Instruction Graph Proofs

Andrew Benson

1 cfgvalid

cfg `cfgvalid` means that the configuration *cfg* is a valid configuration.

$$\frac{\mathbf{P}(v,\ vs)\ \texttt{valid} \qquad \mathbf{V}(n,\ c) \in v :: vs}{(n,\ v :: vs,\ I,\ O)\ \texttt{cfgvalid}}(\texttt{cfg}_{\texttt{cfgvalid}})$$

2 Progress

Theorem 1. *If cfg* `cfgvalid`*, then either*

1. *cfg* `terminated`
2. *cfg* `waiting`
3. $\exists\ cfg'\ \texttt{s.t.} cfg \longmapsto cfg'$

2.1 Proof of Progress

We proceed by case analysis on the judgment *cfg* `cfgvalid`. There is only one rule that concludes *cfg* `cfgvalid`:

$$\frac{\mathbf{P}(v,\ vs)\ \texttt{valid} \qquad \mathbf{V}(n,\ c) \in v :: vs}{(n,\ v :: vs,\ I,\ O)\ \texttt{cfgvalid}}$$

So we know *cfg* is of the form $(n,\ v :: vs,\ I,\ O)$ and $\mathbf{V}(n,\ c) \in v :: vs$. We continue by structural induction on c, which is of the sort `Content`.

Case c is **do** a **then** n':

Then by the rule

$$\frac{\mathbf{V}(n,\ \textbf{do}\ a\ \textbf{then}\ n') \in vs}{(n,\ vs,\ I,\ O) \longmapsto (n',\ vs,\ I,\ a :: O)}$$

we can conclude $(n,\ v :: vs,\ I,\ O) \longmapsto (n',\ v :: vs,\ I,\ a :: O)$.

Case c is **do** a **until** cnd **then** n':

We use structural induction on I.

Subcase I is $[\,]$:

Then by the rule

$$\frac{\mathbf{V}(n,\ \textbf{do}\ a\ \textbf{until}\ cnd\ \textbf{then}\ n') \in vs}{(n,\ vs,\ [\,],\ O)\ \texttt{waiting}}$$

we can conclude $(n,\ v :: vs,\ I,\ O)$ `waiting`.

Subcase I is $true :: I'$:

Then by the rule

$$\frac{\mathbf{V}(n,\ \textbf{do}\ a\ \textbf{until}\ cnd\ \textbf{then}\ n') \in vs}{(n,\ vs,\ true :: I,\ O) \longmapsto (n',\ vs,\ I,\ a :: O)}$$

we can conclude $(n,\ v :: vs,\ I,\ O) \longmapsto (n',\ v :: vs,\ I',\ a :: O)$.

Subcase I is $false :: I'$:

Then by the rule

$$\frac{\mathbf{V}(n,\ \mathbf{do}\ a\ \mathbf{until}\ cnd\ \mathbf{then}\ n') \in vs}{(n,\ vs,\ \mathit{false} :: I,\ O) \longmapsto (n,\ vs,\ I,\ a :: O)}$$

we can conclude $(n,\ v :: vs,\ I,\ O) \longmapsto (n,\ v :: vs,\ I',\ a :: O)$.

Case c is **if** cnd **then** n' **else** n'':

We use structural induction on I.

Subcase I is $[\,]$:

Then by the rule

$$\frac{\mathbf{V}(n,\ \mathbf{if}\ cnd\ \mathbf{then}\ n'\ \mathbf{else}\ n'') \in vs}{(n,\ vs,\ [\,],\ O)\ \texttt{waiting}}$$

we can conclude $(n,\ v :: vs,\ I,\ O)\ \texttt{waiting}$.

Subcase I is $\mathit{true} :: I'$:

Then by the rule

$$\frac{\mathbf{V}(n,\ \mathbf{if}\ cnd\ \mathbf{then}\ n'\ \mathbf{else}\ n'') \in vs}{(n,\ vs,\ \mathit{true} :: I,\ O) \longmapsto (n',\ vs,\ I,\ O)}$$

we can conclude $(n,\ v :: vs,\ I,\ O) \longmapsto (n',\ v :: vs,\ I',\ O)$.

