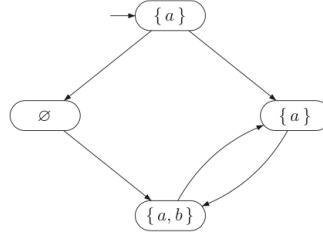


Verificação Formal de Software - Exercícios

Propriedades Temporais Lineares

1. Considerando o sistema de transições sobre as proposições atômicas $\{a, b\}$ desenhado abaixo, indica todos os seus traços.



2. Considera $AP = \{a, b, c\}$ e as seguintes propriedades:
1. Se a fica verdade, depois b fica para sempre verdade ou até c ser verdade.
 2. Entre duas ocorrências de a , b verifica-se sempre.
 3. