Construct Semi-linear Inductive Invariants

A **semi-linear separator** is a pair $(F, B) \subseteq \mathbb{N}^c \times \mathbb{N}^c$ so that

(Semi-linear) F, B are semi-linear

(separator) $post^*(F) \cap B = \emptyset$

The **domain** is $D = \overline{F \cup B}$. Note that D is also semi-linear.

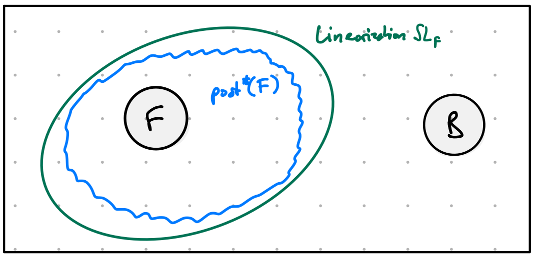
<u>Lemma</u> Let (F,B) be a semi-linear separator with non-empty domain D.
There is a semi-linear separator (F', B') with domain D' so that

(a) $F \subseteq F'$ and $B \subseteq B'$

(b) $\dim(D') < \dim(D)$

Proof: We overapproximate $post^*(F) \cap \overline{F}$ by a semi-linear set SL and choose

$$B' = B \cup \overline{F \cup SL}$$



What is SL?

$$post^*(F) \cap \overline{F} = \underbrace{PL_1 \cup \ldots \cup PL_k}_{\text{semi-pseudo-linear}} \subseteq \underbrace{L_1 \cup \ldots \cup L_k}_{\text{linearizations}} =: SL$$

Then (F, B') is a semi-linear separator:

$$post^*(F) \cap B' = post^*(F) \cap (B \cup \overline{F \cup SL})$$

$$= \underbrace{post^*(F) \cap B}_{\substack{= \emptyset \text{, because} \\ (F,B) \text{ is separator}}} \cup \underbrace{post^*(F) \cap \overline{F} \cap \overline{SL}}_{\substack{= \emptyset \text{, because} \\ post^*(F) \cap \overline{F} \subseteq SL}} = \emptyset$$

Symmetrically, we overapproximate $pre^*(B') \cap \overline{B'}$ by SL':

$$\overline{B'} \cap pre^*(B') = \underbrace{PL'_1 \cup \ldots PL'_\ell}_{\text{semi-pseudo-linear}} \subseteq \underbrace{L'_1 \cup \ldots \cup L'_\ell}_{\text{linearizations}} =: SL'$$

and set $F' = F \cup \overline{B' \cup SL'}$

Then (F', B') is a semi-linear separator:

$$post^*(F') \cap B' = \emptyset \iff F' \cap pre^*(B') = \emptyset$$

and $F' \cap pre^*(B') = (F \cup \overline{B' \cup SL'}) \cap pre^*(B')$

$$= \underbrace{F \cap pre^*(B')}_{\substack{= \emptyset \text{, because} \\ (F,B') \text{ separator}}} \cup \underbrace{\overline{SL'} \cap \overline{B'} \cap pre^*(B')}_{\substack{\emptyset \text{, because} \\ \overline{B'} \cap pre^*(B') \subseteq SL'}} = \emptyset$$

Note that F', B' are semilinear by standard closure properties and $F \subseteq F'$ and $B \subseteq B'$ hold by construction.

It remains to show $\dim(D') < \dim(D)$.

$$D' = \overline{F' \cup B'} = \overline{F \cup (\overline{B' \cup SL'}) \cup B \cup (\overline{F \cup SL})}$$

$$= \overline{F} \cap (B' \cup SL') \cap \overline{B} \cap (F \cup SL)$$

$$= \underbrace{\overline{F} \cap B' \cap \overline{B} \cap (F \cup SL)}_{= \emptyset \text{, because } B' = B \cup \overline{F \cup SL}} \cup \overline{F} \cap SL' \cap \overline{B} \cap (F \cup SL)$$

$$= \underbrace{\overline{F} \cap SL' \cap \overline{B} \cap F}_{\emptyset} \cup \overline{F} \cap SL' \cap \overline{B} \cap SL$$

$$= D \cap SL \cap SL'$$

Then $\dim(D') = \dim(D \cap SL \cap SL') \leq \dim(SL \cap SL')$

$$\leq \max_{\substack{1 \leq i \leq k \\ 1 \leq j \leq l}} \dim(L_i \cap L'_j)$$

$PL_i \cap PL'_j = \emptyset$ + above lemma

$$< \max_{\substack{1 \leq i \leq k \\ 1 \leq j \leq l}} \dim(PL_i \cup PL'_j)$$

$PL_i \subseteq \overline{F} \cap \overline{B} = D$

$PL'_j \subseteq \overline{B'} \cap \overline{F} \subseteq \overline{B} \cap \overline{F} = D$

$$\leq \dim(D)$$

□

We can show the theorem:

Let m_f be not reachable from m_s.

Then $(\{m_s\}, \{m_f\})$ is a semi-linear separator.

By a well-founded induction on the dimension of the domain there is a separator (F, B) with empty domain and $\{m_s\} \subseteq F \wedge \{m_f\} \subseteq B$.

Then, F is a semi-linear inductive invariant:

(initial) $m_s \in F$

(inductive) $post(F) \subseteq post^*(F) \cap (B \cup \overline{B}) = \underbrace{post^*(F) \cap B}_{\emptyset \text{, } (F,B) \text{ separator}} \cup post^*(F) \cap \overline{B} \subseteq F$ $\overline{B} = F$

(safe) $m_f \notin F \Leftrightarrow m_f \in \overline{F} = B$