Theorem 2.21
If $live \models \mathsf{LV}^{\subseteq}(S)$ (with S being label consistent) then:

(i) if $\langle S, \sigma_1 \rangle \to \langle S', \sigma_1' \rangle$ and $\sigma_1 \sim_{N(init(S))} \sigma_2$ then there exists σ_2' such that $\langle S, \sigma_2 \rangle \to \langle S', \sigma_2' \rangle$ and $\sigma_1' \sim_{N(init(S'))} \sigma_2'$, and

(ii) if $\langle S, \sigma_1 \rangle \to \sigma_1'$ and $\sigma_1 \sim_{N(init(S))} \sigma_2$ then there exists σ_2' such that $\langle S, \sigma_2 \rangle \to \sigma_2'$ and $\sigma_1' \sim_{X(init(S))} \sigma_2'$

Proof The proof is by induction on the shape of the inference tree used to establish $\langle S, \sigma_1 \rangle \to \langle S', \sigma_1' \rangle$ and $\langle S, \sigma_1 \rangle \to \sigma_1'$, respectively.

The case [*ass*]. Then $\langle [x := a]^\ell, \sigma_1 \rangle \to \sigma_1[x \mapsto \mathcal{A}[\![a]\!]\sigma_1]$ and from the specification of the constraint system we have

$$N(\ell) = live_{entry}(\ell) \supseteq (live_{exit}(\ell) \backslash \{x\}) \cup FV(a) = (X(\ell) \backslash \{x\}) \cup FV(a)$$

and thus

$$\sigma_1 \sim_{N(\ell)} \sigma_2 \text{ implies } \mathcal{A}[\![a]\!]\sigma_1 = \mathcal{A}[\![a]\!]\sigma_2$$

because the value of a is only affected by the variables occurring in it. Therefore, taking

$$\sigma_2' = \sigma_2[x \mapsto \mathcal{A}[\![a]\!]\sigma_2]$$

we have that $\sigma_1'(x) = \sigma_2'(x)$ and thus $\sigma_1' \sim_{X(\ell)} \sigma_2'$ as required.

The case [*skip*]. Then $\langle [\texttt{skip}]^\ell, \sigma_1 \rangle \to \sigma_1$ and from the specification of the constraint system

$$N(\ell) = live_{entry}(\ell) \supseteq (live_{exit}(\ell) \backslash \emptyset) \cup \emptyset = live_{exit}(\ell) = X(\ell)$$

and we take σ_2' to be σ_2.

The case [seq_1]. Then $\langle S_1; S_2, \sigma_1 \rangle \to \langle S_1'; S_2, \sigma_1' \rangle$ because $\langle S_1, \sigma_1 \rangle \to \langle S_1', \sigma_1' \rangle$. By construction we have $flow(S_1; S_2) \supseteq flow(S_1)$ and also $blocks(S_1; S_2) \supseteq blocks(S_1)$. Thus by Lemma 2.16, *live* is a solution to $LV^{\subseteq}(S_1)$ and thus by the induction hypothesis there exists σ_2' such that

$$\langle S_1, \sigma_2 \rangle \to \langle S_1', \sigma_2' \rangle \text{ and } \sigma_1' \sim_{N(init(S_1'))} \sigma_2'$$

and the result follows.

The case $[seq_2]$. Then $\langle S_1; S_2, \sigma_1\rangle \to \langle S_2, \sigma_1'\rangle$ because $\langle S_1, \sigma_1\rangle \to \sigma_1'$. Once again by Lemma 2.16, *live* is a solution to $LV^{\subseteq}(S_1)$ and thus by the induction hypothesis there exists σ_2' such that:

$$\langle S_1, \sigma_2\rangle \to \sigma_2' \text{ and } \sigma_1' \sim_{X(init(S_1))} \sigma_2'$$

Now

$$\{(\ell, init(S_2)) \mid \ell \in final(S_1)\} \subseteq flow(S_1; S_2)$$

and by Lemma 2.14, $final(S_1) = \{init(S_1)\}$. Thus by Lemma 2.20

$$\sigma_1' \sim_{N(init(S_2))} \sigma_2'$$

and the result follows.

The case $[if_1]$. Then $\langle \texttt{if } [b]^\ell \texttt{ then } S_1 \texttt{ else } S_2, \sigma_1\rangle \to \langle S_1, \sigma_1\rangle$ because $\mathcal{B}[\![b]\!]\sigma_1 = true$. Since $\sigma_1 \sim_{N(\ell)} \sigma_2$ and $N(\ell) = live_{entry}(\ell) \supseteq FV(b)$, we also have that $\mathcal{B}[\![b]\!]\sigma_2 = true$ (the value of b is only affected by the variables occurring in it) and thus:

$$\langle \texttt{if } [b]^\ell \texttt{ then } S_1 \texttt{ else } S_2, \sigma_2\rangle \to \langle S_1, \sigma_2\rangle$$

From the specification of the constraint system, $N(\ell) = live_{entry}(\ell) \supseteq live_{exit}(\ell) = X(\ell)$ and hence $\sigma_1 \sim_{X(\ell)} \sigma_2$. Since $(\ell, init(S_1)) \in flow(S)$, Lemma 2.20 gives $\sigma_1 \sim_{N(init(S_1))} \sigma_2$ as required.

