Abstraction, Minimisation de graphe

Principe général

Principe

Rappel: un système de transitions (aussi appelé graphe) est $M = (S, S_0, R)$ avec

- S un ensemble (fini ou infini) d'états.
- $S_0 \subset S$ les états initiaux.
- $R \subset S \times S$ une relation de transitions totale.

Vérification d'invariant

- Problème de la vérification d'invariant:
  - Données:
    1. un système de transition M,
    2. un prédicat p sur les états.
  - Réponse:
    - Oui si la propriété p est invariante (toute chemin initialisé $\pi = s_0, s_1, \ldots$ de M est tel que s_i satisfait p pour tout i), Non sinon.

Atteignabilité

- Problème de l'atteignabilité:
  - Données:
    1. un système de transitions M,
    2. une région but $\sigma \subset S$.
  - Réponse:
    - Oui s'il existe un chemin initialisé qui atteint un état de σ, Non sinon.

Vérif. Invariant $\equiv$ Atteignabilité

- Un prédicat p sur les états définit la région $[\![p]\!] \subset S$ constituée des états s tels que $s \models p$.
- Théorème: Résoudre le problème de vérification d'invariant $(\mathcal{M}, p)$ est équivalent à résoudre le problème d'atteignabilité $(M, [\![\neg p]\!])$.

  Démonstration: p est un invariant de M ssi il n'existe pas de trajectoire initialisée qui atteint $[\![\neg p]\!]$.

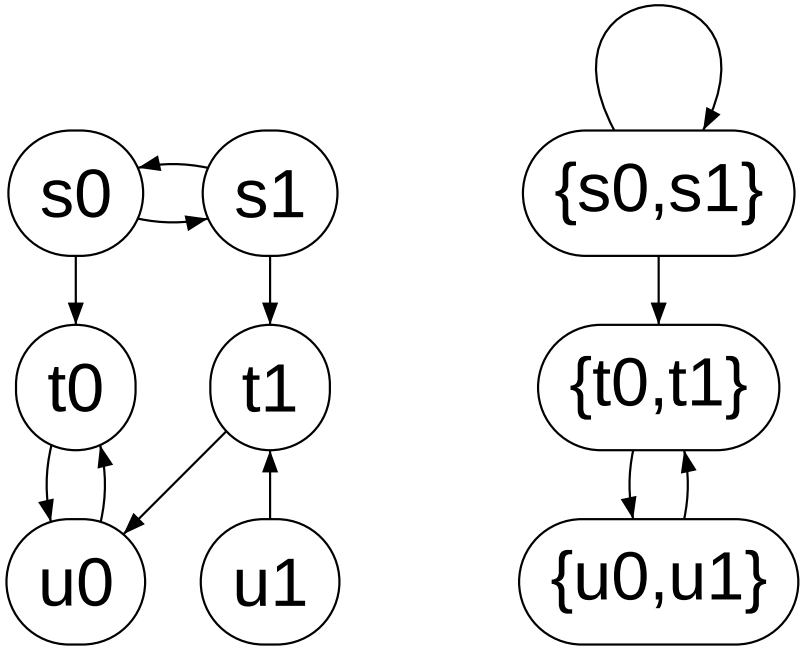
Partition

- Définition: Une *partition* $\simeq$ est une relation d'équivalence sur S. Une *région* est une classe d'équivalence de $\simeq$.

  (rappel: une relation d'équivalence est une relation symétrique, réflexive et transitive).

- Définition: le *graphe quotient de M par $\simeq$*, est le graphe $M/\simeq = (S/\simeq, S_0/\simeq, R/\simeq)$ tel que
  - l'espace des états $S/\simeq$ est constitué des régions.
  - l'ensemble des états initiaux $S_0/\simeq$ est défini par $S_0/\simeq = \{\sigma | \sigma \cap S_0 \neq \emptyset\}$, i.e. est constitué des régions qui contiennent un état initial.
  - la relation de transitions $R/\simeq$ est défini par: $R/\simeq (\sigma, \tau)$ ssi il existe $s \in \sigma$, $t \in \tau$ avec $R(s,t)$.
- Principe des techniques d'abstraction: choisir une partition $\simeq$ et analyser le quotient $M/\simeq$ plutôt que M.

