of times to construct ω_2 and then finally rule 1 is applied once.

- Rule 8 is applied:

  $$\langle \omega_1 \Delta \begin{bmatrix} \texttt{skip} \\ \pi' \end{bmatrix} \rangle_1 \xrightarrow{8} \langle \omega_1 \begin{bmatrix} \texttt{skip} \\ \texttt{skip} \end{bmatrix} \Delta \begin{bmatrix} \varepsilon \\ \pi' \end{bmatrix} \rangle_1$$

  Rule 4 is applied on the other derivation:

  $$\langle \omega_1 \Delta \begin{bmatrix} \varepsilon \\ \pi' \end{bmatrix} \rangle_2 \xrightarrow{4} \langle \omega_1 \begin{bmatrix} \texttt{skip} \\ \texttt{skip} \end{bmatrix} \Delta \begin{bmatrix} \varepsilon \\ \pi' \end{bmatrix} \rangle_2$$

  And then an identical sequence of production rules is applied on both of the configurations to produce ω_2.

- Rule 9 is applied:

  $$\langle \omega_1 \Delta \begin{bmatrix} \texttt{skip} \\ \pi' \end{bmatrix} \rangle_1 \xrightarrow{9} \langle \omega_1 \begin{bmatrix} \texttt{skip} \\ g \end{bmatrix} \Delta \begin{bmatrix} \varepsilon \\ \pi'' \end{bmatrix} \rangle_1$$

Here we suppose that $\pi' = g\pi''$. Furthermore, rule 3 is applied on the other derivation:

$$\langle \omega_1 \Delta \begin{bmatrix} \varepsilon \\ \pi' \end{bmatrix} \rangle_2 \xrightarrow{3} \langle \omega_1 \begin{bmatrix} \texttt{skip} \\ g \end{bmatrix} \Delta \begin{bmatrix} \varepsilon \\ \pi'' \end{bmatrix} \rangle$$

Now an identical sequence or production rules is applied on both of the configurations in order to produce ω_2.

□

Lemma 5. *We consider the two CFGs:*

$$G_c = \mathsf{c2cfg}(c, n^c_{in}, n^c_{fi}) \\ \textit{and} \\ G_d = \mathsf{c2cfg}(d, n^d_{in}, n^d_{fi})$$

and their compositions: $G_{c,d} = \mathsf{pc2cfg}(c, d, n_{in}, n_{fi})$. *The following holds:*

a) If c and d are not composable, then $G_{c,d} = \mathsf{pc2cfg}(c, d, n_{in}, n_{fi})$ satisfies the conditions of Definition 3 in [1] with respect to G_c and G_d without further conditions.

b) If $c = d = \texttt{skip}$ or $c = d = x\texttt{:=}e$, then $G_{c,d} = \mathsf{pc2cfg}(c, d, n_{in}, n_{fi})$ satisfies the conditions of Definition 3 in [1] with respect to G_c and G_d without further conditions.

c) We suppose that $G_{p_{\mathtt{tt}},r_{\mathtt{tt}}} = \mathsf{pp2cfg}(p_{\mathtt{tt}}, r_{\mathtt{tt}}, n^{\mathtt{tt},\mathtt{tt}}_{in}, n_{fi})$ is a composition of $G_{p_{\mathtt{tt}}} = \mathsf{p2cfg}(p_{\mathtt{tt}}, n^{\mathtt{tt},c}_{in}, n^c_{fi})$ and $G_{r_{\mathtt{tt}}} = \mathsf{p2cfg}(r_{\mathtt{tt}}, n^{\mathtt{tt},d}_{in}, n^d_{fi})$ according to Definition 3 in [1], $G_{p_{\mathtt{tt}},r_{ff}} = \mathsf{pp2cfg}(p_{\mathtt{tt}}, r_{ff}, n^{\mathtt{tt},ff}_{in}, n_{fi})$ is a composition of $G_{p_{\mathtt{tt}}} = \mathsf{p2cfg}(p_{\mathtt{tt}}, n^{\mathtt{tt},c}_{in}, n^c_{fi})$ and $G_{r_{ff}} = \mathsf{p2cfg}(r_{ff}, n^{ff,d}_{in}, n^d_{fi})$ according to Definition 3 in [1], $G_{ff,\mathtt{tt}} = \mathsf{pp2cfg}(p_{ff}, r_{\mathtt{tt}}, n^{ff,\mathtt{tt}}_{in}, n_{fi})$ is a composition of $G_{p_{ff}} = \mathsf{p2cfg}(p_{ff}, n^{ff,c}_{in}, n^c_{fi})$ and $G_{r_{\mathtt{tt}}} = \mathsf{p2cfg}(r_{\mathtt{tt}}, n^{\mathtt{tt},d}_{in}, n^d_{fi})$ according to Definition 3 in [1] and $G_{ff,ff} = \mathsf{pp2cfg}(p_{ff}, r_{ff}, n^{ff,ff}_{in}, n_{fi})$ is a composition of $G_{p_{ff}} = \mathsf{p2cfg}(p_{ff}, n^{ff,c}_{in}, n^c_{fi})$ and $G_{r_{ff}} = \mathsf{p2cfg}(r_{ff}, n^{ff,d}_{in}, n^d_{fi})$ according to Definition 3 in [1].

In this case, if $c = \texttt{if}\ b_1\ \texttt{then \{}p_{\mathtt{tt}}\texttt{\} else \{}p_{ff}\texttt{\}}$ and $d = \texttt{if}\ b_2\ \texttt{then \{}r_{\mathtt{tt}}\texttt{\} else \{}r_{ff}\texttt{\}}$ then $G_{c,d} = \mathsf{pc2cfg}(c, d, n_{in}, n_{fi})$ satisfies the conditions of Definition 3 in [1] with respect to $G_c = (c, n^c_{in}, n^c_{fi})$ and $G_d = (d, n^d_{in}, n^d_{fi})$.

d) We suppose that $G_{p,r} = \mathsf{pp2cfg}(p, r, n^{\mathtt{tt},\mathtt{tt}}_{in}, n_{in})$ is a composition of $G_p = \mathsf{p2cfg}(p, n^{\mathtt{tt},c}_{in}, n^c_{in})$ and $G_r = \mathsf{p2cfg}(r, n^{\mathtt{tt},d}_{in}, n^d_{in})$ according to Definition 3 in [1].

In this case if $c = \texttt{while}\ b_1\ \texttt{do \{}p\texttt{\}}$ and $d = \texttt{while}\ b_2\ \texttt{do \{}r\texttt{\}}$ then $G_{c,d} = \mathsf{pc2cfg}(c, d, n_{in}, n_{fi})$ satisfies the conditions of Definition 3 in [1] with respect to $G_c = \mathsf{c2cfg}(c, n^c_{in}, n^c_{fi})$ and $G_d = \mathsf{c2cfg}(d, n^d_{in}, n^d_{fi})$.

Proof. We assume that the nodes generated by the functions $\mathsf{c2cfg}$, $\mathsf{p2cfg}$, $\mathsf{pc2cfg}$ and $\mathsf{pp2cfg}$ are always fresh. Therefore, the generated subgraphs of the function calls are only connected by the initial and final nodes given in the arguments.

We prove according to the cases of the statement of the lemma.

a) In this case according to Section 3 in [1]:

$$\mathsf{pc2cfg}(c, d, n_{in}, n_{fi}) \quad = \quad \mathsf{skip2}(\mathrm{c2cfg}(c, n_{in}, n')) \cup \mathsf{skip1}(\mathrm{c2cfg}(d, n', n_{fi}))$$

According to the properties of the function $\mathsf{c2cfg}$ there is only one common node in $\mathsf{skip2}(\mathrm{c2cfg}(c, n_{in}, n'))$ and $\mathsf{skip1}(\mathrm{c2cfg}(d, n', n_{fi})$, which is n'. Let us consider an arbitrary path $\pi_c = f_1, ..., f_k$ of the graph $G_c = \mathsf{c2cfg}(c, n_{in}, n')$ from node n_{in} to n', and an arbitrary path $\pi_d = g_1, ..., g_l$ of the graph $G_d = \mathsf{c2cfg}(d, n', n_{fi})$ from n' to n_{fi}. According to the definition of the functions $\mathsf{skip1}$ and $\mathsf{skip2}$, then $\mathsf{skip2}(G_c)$ has a path $\pi'_c = \begin{bmatrix} f_1 \\ \texttt{skip} \end{bmatrix} ... \begin{bmatrix} f_k \\ \texttt{skip} \end{bmatrix}$ and $\mathsf{skip1}(G_d)$ has a path $\pi'_d = \begin{bmatrix} \texttt{skip} \\ g_1 \end{bmatrix} ... \begin{bmatrix} \texttt{skip} \\ g_l \end{bmatrix}$ with the same initial and final nodes as π_c and π_d. Since the final node of π'_c on the subgraph $\mathsf{skip2}(G_c)$ and the initial node of π'_d on the subgraph $\mathsf{skip1}(G_d)$ is n' in $G_{c,d}$, $\omega = \begin{bmatrix} f_1 \\ \texttt{skip} \end{bmatrix} ... \begin{bmatrix} f_k \\ \texttt{skip} \end{bmatrix} \begin{bmatrix} \texttt{skip} \\ g_1 \end{bmatrix} ... \begin{bmatrix} \texttt{skip} \\ g_l \end{bmatrix}$ is a path of $G_{c,d}$ from n_{in} to n_{fi}. Furthermore we know that:

$$\omega = \begin{bmatrix} f_1 \\ \texttt{skip} \end{bmatrix} ... \begin{bmatrix} f_k \\ \texttt{skip} \end{bmatrix} \begin{bmatrix} \texttt{skip} \\ g_1 \end{bmatrix} ... \begin{bmatrix} \texttt{skip} \\ g_l \end{bmatrix} \in L\Big(\Delta \begin{bmatrix} \pi_c \\ \pi_d \end{bmatrix}\Big)$$

Therefore, our statement is proved.

b) $c = x_1\texttt{:=}e_1$, $d = x_2\texttt{:=}e_2$ or $c = d = \texttt{skip}$. Now, $\mathsf{pc2cfg}(c, d, n_{in}, n_{fi}) = (n_{in}, \begin{bmatrix} c \\ d \end{bmatrix}, n_{fi})$, and this graph has only one path $\begin{bmatrix} c \\ d \end{bmatrix}$. $\mathsf{c2cfg}(c, n^c_{in}, n^c_{fi}) = (n^c_{in}, c, n^c_{fi})$ has the only path c and $\mathsf{c2cfg}(d, n^d_{in}, n^d_{fi}) = (n^d_{in}, d, n^d_{fi})$ has the only path d. Since $\begin{bmatrix} c \\ d \end{bmatrix} \in L\Big(\Delta \begin{bmatrix} c \\ d \end{bmatrix}\Big)$, our statement trivially holds.

c) Now we investigate the case when $c = \texttt{if } b_1 \texttt{ then \{}p_{\texttt{tt}}\texttt{\} else \{}p_{\texttt{ff}}\texttt{\}}$ and $d = \texttt{if } b_2 \texttt{ then \{}r_{\texttt{tt}}\texttt{\} else \{}r_{\texttt{ff}}\texttt{\}}$.

Let us suppose that the graph $G_c = \mathsf{c2cfg}(c, n^c_{in}, n^c_{fi})$ has a path $\pi_c = f_0, f_1, ..., f_k$ from node n^c_{in} to node n^c_{fi}, and similarly, the graph $G_d = \mathsf{c2cfg}(d, n^d_{in}, n^d_{fi})$ has a path $\pi_d = g_0, g_1, ..., g_l$ from node n^d_{in} to n^d_{fi}. According to the CFG corresponding to the $\texttt{if}$ construct generated by the function $\mathsf{c2cfg}$, each path of G_c begins with either a $f_0 = b_1$ or a $f_0 = \neg b_1$. Similarly, each path on G_d must start with either a $g_0 = b_2$ or a $g_0 = \neg b_2$. Therefore, we would need to examine four cases depending on the values of f_0 and g_0. We show the proof for the case when $f_0 = b_1$ and $g_0 = \neg b_2$, the other three cases can be shown analogously. In this case $\pi_{p_{\texttt{tt}}} = f_1, ..., f_k$ is a path on $G_{p_{\texttt{tt}}}$ from node $n^{\texttt{tt},c}_{in}$ to node n^c_{fi}, and $\pi_{r_{\texttt{ff}}} = g_1, ..., g_l$ is a path on $G_{r_{\texttt{ff}}}$ from node $n^{\texttt{ff},d}_{in}$ to node n^d_{fi}. According to the assumptions, there is an $\omega \in L\Big(\Delta \begin{bmatrix} f_1, ..., f_k \\ g_1, ..., g_l \end{bmatrix}\Big)$ on $G_{p_{\texttt{tt}}, r_{\texttt{ff}}}$ from node $n^{\texttt{tt},\texttt{ff}}_{in}$ to node n_{fi}.

Furthermore, $\begin{bmatrix} b_1 \\ \neg b_2 \end{bmatrix}\omega$ is a path on $G_{c,d}$ from node n_{in} to node n_{fi}. Since $\begin{bmatrix} b_1 \\ \neg b_2 \end{bmatrix}\omega \in L\Big(\Delta\begin{bmatrix} \pi_c \\ \pi_d \end{bmatrix}\Big)$ and it is a path on $G_{c,d} = \mathsf{pc2cfg}(c, d, n_{in}, n_{fi})$ generated by the function $\mathsf{pc2cfg}$, the statement is proved.

d) Now we consider the case when $c =$ `while` b_1 `do {`p`}` and $d =$ `while` b_2 `do {`r`}`.