The case $[if_2]$ is similar to the previous case.

The case $[wh_1]$. Then $\langle \texttt{while } [b]^\ell \texttt{ do } S, \sigma_1\rangle \to \langle S; \texttt{while } [b]^\ell \texttt{ do } S, \sigma_1\rangle$ because $\mathcal{B}[\![b]\!]\sigma_1 = true$. Since $\sigma_1 \sim_{N(\ell)} \sigma_2$ and $N(\ell) \supseteq FV(b)$, we also have that $\mathcal{B}[\![b]\!]\sigma_2 = true$ and thus

$$\langle \texttt{while } [b]^\ell \texttt{ do } S, \sigma_2\rangle \to \langle S; \texttt{while } [b]^\ell \texttt{ do } S, \sigma_2\rangle$$

and again, since $N(\ell) = live_{entry}(\ell) \supseteq live_{exit}(\ell) = X(\ell)$ we have $\sigma_1 \sim_{X(\ell)} \sigma_2$ and then

$$\sigma_1 \sim_{N(init(S))} \sigma_2$$

follows from Lemma 2.20 because $(\ell, init(S)) \in flow(\texttt{while } [b]^\ell \texttt{ do } S)$.

The case $[wh_2]$. Then $\langle \texttt{while } [b]^\ell \texttt{ do } S, \sigma_1\rangle \to \sigma_1$ because $\mathcal{B}[\![b]\!]\sigma_1 = false$. Since $\sigma_1 \sim_{N(\ell)} \sigma_2$ and $N(\ell) \supseteq FV(b)$, we also have that $\mathcal{B}[\![b]\!]\sigma_2 = false$ and thus:

$$\langle \texttt{while } [b]^\ell \texttt{ do } S, \sigma_2\rangle \to \sigma_2$$

From the specification of $\mathsf{LV}^{\subseteq}(S)$, we have $N(\ell) = live_{entry}(\ell) \supseteq live_{exit}(\ell) = X(\ell)$ and thus $\sigma_1 \sim_{X(\ell)} \sigma_2$.

This completes the proof. ∎

MOP versus MFP solutions. We shall shortly prove that the MFP solution safely approximates the MOP solution (informally, MFP $\sqsupseteq$ MOP). In the case of a $(\bigcap, \rightarrow, \uparrow)$ or $(\bigcap, \leftarrow, \uparrow)$ analysis, the MFP solution is a subset of the MOP solution ($\sqsupseteq$ is $\subseteq$); in the case of a $(\bigcup, \rightarrow, \downarrow)$ or $(\bigcup, \leftarrow, \downarrow)$ analysis, the MFP solution is a superset of the MOP solution. We can also show that, in the case of Distributive Frameworks, the MOP and MFP solutions coincide.

Lemma 2.32 Consider the MFP and MOP solutions to an instance $(L, \mathcal{F}, F, B, \iota, f_\cdot)$ of a Monotone Framework; then:

$$MFP_\circ \sqsupseteq MOP_\circ \text{ and } MFP_\bullet \sqsupseteq MOP_\bullet$$

If the framework is distributive and if $path_\circ(\ell) \neq \emptyset$ for all ℓ in E and F then:

$$MFP_\circ = MOP_\circ \text{ and } MFP_\bullet = MOP_\bullet$$

■

Proof It is straightforward to show that:

$$\forall \ell : MOP_\bullet(\ell) \sqsubseteq f_\ell(MOP_\circ(\ell))$$
$$\forall \ell : MFP_\bullet(\ell) = f_\ell(MFP_\circ(\ell))$$

For the first part of the lemma it therefore suffices to prove that:

$$\forall \ell : MOP_\circ(\ell) \sqsubseteq MFP_\circ(\ell)$$

Note that $MFP_\circ$ is the least fixed point of the functional F defined by:

$$F(A_\circ)(\ell) = (\bigsqcup\{f_{\ell'}(A_\circ(\ell')) \mid (\ell', \ell) \in F\}) \sqcup \iota_E^\ell$$

Next let us restrict the length of the paths used to compute $MOP_\circ$; for $n \geq 0$ define:

$$MOP_\circ^n(\ell) = \bigsqcup\{f_{\vec{\ell}}(\iota) \mid \vec{\ell} \in path_\circ(\ell), |\vec{\ell}| < n\}$$