Subcase I is $\mathit{false} :: I'$:

Then by the rule

$$\frac{\mathbf{V}(n,\ \mathbf{if}\ cnd\ \mathbf{then}\ n'\ \mathbf{else}\ n'') \in vs}{(n,\ vs,\ \mathit{false} :: I,\ O) \longmapsto (n'',\ vs,\ I,\ O)}$$

we can conclude $(n,\ v :: vs,\ I,\ O) \longmapsto (n'',\ v :: vs,\ I',\ O)$.

Case c is **goto** n':

Then by the rule

$$\frac{\mathbf{V}(n,\ \mathbf{goto}\ n') \in vs}{(n,\ vs,\ I,\ O) \longmapsto (n',\ vs,\ I,\ O)}$$

we can conclude $(n,\ v :: vs,\ I,\ O) \longmapsto (n',\ v :: vs,\ I,\ O)$.

Case c is **end**:

Then by the rule

$$\frac{\mathbf{V}(n,\ \mathbf{end}) \in vs}{(n,\ vs,\ I,\ O)\ \texttt{terminated}}$$

we can conclude $(n,\ v :: vs,\ I,\ O)$ `terminated`.

3 Preservation

Theorem 2. *If cfg* `cfgvalid` *and* $cfg \longmapsto cfg'$ *then* cfg' `cfgvalid`.

3.1 Lemma 1

If $(vs,\ U_v,\ n,\ U)$ `connected` then $\forall n' \in U\ .\ \exists\ U'_v,\ U'$ such that U' is nonempty and $(vs,\ U'_v,\ n',\ U')$ `connected`.

Proof: We proceed by rule induction on $(vs,\ U_v,\ n,\ U)$ `connected`.

Case $\dfrac{(vs,\ U)\ \texttt{defined} \qquad U_v \subseteq U \qquad n \in U_v}{(vs,\ U_v,\ n,\ \emptyset)\ \texttt{connected}}$

Then U is the empty set so the lemma is vacuously true.

$$\text{Case } \frac{(vs,\ U)\ \texttt{defined} \qquad U_v \subseteq U \qquad \mathbf{V}(n,\ \mathbf{end}) \in vs \qquad n \notin U_v}{(vs,\ U_v,\ n,\ \{n\})\ \texttt{connected}}$$

Then U contains exactly n. But we already have $(vs,\ U_v,\ n,\ \{n\})$ `connected` so the lemma is satisfied.

$$\text{Case } \frac{\begin{array}{c}\mathbf{V}(n,\ \mathbf{do}\ a\ \mathbf{then}\ n') \in vs \\ (vs,\ U_v \cup \{n\},\ n',\ U)\ \texttt{connected} \qquad n \notin U_v\end{array}}{(vs,\ U_v,\ n,\ U \cup \{n\})\ \texttt{connected}}$$

Then by the inductive hypothesis, since $(vs,\ U_v \cup \{n\},\ n',\ U)$ `connected` we know the lemma is satisfied for all $n' \in U$. All that's left is to show it is satisfied for n, but we have $(vs,\ U_v,\ n,\ U \cup \{n\})$ `connected`.

$$\text{Case } \frac{\begin{array}{c}\mathbf{V}(n,\ \mathbf{do}\ a\ \mathbf{until}\ cnd\ \mathbf{then}\ n') \in vs \\ (vs,\ U_v \cup \{n\},\ n',\ U)\ \texttt{connected} \qquad n \notin U_v\end{array}}{(vs,\ U_v,\ n,\ U \cup \{n\})\ \texttt{connected}}$$

Analogous to the case above.

$$\text{Case } \frac{\mathbf{V}(n,\ \mathbf{goto}\ n') \in vs \qquad (vs,\ U_v \cup \{n\},\ n',\ U)\ \texttt{connected} \qquad n \notin U_v}{(vs,\ U_v,\ n,\ U \cup \{n\})\ \texttt{connected}}$$

Analogous to the case above.

$$\text{Case } \frac{\begin{array}{c}\mathbf{V}(n,\ \mathbf{if}\ cnd\ \mathbf{then}\ n'\ \mathbf{else}\ n'') \in vs \qquad (vs,\ U_v \cup \{n\},\ n',\ U)\ \texttt{connected} \\ (vs,\ U_v \cup U \cup \{n\},\ n'',\ U')\ \texttt{connected} \qquad n \notin U_v\end{array}}{(vs,\ U_v,\ n,\ U \cup U' \cup \{n\})\ \texttt{connected}}$$

Then by the inductive hypothesis, since $(vs,\ U_v \cup \{n\},\ n',\ U)$ `connected` and $(vs,\ U_v \cup U \cup \{n\},\ n'',\ U')$ `connected` we know the lemma is satisfied for all $n' \in U \cup U'$. All that's left is to show it is satisfied for n, but we have $(vs,\ U_v,\ n,\ U \cup U' \cup \{n\})$ `connected`.