Let us suppose that the graph $G_c = \mathsf{c2cfg}(c, n^c_{in}, n^c_{fi})$ has a path π_c from node n^c_{in} to node n^c_{fi}, and similarly, the graph $G_d = \mathsf{c2cfg}(d, n^d_{in}, n^d_{fi})$ has a path π_d from node n^d_{in} to node n^d_{fi}. In general π_c starts with i number of loops $b_1\pi^k_p$ on G_c from node n^c_{in} to n^c_{in} so that π^k_p is a path from $n^{\mathtt{tt},c}_{in}$ to n^c_{in} on G_p during loop number k, and π_d starts with j number of loops $b_2\pi^l_r$ on G_d from node n^d_{in} to n^d_{in} so that π^l_r is a path from $n^{\mathtt{tt},d}_{in}$ to n^d_{in} on G_r during the loop number l. We prove here the statement for the case when $i \leq j$. For the case when $i > j$ the statement can be proved analogously. Therefore, we split π_d into two parts. In the first part the body of d is executed i times, in the second yet another $j - i$ times. Accordingly, π_c and π_d look the following:

$$\begin{aligned} \pi_c &= \overbrace{b_1\pi^1_p b_1\pi^2_p ... \pi^i_p}^{\pi'_c} \neg b_1 \\ \pi_d &= \overbrace{b_2\pi^1_r b_2\pi^2_r ... \pi^i_r}^{\pi'_d}\, b_2\, \overbrace{\pi^{i+1}_r ... b_2\pi^j_r \neg b_2}^{\pi''_d} \end{aligned} \tag{19}$$

According to our assumption, for all pairs of paths π^ξ_p and π^ξ_r of G_p and G_r where $1 \leq \xi \leq i$ there is a path ω^ξ on $G_{p,r} = \mathsf{pp2cfg}(p, r, n^{\mathtt{tt},\mathtt{tt}}_{in}, n_{in})$ so that $\omega^\xi \in L\Big(\Delta\begin{bmatrix} \pi^\xi_p \\ \pi^\xi_r \end{bmatrix}\Big)$. Therefore, we have a path

$$\omega' = \begin{bmatrix} b_1 \\ b_2 \end{bmatrix}\omega^1 ... \begin{bmatrix} b_1 \\ b_2 \end{bmatrix}\omega^i$$

on $G_{c,d} = \mathsf{pc2cfg}(c, d, n_{in}, n_{fi})$ from node n_{in} to n_{in}. There are two cases now.

- If $i = j$ then $\pi_c = \pi'_c \neg b_1$ and $\pi_d = \pi'_d \neg b_2$. Now we have an ω on $G_{c,d}$:

  $$\omega = \omega'\begin{bmatrix} \neg b_1 \\ \neg b_2 \end{bmatrix} = \begin{bmatrix} b_1 \\ b_2 \end{bmatrix}\omega^1 ... \begin{bmatrix} b_1 \\ b_2 \end{bmatrix}\omega^i\begin{bmatrix} \neg b_1 \\ \neg b_2 \end{bmatrix}$$

  We know about ω the following:

  $$\omega \in L\Big(\begin{bmatrix} b_1 \\ b_2 \end{bmatrix}\Delta\begin{bmatrix} \pi^1_p \\ \pi^1_r \end{bmatrix} ... \begin{bmatrix} b_1 \\ b_2 \end{bmatrix}\Delta\begin{bmatrix} \pi^i_p \\ \pi^i_r \end{bmatrix}\begin{bmatrix} \neg b_1 \\ \neg b_2 \end{bmatrix}\Big)$$

  Because $\begin{bmatrix} f \\ g \end{bmatrix} \in L\Big(\Delta\begin{bmatrix} f \\ g \end{bmatrix}\Big)$, it follows that:

  $$\omega \in L\Big(\Delta\begin{bmatrix} b_1 \\ b_2 \end{bmatrix}\Delta\begin{bmatrix} \pi^1_p \\ \pi^1_r \end{bmatrix} ... \Delta\begin{bmatrix} b_1 \\ b_2 \end{bmatrix}\Delta\begin{bmatrix} \pi^i_p \\ \pi^i_r \end{bmatrix}\Delta\begin{bmatrix} \neg b_1 \\ \neg b_2 \end{bmatrix}\Big)$$

From Lemma 3 follows:

$$\omega \in L\Big(\Delta\begin{bmatrix} b_1\pi_p^1...b_1\pi_p^i\neg b_1 \\ b_2\pi_r^1...b_2\pi_r^i\neg b_2 \end{bmatrix}\Big) = L\Big(\Delta\begin{bmatrix} \pi_c \\ \pi_d \end{bmatrix}\Big)$$

Furthermore, because ω is a path from n_{in} to n_{fi} on $G_{c,d}$, the statement is proved.

- In this case $i < j$. According to the graph $G_{c,d}$ generated by the function $\mathsf{pc2cfg}$ and the definition of $\mathsf{skip1}(\mathsf{p2cfg}(r, n_{in}^{\mathtt{ff,tt}}, n''))$ there is a path ω'' beginning with $n_{in}^{\mathtt{ff,tt}}$ and ending with n_{fi} so that it trespasses the graph $G_{\mathtt{skip},2} = \mathsf{skip1}(\mathsf{p2cfg}(r, n_{in}^{\mathtt{ff,tt}}, n''))$ at least once. Now, it holds that $\omega'' \in L\Big(\Delta\begin{bmatrix} \varepsilon \\ \pi_d'' \end{bmatrix}\Big)$. Therefore, $\omega'\begin{bmatrix} \neg b_1 \\ b_2 \end{bmatrix}\omega''$ is a path on $G_{c,d}$ from n_{in} to n_{fi}. Furthermore, we know the following about $\omega = \omega'\begin{bmatrix} \neg b_1 \\ b_2 \end{bmatrix}\omega''$:

$$\omega = \omega'\begin{bmatrix} \neg b_1 \\ b_2 \end{bmatrix}\omega'' = \begin{bmatrix} b_1 \\ b_2 \end{bmatrix}\omega^1...\begin{bmatrix} b_1 \\ b_2 \end{bmatrix}\omega^i\begin{bmatrix} \neg b_1 \\ \neg b_2 \end{bmatrix}\omega''$$

Therefore:

$$\omega \in L\Big(\begin{bmatrix} b_1 \\ b_2 \end{bmatrix}\Delta\begin{bmatrix} \pi_p^1 \\ \pi_r^1 \end{bmatrix}...\begin{bmatrix} b_1 \\ b_2 \end{bmatrix}\Delta\begin{bmatrix} \pi_p^i \\ \pi_r^i \end{bmatrix}\begin{bmatrix} \neg b_1 \\ \neg b_2 \end{bmatrix}\Delta\begin{bmatrix} \varepsilon \\ \pi_d'' \end{bmatrix}\Big)$$

Because $\begin{bmatrix} f \\ g \end{bmatrix} \in L\Big(\Delta\begin{bmatrix} f \\ g \end{bmatrix}\Big)$, it follows now that:

$$\omega \in L\Big(\Delta\begin{bmatrix} b_1 \\ b_2 \end{bmatrix}\Delta\begin{bmatrix} \pi_p^1 \\ \pi_r^1 \end{bmatrix}...\Delta\begin{bmatrix} b_1 \\ b_2 \end{bmatrix}\Delta\begin{bmatrix} \pi_p^i \\ \pi_r^i \end{bmatrix}\Delta\begin{bmatrix} \neg b_1 \\ \neg b_2 \end{bmatrix}\Delta\begin{bmatrix} \varepsilon \\ \pi_d'' \end{bmatrix}\Big)$$

From Lemma 3 follows:

$$\omega \in L\Big(\Delta\begin{bmatrix} b_1\pi_p^1...b_1\pi_p^i\neg b_1 \\ b_2\pi_r^1...b_2\pi_r^i\neg b_2\pi_d'' \end{bmatrix}\Big) = L\Big(\Delta\begin{bmatrix} \pi_c \\ \pi_d \end{bmatrix}\Big)$$

Therefore, the statement is proved.

□

Lemma 6. *We suppose about an arbitrary set C that for all commands $c, d \in C \cup \{\textbf{\textit{skip}}\}$, $G_{c,d} = \mathsf{pc2cfg}(c, d, n_{in}^{c,d}, n_{fi}^{c,d})$ satisfies the conditions of Definition 3 in [1] with respect to the CFGs $G_c = \mathsf{c2cfg}(c, n_{in}^c, n_{fi}^c)$ and $G_d = \mathsf{c2cfg}(d, n_{in}^d, n_{fi}^d)$. In this case, if $p = c_1\,\mathtt{;}...\mathtt{;}c_k$ and $r = d_1\,\mathtt{;}...\mathtt{;}d_l$ are so that for each i and j, $c_i, d_j \in C \cup \{\textbf{\textit{skip}}\}$, then $G_{p,r} = \mathsf{pp2cfg}(p, r, n_{in}, n_{fi})$ satisfies the conditions of Definition 3 in [1] with respect to $G_p = \mathsf{p2cfg}(p, n_{in}^p, n_{fi}^p)$ and $G_r = \mathsf{p2cfg}(r, n_{in}^r, n_{fi}^r)$.*

Proof. We assume that the nodes generated by the functions $\mathsf{c2cfg}$, $\mathsf{p2cfg}$, $\mathsf{pc2cfg}$ and $\mathsf{pp2cfg}$ are always fresh. Therefore, the generated subgraphs of the function calls are only connected by the initial and final nodes given in the arguments.

Let us suppose that the function $\mathsf{pp2cfg}(p, r, n_{in}, n_{\mathit{fi}})$ computes the alignment of commands: $\Omega = \begin{bmatrix} c'_1 \\ d'_1 \end{bmatrix}, \ldots, \begin{bmatrix} c'_m \\ d'_m \end{bmatrix} \in L\Big(\Delta\begin{bmatrix} p \\ r \end{bmatrix}\Big) = L\Big(\Delta\begin{bmatrix} c_1\mathtt{;}\ldots\mathtt{;}c_k \\ d_1\mathtt{;}\ldots\mathtt{;}d_l \end{bmatrix}\Big)$. The result of the function $\mathsf{pp2cfg}(p, r, n_{in}, n_{\mathit{fi}})$ equals to the following:

$$\mathsf{pc2cfg}(c'_1, d'_1, n_{in}, n_1) \cup \mathsf{pc2cfg}(c'_2, d'_2, n_1, n_2) \cup \ldots \cup \mathsf{pc2cfg}(c'_m, d'_m, n_{m-1}, n_{\mathit{fi}})$$

Therefore, any path from n_{in} to n_{fi} in $G_{p,r}$ crosses the nodes n_{in}, n_1, ..., n_{fi}. Therefore, we can split any path $\omega_{p,r}$ on $G_{p,r}$ into subpaths $\omega_{c'_i,d'_i}$, each corresponding to the actual pair of commands $\begin{bmatrix} c'_i \\ d'_i \end{bmatrix}$.

Now we construct a path ω on $G_{p,r}$ from node n_{in} to node n_{fi} for any pair of paths π_p and π_r so that it fulfills the requirements of this lemma, where π_p is a path on G_p from node n^p_{in} to node n^p_{fi} and π_r is a path on G_r from node n^r_{in} to n^r_{fi}. We follow the choices made by the function $\mathsf{pp2cfg}(p, r, n_{in}, n_{\mathit{fi}})$ at the construction of the alignment of commands Ω, and we construct ω along these choices. We prove the statement inductively on the length of the prefix $\omega^{i,j}$ of ω which has already been constructed. Let us suppose that the prefix $\omega^{i,j}$ is already constructed so that it holds that $\omega^{i,j} \in L\Big(\Delta\begin{bmatrix} \pi^i_p \\ \pi^j_r \end{bmatrix}\Big)$ where $\pi_p = \pi^i_p \pi_{c_{i+1}} \pi^{i+2,k}_p$ and $\pi_r = \pi^j_r \pi_{d_{j+1}} \pi^{j+2,l}_r$, so that the path π^i_p is on the CFG of the program $c_1\mathtt{;}\ldots\mathtt{;}c_i$ and π^j_r is on the CFG of the program $d_1\mathtt{;}\ldots\mathtt{;}d_j$ from the corresponding initial to the corresponding final nodes. $\pi_{c_{i+1}}$ and $\pi_{d_{j+1}}$ are fragments of the path on G_p and G_r corresponding to the commands c_{i+1} and d_{j+1}. Therefore, $\pi_{c_{i+1}}$ is a path on $G_{c_{i+1}} = \mathsf{c2cfg}(c_{i+1}, n^{c_{i+1}}_{in}, n^{c_{i+1}}_{\mathit{fi}})$ from node $n^{c_{i+1}}_{in}$ to node $n^{c_{i+1}}_{\mathit{fi}}$, and $\pi_{d_{j+1}}$ is a path on $G_{d_{j+1}} = \mathsf{c2cfg}(d_{j+1}, n^{d_{j+1}}_{in}, n^{d_{j+1}}_{\mathit{fi}})$. $\pi^{i+2,k}$ stands for a path on the CFG of the program $c_{i+2}\mathtt{;}\ldots\mathtt{;}c_k$, and $\pi^{j+2,l}$ stands for a path on the CFG of the program $d_{j+2}\mathtt{;}\ldots\mathtt{;}d_l$.

Initially, $i = j = 0$, and $\omega^{0,0} = \pi^0_p = \pi^0_r = \varepsilon$. In the initial case the statement holds because $\varepsilon \in L\Big(\Delta\begin{bmatrix} \varepsilon \\ \varepsilon \end{bmatrix}\Big)$. In the next step of the construction of the alignment of commands Ω the following choices can be made:

- The next element of the alignment of commands Ω is $\begin{bmatrix} \mathtt{skip} \\ d_{j+1} \end{bmatrix}$. We suppose that this twin command is number o in the sequence of twin commands that have already been processed. According to the assumptions of the lemma there is a path $\omega_{\mathtt{skip},d_{j+1}}$ on $G_{\mathtt{skip},d_{j+1}} = \mathsf{pc2cfg}(\mathtt{skip}, d_{j+1}, n_o, n_{o+1})$ so that $\omega_{\mathtt{skip},d_{j+1}} \in L\Big(\Delta\begin{bmatrix} \pi_{\mathtt{skip}} \\ \pi_{d_{j+1}} \end{bmatrix}\Big)$, where $\pi_{\mathtt{skip}} = \mathtt{skip}$ is a path on the CFG $G_{\mathtt{skip}} = \mathsf{c2cfg}(\mathtt{skip}, n^*_{in}, n^*_{\mathit{fi}})$ and $\pi_{d_{j+1}}$ is a path on the CFG $G_{d_{j+1}} = \mathsf{c2cfg}(d_{j+1}, n^{**}_{in}, n^{**}_{\mathit{fi}})$. From Lemma 3 follows that:

  $$L\Big(\Delta\begin{bmatrix} \pi^i_p \\ \pi^j_r \pi_{d_{j+1}} \end{bmatrix}\Big) \supseteq L\Big(\Delta\begin{bmatrix} \pi^i_p \\ \pi^j_r \end{bmatrix}\Delta\begin{bmatrix} \varepsilon \\ \pi_{d_{j+1}} \end{bmatrix}\Big)$$

  From Lemma 4 follows that:

  $$L\Big(\Delta\begin{bmatrix} \pi^i_p \\ \pi^j_r \end{bmatrix}\Delta\begin{bmatrix} \varepsilon \\ \pi_{d_{j+1}} \end{bmatrix}\Big) \supseteq L\Big(\Delta\begin{bmatrix} \pi^i_p \\ \pi^j_r \end{bmatrix}\Delta\begin{bmatrix} \pi_{\mathtt{skip}} \\ \pi_{d_{j+1}} \end{bmatrix}\Big)$$

Therefore, $\omega_{p^i,r^i}\omega_{\texttt{skip},d_{j+1}} \in L\Big(\Delta\begin{bmatrix}\pi_p^i\\ \pi_r^j\end{bmatrix}\Delta\begin{bmatrix}\pi_{\texttt{skip}}\\ \pi_{d_{j+1}}\end{bmatrix}\Big)$ entails $\omega_{p^i,r^i}\omega_{\texttt{skip},d_{j+1}} \in L\Big(\Delta\begin{bmatrix}\pi_p^i\\ \pi_r^j\pi_{d_{j+1}}\end{bmatrix}\Big)$. The rest postfix of the path π_p that needs to be processed in the next step is $\pi_{c_{i+1}}\pi_p^{i+2,k}$, and the rest postfix of the path π_r that needs to be processed in the next step is $\pi_r^{j+2,l}$.

- If the next element of the alignment of commands Ω is $\begin{bmatrix}c_{j+1}\\ \texttt{skip}\end{bmatrix}$ then the statement of the lemma can be proved symmetrically to the case above.

- The next element of the alignment of commands Ω to be processed is $\begin{bmatrix}c_{i+1}\\ d_{j+1}\end{bmatrix}$. We suppose that this is number o in the sequence of twin commands that have already been processed. According to the assumptions of the lemma there is a path $\omega_{c_{i+1},d_{j+1}}$ on $G_{c_{i+1},d_{j+1}} = \mathsf{pc2cfg}(c_{i+1}, d_{j+1}, n_o, n_{o+1})$ from n_o to n_{o+1}, so that $\omega_{c_{i+1},d_{j+1}} \in L\Big(\Delta\begin{bmatrix}\pi_{c_{i+1}}\\ \pi_{d_{j+1}}\end{bmatrix}\Big)$, where $\pi_{c_{i+1}}$ is a path on the CFG $G_{c_{i+1}} = \mathsf{c2cfg}(c_{i+1}, n_{in}^*, n_{fi}^*)$ and $\pi_{d_{j+1}}$ is a path on the CFG $G_{d_{j+1}} = \mathsf{c2cfg}(d_{j+1}, n_{in}^{**}, n_{fi}^{**})$ from the corresponding initial nodes to the corresponding final nodes. Therefore, $\omega_{p^i,r^j}\omega_{c_{i+1},d_{j+1}} \in L\Big(\Delta\begin{bmatrix}p^i\\ r^j\end{bmatrix}\Delta\begin{bmatrix}c_{i+1}\\ d_{j+1}\end{bmatrix}\Big)$. According to Lemma 3:

$$\omega_{p^i,r^j}\omega_{c_{i+1},d_{j+1}} \in L\Big(\Delta\begin{bmatrix}p^i\\ r^j\end{bmatrix}\Delta\begin{bmatrix}c_{i+1}\\ d_{j+1}\end{bmatrix}\Big) \text{ entails}$$
$$\omega_{p^i,r^j}\omega_{c_{i+1},d_{j+1}} \in L\Big(\Delta\begin{bmatrix}p^i c_{i+1}\\ r^j d_{j+1}\end{bmatrix}\Big)$$