Clearly, $MOP_\circ(\ell) = \bigsqcup_n MOP_\circ^n(\ell)$ and to prove $MFP_\circ \sqsupseteq MOP_\circ$ is therefore suffices to prove

$$\forall n : MFP_\circ \sqsupseteq MOP_\circ^n$$

and we do so by numerical induction. The basis, $MFP_\circ \sqsupseteq MOP_\circ^0$, is trivial. The inductive step proceeds as follows:

$$MFP_\circ(\ell) \quad = \quad F(MFP_\circ)(\ell)$$

$$\begin{aligned}
&= (\bigsqcup\{f_{\ell'}(MFP_\circ(\ell')) \mid (\ell',\ell) \in F\}) \sqcup \iota_E^\ell \\
&\sqsupseteq (\bigsqcup\{f_{\ell'}(MOP_\circ^n(\ell')) \mid (\ell',\ell) \in F\}) \sqcup \iota_E^\ell \\
&= (\bigsqcup\{f_{\ell'}(\bigsqcup\{f_{\vec{\ell}}(\iota) \mid \vec{\ell} \in path_\circ(\ell'), |\vec{\ell}| < n\}) \mid (\ell',\ell) \in F\}) \sqcup \iota_E^\ell \\
&\sqsupseteq (\bigsqcup(\{\bigsqcup\{f_{\ell'}(f_{\vec{\ell}}(\iota)) \mid \vec{\ell} \in path_\circ(\ell'), |\vec{\ell}| < n\} \mid (\ell',\ell) \in F\}) \sqcup \iota_E^\ell \\
&= \bigsqcup(\{f_{\vec{\ell}}(\iota) \mid \vec{\ell} \in path_\circ(\ell), 1 \le |\vec{\ell}| \le n\}) \sqcup \iota_E^\ell \\
&= MOP_\circ^{n+1}(\ell)
\end{aligned}$$

where we have used the induction hypothesis to get the first inequality. This completes the proof of $MFP_\circ \sqsupseteq MOP_\circ$ and $MFP_\bullet \sqsupseteq MOP_\bullet$.

To prove the second part of the lemma we now assume that the framework is distributive. Consider ℓ in E or F. By assumption f_ℓ is distributive, that is $f_\ell(l_1 \sqcup l_2) = f_\ell(l_1) \sqcup f_\ell(l_2)$, and from Lemma A.9 of Appendix A it follows that

$$f_\ell(\bigsqcup Y) = \bigsqcup\{f_\ell(l) \mid l \in Y\}$$

whenever Y is non-empty. By assumption we also have $path_\circ(\ell) \neq \emptyset$ and it follows that

$$\begin{aligned}
f_\ell(\bigsqcup\{f_{\vec{\ell}}(\iota) \mid \vec{\ell} \in path_\circ(\ell)\}) &= \bigsqcup\{f_\ell(f_{\vec{\ell}}(\iota)) \mid \vec{\ell} \in path_\circ(\ell)\} \\
&= \bigsqcup\{f_{\vec{\ell}}(\iota) \mid \vec{\ell} \in path_\bullet(\ell)\}
\end{aligned}$$

and this shows that:

$$\forall \ell : f_\ell(MOP_\circ(\ell)) = MOP_\bullet(\ell)$$

Next we calculate:

$$\begin{aligned}
MOP_\circ(\ell) &= \bigsqcup\{f_{\vec{\ell}}(\iota) \mid \vec{\ell} \in path_\circ(\ell)\} \\
&= \bigsqcup\{f_{\vec{\ell}}(\iota) \mid \vec{\ell} \in \bigcup\{path_\bullet(\ell') \mid (\ell',\ell) \in F\} \cup \{[\,] \mid \ell \in E\}\} \\
&= \bigsqcup(\{f_{\ell'}(f_{\vec{\ell}}(\iota)) \mid \vec{\ell} \in path_\circ(\ell'), (\ell',\ell) \in F\} \cup \{\iota \mid \ell \in E\}) \\
&= (\bigsqcup\{f_{\ell'}(\bigsqcup\{f_{\vec{\ell}}(\iota) \mid \vec{\ell} \in path_\circ(\ell')\} \mid (\ell',\ell) \in F\}) \sqcup \iota_E^\ell \\
&= (\bigsqcup\{f_{\ell'}(MOP_\circ(\ell')) \mid (\ell',\ell) \in F\}) \sqcup \iota_E^\ell
\end{aligned}$$

Together this shows that ($MOP_\circ$, $MOP_\bullet$) is a solution to the data flow equations. Using Proposition A.10 of Appendix A and the fact that ($MFP_\circ$, $MFP_\bullet$) is the least solution we get $MOP_\circ \sqsupseteq MFP_\circ$ and $MOP_\bullet \sqsupseteq MFP_\bullet$. Together with the results of the first part of the lemma we get $MOP_\circ = MFP_\circ$ and $MOP_\bullet = MFP_\bullet$. ∎