Exemple de quotient



M $\qquad\qquad$ $M/\simeq$

Exemple: Propriétés d'atteignabilité

- Principe: on veut remplacer le problème d'atteignabilité (M, σ^T) par celui de $(M/\simeq, \sigma^T/\simeq)$ avec

$$\sigma^T/\simeq = \{\sigma | \sigma \cap \sigma^T \neq \emptyset\}.$$

- Proposition: si $\sigma^T/\simeq$ n'est pas atteignable dans $M/\simeq$, alors σ^T n'est pas atteignable dans M.

- La réciproque est fausse dans le cas général. Si $\sigma^T/\simeq$ est atteignable dans $M/\simeq$ alors on ne peut rien dire sur l'atteignabilité dans M de σ^T.

  Exemple: u_1 n'est pas atteignable depuis s_0 dans l'exemple précédent, alors que $\{u_1, u_0\}$ l'est depuis $\{s_0, s_1\}$.

- Autrement dit, dans le cas général, c'est une technique valide pour vérifier l'atteignabilité mais non-complète.

- Question: conditions nécessaires et suffisantes pour que $M/\simeq$ préserve l'atteignabilité?
  Solution: notion de partition stable.
- Intéret: trouver des hypothèses sur $\simeq$, qui permette de garantir

$$Atteignable(M, \sigma^T) \text{ ssi } Atteignable(M/\simeq, \sigma^T/\simeq)$$

et donc de permettre la vérification sur $M/\simeq$.

Partition stable

- Une partition $\simeq$ est *stable* si $s \simeq t$ et $R(s, s')$ implique l'existence d'un t' avec $s' \simeq t'$ et $R(t, t')$.
- Théorème: supposons que
  1. $\simeq$ est une partition stable,
  2. σ^T est un bloc de $\simeq$,

     (on appelle bloc une une union de régions; on suppose donc que σ^T correspond à un nombre entier de régions de la relation d'équivalence), (formellement $\forall \sigma$ region, $\sigma \cap \sigma^T \neq \emptyset$ implique $\sigma \subset \sigma^T$)

  Alors $\sigma^T / \simeq$ est atteignable dans $M / \simeq$ ssi σ^T est atteignable dans M.

Démonstration:

Sens $\Rightarrow$: A chaque trajectoire $\pi = s_0 s_1 \dots s_n$ de M correspond la trajectoire $\sigma_0 \sigma_1 \dots \sigma_n$ de $M/\simeq$, où σ_i est la classe d'équivalence de s_i. Si la trajectoire et initialisée et atteint σ^T, la trajectoire correspondante et aussi initialisée et atteint $\sigma^T/\simeq$.

Sens $\Leftarrow$: Supposons qu'on ait une trajectoire $\sigma_0 \sigma_1 \dots \sigma_n$ de $M/\simeq$. Prenons t_0 quelconque dans S_0. On montre par récurrence sur i, qu'il y a une trajectoire $t_0 t_1 \dots t_i$ de M avec t_i dans σ_i. C'est vrai au rang 0. Supposons au rang i, puisque $R/\simeq(\sigma_i, \sigma_{i+1})$, il existe $s \in \sigma_i, s' \in \sigma_{i+1}$ avec $R(s, s')$. Par stabilité, puisque $s \simeq t_i$, et $R(s, s')$, il existe $t' = t_{i+1}$ avec $R(t_i, t_{i+1})$, qui implique l'hypothèse de récurrence au rang $i+1$ pour la trajectoire $t_0 t_1 \dots t_{i+1}$.

Si la trajectoire $\sigma_0 \sigma_1 \dots \sigma_n$ de $M/\simeq$ est initialisée et atteint $\sigma^T/\simeq$, alors la trajectoire $t_0 t_1 \dots t_n$ est aussi initialisée, et puisque $\sigma_n \in \sigma^T/\simeq$, par définition $\sigma_n \cap \sigma^T \neq \emptyset$. Puisque σ^T est un bloc, $\sigma_n \subset \sigma^T$, et donc $t_n \in \sigma^T$.

Applications

1. Projection sur ensemble de variables.
2. Symétries.
3. Raffinement automatique de partition.