Multithreaded Cartesian Abstraction

Consider a program with the set of states $State$ and initial states $init \subseteq State$. Let $D = \mathcal{P}(State)$ and $post: D \to D$ be the successor operator. Abstractions of the program for the sake of tractability usually involve a loss of precision: not all properties can be proven by an abstraction. Such a precision loss can often be described by an operator $D \to D$ that overapproximates sets of states

Def: An upper closure operator (shortly closure) on a poset $(X, \leq)$ is a map $\eta: X \to X$ that is
- monotone,
- extensive, i.e. $\forall x \in X.\ x \leq \eta(x)$,
- idempotent, i.e. $\eta \circ \eta = \eta$

Consider a multithreaded program with shared states $Shared$, local states $Local_t$ $(t \in Tid)$ and thread transition relations $\to_t$ $(t \in Tid)$. Let $D^\# = \prod_{t \in Tid} \mathcal{P}(Shared \times Local_t)$ be equipped with the product order $(X \sqsubseteq Y :\Leftrightarrow \forall t \in Tid.\ X_t \subseteq Y_t)$.

Remember: $\gamma_{mc}: D^\# \to D,\ (S_t)_{t \in Tid} \mapsto \{(g, l) \mid \forall t \in Tid.\ (g, l_t) \in S_t\}$.

Def: The multithreaded Cartesian abstraction is the map

$$\alpha_{mc}: D \to D^\#,\ S \mapsto (\{(g, l_t) \mid (g, l) \in S\})_{t \in Tid}$$

Example: $Tid = \mathbb{N}_3$, $D^\# = \mathcal{P}(Shared \times Local_1) \times \mathcal{P}(Shared \times Local_2) \times$

The multi-threaded Cartesian approximation is the map

$\rho_{mc} : D \to D, \quad S \mapsto \gamma_{mc} \circ \alpha_{mc}(S)$

Prop ρ_{mc} is a closure.

Proof:

- Monotonicity
  - α_{mc} is monotone:
    Let $S \subseteq S'$. Let $t \in Tid$, $(g,m) \in (\alpha_{mc}(S))_t$. Then there is l such that $l_t = m$ and $(g,l) \in S$. So $(g,l) \in S'$. So $(g,l_t) \in (\alpha_{mc}(S'))_t$. So $\alpha_{mc}(S) \sqsubseteq \alpha_{mc}(S')$
  - γ_{mc} is monotone:
    Let $(S_t)_{t \in Tid}, (S'_t)_{t \in Tid} \in D^\#$, $(S_t)_{t \in Tid} \sqsubseteq (S'_t)_{t \in Tid}$.
    Let $(g,l) \in \gamma_{mc}((S_t)_{t \in Tid})$. Then $\forall t \in Tid.\ (g,l_t) \in S_t$.
    So $\forall t \in Tid.\ (g,l_t) \in S'_t$. So $(g,l) \in \gamma_{mc}((S'_t)_{t \in Tid})$
- Extensivity: Let $S \subseteq State$. Let $(g,l) \in S$. By def of α_{mc}, $\forall t \in Tid.\ (g,l_t) \in (\alpha_{mc}(S))_t$. So $(g,l) \in \gamma_{mc}((\alpha_{mc}(S))_{t \in Tid})$
  $= \gamma_{mc}(\alpha_{mc}(S)) = \rho_{mc}(S)$
- Idempotence: Let $S \subseteq State$. Will show $\rho_{mc}(\rho_{mc}(S)) = \rho_{mc}(S)$
  "$\subseteq$": Let $(g,l) \in \rho_{mc}(\rho_{mc}(S)) = \gamma_{mc}(\alpha_{mc}(\gamma_{mc}(\alpha_{mc}(S))))$. Then $\forall t \in Tid.\ (g,l_t) \in (\alpha_{mc}(\gamma_{mc}(\alpha_{mc}(S))))_t$. Then for each $t \in Tid$ there is some $h(t) \in \prod_{t \in Tid} Local_t$ such that $(h(t))_t = l_t$ and $(g,h(t)) \in \gamma_{mc}(\alpha_{mc}(S))$. Then $(g,(h(t))_t) \in (\alpha_{mc}(S))_t$. So $(g,l_t) \in (\alpha_{mc}(S))_t$.
  By def of γ_{mc}, $(g,l) \in \gamma_{mc}(\alpha_{mc}(S)) = \rho_{mc}(S)$
  "$\supseteq$": By extensivity ☐

Corollary. $\lambda S.\ \rho_{mc}(init \cup post(S))$ is monotone
Thus it has the least fixpoint

Thm: Let $((R_t)_{t \in Tid}, (G_t)_{t \in Tid})$ be the strongest thread-modular proof. Then

$$lfp\,(\underbrace{\lambda S.\ \rho_{mc}(init \cup post(S))}_{f}) = \underbrace{\gamma_{mc}((R_t)_{t \in Tid})}_{RHS}$$

Proof idea: By Tarski's fixpoint theorem

$lfp\, f = \bigcap \{S \in D \mid f(S) \subseteq S\}$.

It suffices to show: $f(RHS) \subseteq RHS$

- For any $S \in D$ with $f(S) \subseteq S$ we have $RHS \subseteq S$. ☐