  Therefore, the statement of the lemma holds. The rest postfix of the path π_p that needs to be processed in the next step is $\pi_p^{i+2,k}$, and the rest postfix of the path π_r that needs to be processed in the next step is $\pi_r^{j+2,l}$.

□

Lemma 7. *Given two programs p, r, and the corresponding control flow graphs $G_p = \mathsf{p2cfg}(p, n_{in}^p, n_{fi}^p)$ and $G_r = \mathsf{p2cfg}(r, n_{in}^r, n_{fi}^r)$, their composition $G_{p,r}$ constructed by the call $\mathsf{pp2cfg}(p, r, n_{in}, n_{fi})$ satisfies the conditions of Definition 3 in [1].*

Proof. We prove the statement inductively on the maximal number of commands embedded into each other on the root-leaf paths of the abstract syntax trees corresponding to the subprograms of p and r. We collect the subprograms of p and r having m commands on their root-leaf paths at the maximum into the set P_m.

The initial case. In the initial case, the members $p', r' \in P_1$ are programs having 1 command on any root-leaf path of the abstract syntax trees. Therefore, each member of P_1 is a sequence of commands of the form `skip` and x`:=`e. According to Lemma 5 for pairs of commands c and d of this form it always holds that $G_{c,d} = \mathsf{pc2cfg}(c, d, n^*_{in}, n^*_{fi})$ satisfies the conditions of Definition 3 in [1] with respect to $G_c = \mathsf{c2cfg}(c, n^c_{in}, n^c_{fi})$ and $G_d = \mathsf{c2cfg}(d, n^d_{in}, n^d_{fi})$. According to Lemma 6, $G_{p',r'} = \mathsf{pp2cfg}(p', r', n_{in}, n_{fi})$ then satisfies the conditions of Definition 3 in [1] with respect to $G_{p'} = \mathsf{p2cfg}(p', n^{p'}_{in}, n^{p'}_{fi})$ and $G_{r'} = \mathsf{p2cfg}(r', n^{r'}_{in}, n^{r'}_{fi})$.

The inductive case. We suppose now that the members of the set P_m are programs having at most m commands on any root-leaf path of the corresponding abstract syntax trees. We suppose that for each pair $p', r' \in P_m$ it holds that $G_{p',r'} = \mathsf{pp2cfg}(p', r', n_{in}, n_{fi})$ satisfies the conditions of Definition 3 in [1] with respect to $G_{p'} = \mathsf{p2cfg}(p', n^{p'}_{in}, n^{p'}_{fi})$ and $G_{r'} = \mathsf{p2cfg}(r', n^{r'}_{in}, n^{r'}_{fi})$. In this case according to Lemma 5 for each pair of commands c and d that are composed of the members of P_m, $G_{c,d} = \mathsf{pc2cfg}(c, d, n_{in}, n_{fi})$ satisfies the conditions of Definition 3 in [1] with respect to $G_c = \mathsf{c2cfg}(c, n^c_{in}, n^c_{fi})$ and $G_d = \mathsf{c2cfg}(d, n^d_{in}, n^d_{fi})$. Let us call the set of these commands C_{m+1}. Let us denote the set of programs composed from the set of commands in C_{m+1} by P_{m+1}. According to Lemma 6, for all pairs of programs $p'', r'' \in P_{m+1}$, $G_{p'',r''} = \mathsf{pp2cfg}(p'', r'', n_{in}, n_{fi})$ satisfies the conditions of Definition 3 in [1] with respect to $G_{p''} = \mathsf{p2cfg}(p'', n^{p''}_{in}, n^{p''}_{fi})$ and $G_{r''} = \mathsf{p2cfg}(r'', n^{r''}_{in}, n^{r''}_{fi})$. Therefore, the statement of this lemma holds on each pair of programs that are members of P_{m+1}.

□

References

[1] Máté Kovács, Helmut Seidl, and Bernd Finkbeiner. Relational abstract interpretation for the verification of 2-hypersafety properties. In *Proceedings of the 2013 ACM Conference on Computer and Communications Security*, CCS '13. ACM, 2013.