3.2 Lemma 2

If $\mathbf{V}(n,\ c) \in vs$ and $(vs,\ U)$ `defined` then $n \in U$.

Proof: We proceed by rule induction on $(vs,\ U)$ `defined`.

Case $\dfrac{}{(nil,\ \{\ \})\ \texttt{defined}}$

But vs is nil, so the lemma is vacuously true.

Case $\dfrac{(vs,\ U)\ \texttt{defined} \qquad n' \notin U}{(\mathbf{V}(n',\ c) :: vs,\ U \cup \{n'\})\ \texttt{defined}}$

(n is replaced by n' in this statement of the rule to avoid ambiguity.)

The vertex in question, $\mathbf{V}(n,\ c)$, is either $\mathbf{V}(n',\ c)$ or $\in vs$. If it is the former, we are done since $n' \in U \cup \{n'\}$. If it is the latter, then by the inductive hypothesis, since $(vs,\ U)$ `defined` we know $n \in U$ so $n \in U \cup \{n'\}$.

3.3 Lemma 3

If $(vs,\ U)$ `defined` and $n \in U$ then $\mathbf{V}(n,\ c) \in vs$ for some c.

Proof: We proceed by rule induction on $(vs,\ U)$ `defined`.

Case $\dfrac{}{(nil,\ \{\ \})\ \texttt{defined}}$

But U is empty so the lemma is vacuously true.

Case $\dfrac{(vs,\ U)\ \texttt{defined} \qquad n' \notin U}{(\mathbf{V}(n',\ c) :: vs,\ U \cup \{n'\})\ \texttt{defined}}$

(n is replaced by n' in this statement of the rule to avoid ambiguity.)

n is either $\in U$ or is n'. We know it's not both since $n' \notin U$. If it's the former, then by the inductive hypothesis, since $(vs,\ U)$ `defined`, we know there is a $\mathbf{V}(n,\ c) \in vs$, which is also in $\mathbf{V}(n',\ c) :: vs$. If it's the latter, then clearly $\mathbf{V}(n',\ c) \in \mathbf{V}(n',\ c) :: vs$.

3.4 Lemma 4

If $(vs,\ U)$ `defined` and $\mathbf{V}(n,\ c) \in vs$ and $\mathbf{V}(n,\ c') \in vs$ then $c = c'$.

Proof: We proceed by induction on $(vs,\ U)$ `defined`.

Case $\dfrac{}{(nil,\ \{\ \})\ \texttt{defined}}$

But vs is nil so the lemma is vacuously true.

Case $\dfrac{(vs,\ U)\ \texttt{defined} \qquad n' \notin U}{(\mathbf{V}(n',\ c) :: vs,\ U \cup \{n'\})\ \texttt{defined}}$

(n is replaced by n' in this statement of the rule to avoid ambiguity.)

Suppose that $\mathbf{V}(n,\ c)$ and $\mathbf{V}(n,\ c')$ are both $\mathbf{V}(n',\ c)$. Then clearly $c = c'$.

Suppose instead that one of the two is $\mathbf{V}(n',\ c)$ (so $n = n'$) and the other is $\in vs$. Then by Lemma 2, $n \in U$. But $n' \notin U$, contradiction.

Suppose lastly that both are $\in vs$. Then by the inductive hypothesis, $c = c'$.

3.5 Lemma 5

If $(vs,\ U_v,\ n,\ U)$ `connected`, then $\forall\, n' \in U_v\ .\ \exists\, c'$ such that $\mathbf{V}(n',\ c') \in vs$.

Proof: We proceed by rule induction on $(vs,\ U_v,\ n,\ U)$ `connected`.

$$\text{Case}\ \frac{(vs,\ U)\ \texttt{defined} \qquad U_v \subseteq U \qquad n \in U_v}{(vs,\ U_v,\ n,\ \emptyset)\ \texttt{connected}}$$

Since $U_v \subseteq U$, it suffices to check this is true for every element in U. Since we have $(vs,\ U)$ `defined`, we have this property by Lemma 3.

$$\text{Case}\ \frac{(vs,\ U)\ \texttt{defined} \qquad U_v \subseteq U \qquad \mathbf{V}(n,\ \mathbf{end}) \in vs \qquad n \notin U_v}{(vs,\ U_v,\ n,\ \{n\})\ \texttt{connected}}$$

Analogous to the case above.

$$\text{Case}\ \frac{\begin{array}{c}\mathbf{V}(n,\ \mathbf{do}\ a\ \mathbf{then}\ n') \in vs \\ (vs,\ U_v \cup \{n\},\ n',\ U)\ \texttt{connected} \qquad n \notin U_v\end{array}}{(vs,\ U_v,\ n,\ U \cup \{n\})\ \texttt{connected}}$$

Then by the inductive hypothesis, since $(vs,\ U_v \cup \{n\},\ n',\ U)$ `connected` we know the lemma is satisfied for all $n' \in U_v \cup \{n\}$. Since $U_v \subseteq U_v \cup \{n\}$, this is also true for all $n' \in U_v$.

$$\text{Case}\ \frac{\begin{array}{c}\mathbf{V}(n,\ \mathbf{do}\ a\ \mathbf{until}\ cnd\ \mathbf{then}\ n') \in vs \\ (vs,\ U_v \cup \{n\},\ n',\ U)\ \texttt{connected} \qquad n \notin U_v\end{array}}{(vs,\ U_v,\ n,\ U \cup \{n\})\ \texttt{connected}}$$

Analogous to the case above.

$$\text{Case}\ \frac{\mathbf{V}(n,\ \mathbf{goto}\ n') \in vs \qquad (vs,\ U_v \cup \{n\},\ n',\ U)\ \texttt{connected} \qquad n \notin U_v}{(vs,\ U_v,\ n,\ U \cup \{n\})\ \texttt{connected}}$$

Analogous to the case above.

$$\text{Case}\ \frac{\mathbf{V}(n,\ \textbf{if}\ \mathit{cnd}\ \textbf{then}\ n'\ \textbf{else}\ n'') \in \mathit{vs} \qquad (\mathit{vs},\ U_v \cup \{n\},\ n',\ U)\ \texttt{connected} \qquad (\mathit{vs},\ U_v \cup U \cup \{n\},\ n'',\ U')\ \texttt{connected} \qquad n \notin U_v}{(\mathit{vs},\ U_v,\ n,\ U \cup U' \cup \{n\})\ \texttt{connected}}$$

Analogous to the case above.

3.6 Proof of Preservation

Recall that we stated preservation as "If cfg $\texttt{cfgvalid}$ and $\mathit{cfg} \longmapsto \mathit{cfg}'$ then cfg' $\texttt{cfgvalid}$."

We begin by case analyzing on cfg $\texttt{cfgvalid}$ in order to conclude some important facts.

The only case is

$$\frac{\mathbf{P}(v,\ \mathit{vs})\ \texttt{valid} \qquad \mathbf{V}(n,\ c) \in v :: \mathit{vs}}{(n,\ v :: \mathit{vs},\ I,\ O)\ \texttt{cfgvalid}}$$

so we can conclude:

$$\mathit{cfg} = (n,\ v :: \mathit{vs},\ I,\ O) \tag{1}$$

$$\mathbf{P}(v,\ \mathit{vs})\ \texttt{valid} \tag{2}$$

$$\mathbf{V}(n,\ c) \in v :: \mathit{vs} \tag{3}$$

We case analyze on $\mathbf{P}(v,\ \mathit{vs})$ $\texttt{valid}$. The only case is

$$\frac{(\mathbf{V}(s,\ c_s) :: \mathit{vs},\ U)\ \texttt{defined} \qquad (\mathbf{V}(s,\ c_s) :: \mathit{vs},\ \emptyset,\ s,\ U)\ \texttt{connected}}{\mathbf{P}(\mathbf{V}(s,\ c_s),\ \mathit{vs})\ \texttt{valid}}$$

so we can conclude:

$$v = \mathbf{V}(s,\ c_s) \tag{4}$$

$$(\mathbf{V}(s,\ c_s) :: vs,\ U)\ \texttt{defined} \tag{5}$$

$$(\mathbf{V}(s,\ c_s) :: vs,\ \emptyset,\ s,\ U)\ \texttt{connected} \tag{6}$$

From (3), (4), and (5), using Lemma 2 we can conclude

$$n \in U \tag{7}$$

From (6) and (7), using Lemma 1 we can conclude $\exists\ U'_v,\ U'$ where U' is not empty such that

$$(v :: vs,\ U'_v,\ n,\ U')\ \texttt{connected} \tag{8}$$

We continue by case analyzing on $cfg \longmapsto cfg'$.

Case $\dfrac{\mathbf{V}(n,\ \mathbf{do}\ a\ \mathbf{then}\ n') \in vs'}{(n,\ vs',\ I,\ O) \longmapsto (n',\ vs',\ I,\ a :: O)}$

So taking into account (1), cfg is of the form $(n,\ v :: vs,\ I,\ O)$ and cfg' is of the form $(n',\ v :: vs,\ I,\ a :: O)$. We do another case analysis on (8).

Subcase $\dfrac{(v :: vs,\ U)\ \texttt{defined} \qquad U'_v \subseteq U \qquad n \in U'_v}{(v :: vs,\ U'_v,\ n,\ \emptyset)\ \texttt{connected}}$

But U' is not empty, contradiction.

All but one of all of the other subcases have a premise of the form $\mathbf{V}(n,\ c') \in v :: vs$ where c' is not **do** a **then** n'. This is a contradiction by Lemma 4 since we have $\mathbf{V}(n,\ \textbf{do}\ a\ \textbf{then}\ n') \in v :: vs$.

Thus the only subcase left is

$$\frac{\mathbf{V}(n,\ \textbf{do}\ a\ \textbf{then}\ n') \in vs \qquad (v :: vs,\ U'_v \cup \{n\},\ n',\ U'')\ \texttt{connected} \qquad n \notin U'_v}{(v :: vs,\ U'_v,\ n,\ U'' \cup \{n\})\ \texttt{connected}}$$

If we let U''_v be $U'_v \cup \{n\}$, then we can case analyze on $(v :: vs,\ U''_v,\ n',\ U'')\ \texttt{connected}$:

Sub-subcase $\dfrac{(v :: vs,\ U)\ \texttt{defined} \qquad U''_v \subseteq U \qquad n' \in U''_v}{(v :: vs,\ U''_v,\ n',\ \emptyset)\ \texttt{connected}}$

Then since we have $n' \in U''_v$, by Lemma 5, $\exists\ c'$ such that $\mathbf{V}(n',\ c') \in v :: vs$.

In any of the other sub-subcases, one of the premises gives us $\mathbf{V}(n',\ c') \in v :: vs$ for some c'.

So regardless of the sub-subcase, we have $\mathbf{V}(n',\ c') \in v :: vs$. Combining with (2), we can conclude $(n',\ v :: vs,\ I,\ a :: O)\ \texttt{cfgvalid}$ as desired.

Case $\dfrac{\mathbf{V}(n,\ \textbf{do}\ a\ \textbf{until}\ cnd\ \textbf{then}\ n') \in vs}{(n,\ vs,\ true :: I,\ O) \longmapsto (n',\ vs,\ I,\ a :: O)}$

So taking into account (1), cfg is of the form $(n,\ v :: vs,\ true :: I',\ O)$ and cfg' is of the form $(n',\ v :: vs,\ I',\ a :: O)$. The rest of the proof for this case is analogous to above except c is **do** a **until** cnd **then** n' and the end conclusion is that $(n',\ v :: vs,\ I',\ a :: O)\ \texttt{cfgvalid}$.

Case $\dfrac{\mathbf{V}(n,\ \textbf{do}\ a\ \textbf{until}\ cnd\ \textbf{then}\ n') \in vs}{(n,\ vs,\ false :: I,\ O) \longmapsto (n,\ vs,\ I,\ a :: O)}$

So taking into account (1), *cfg* is of the form $(n,\ v :: vs,\ \mathit{false} :: I',\ O)$ and cfg' is of the form $(n,\ v :: vs,\ I',\ a :: O)$. The rest of the proof for this case is analogous to above except c is **do** a **until** cnd **then** n' and the end conclusion is that $(n,\ v :: vs,\ I',\ a :: O)$ `cfgvalid`.

$$\text{Case}\ \frac{\mathbf{V}(n,\ \mathbf{goto}\ n') \in vs}{(n,\ vs,\ I,\ O) \longmapsto (n',\ vs,\ I,\ O)}$$

So taking into account (1), *cfg* is of the form $(n,\ v :: vs,\ I,\ O)$ and cfg' is of the form $(n',\ v :: vs,\ I,\ O)$. The rest of the proof for this case is analogous to above except c is **goto** n' and the end conclusion is that $(n',\ v :: vs,\ I,\ O)$ `cfgvalid`.

$$\text{Case}\ \frac{\mathbf{V}(n,\ \mathbf{if}\ \mathit{cnd}\ \mathbf{then}\ n'\ \mathbf{else}\ n'') \in vs}{(n,\ vs,\ \mathit{true} :: I,\ O) \longmapsto (n',\ vs,\ I,\ O)}$$

So taking into account (1), *cfg* is of the form $(n,\ v :: vs,\ \mathit{true} :: I',\ O)$ and cfg' is of the form $(n',\ v :: vs,\ I',\ O)$. The rest of the proof for this case is analogous to above except c is **if** cnd **then** n' **else** n'' and the end conclusion is that $(n',\ v :: vs,\ I',\ a :: O)$ `cfgvalid`.

$$\text{Case}\ \frac{\mathbf{V}(n,\ \mathbf{if}\ \mathit{cnd}\ \mathbf{then}\ n'\ \mathbf{else}\ n'') \in vs}{(n,\ vs,\ \mathit{false} :: I,\ O) \longmapsto (n'',\ vs,\ I,\ O)}$$

So taking into account (1), *cfg* is of the form $(n,\ v :: vs,\ \mathit{false} :: I',\ O)$ and cfg' is of the form $(n'',\ v :: vs,\ I',\ O)$. We do another case analysis on (8).

$$\text{Subcase}\ \frac{(v :: vs,\ U)\ \texttt{defined} \qquad U'_v \subseteq U \qquad n \in U'_v}{(v :: vs,\ U'_v,\ n,\ \emptyset)\ \texttt{connected}}$$

But U' is not empty, contradiction.

All but one of all of the other subcases have a premise of the form $\mathbf{V}(n,\ c') \in v :: vs$ where c' is not $\textbf{if}\ cnd\ \textbf{then}\ n'\ \textbf{else}\ n''$. This is a contradiction by Lemma 4 since we have $\mathbf{V}(n,\ \textbf{if}\ cnd\ \textbf{then}\ n'\ \textbf{else}\ n'') \in v :: vs$.

Thus the only subcase left is

$$\frac{\begin{array}{c}\mathbf{V}(n,\ \textbf{if}\ cnd\ \textbf{then}\ n'\ \textbf{else}\ n'') \in v :: vs \\ (v :: vs,\ U'_v \cup \{n\},\ n',\ U)\ \texttt{connected} \\ (v :: vs,\ U'_v \cup U \cup \{n\},\ n'',\ U'')\ \texttt{connected} \qquad n \notin U'_v\end{array}}{(v :: vs,\ U'_v,\ n,\ U \cup U'' \cup \{n\})\ \texttt{connected}}$$

If we let U''_v be $U'_v \cup U \cup \{n\}$, then we can case analyze on $(v :: vs,\ U''_v,\ n'',\ U'')\ \texttt{connected}$:

Sub-subcase $\dfrac{(v :: vs,\ U)\ \texttt{defined} \qquad U''_v \subseteq U \qquad n'' \in U''_v}{(v :: vs,\ U''_v,\ n'',\ \emptyset)\ \texttt{connected}}$

Then since we have $n'' \in U''_v$, by Lemma 5, $\exists\ c'$ such that $\mathbf{V}(n'',\ c') \in v :: vs$.

In any of the other sub-subcases, one of the premises gives us $\mathbf{V}(n'',\ c') \in v :: vs$ for some c'.

So regardless of the sub-subcase, we have $\mathbf{V}(n'',\ c') \in v :: vs$. Combining with (2), we can conclude $(n'',\ v :: vs,\ I',\ O)\ \texttt{cfgvalid}$ as desired.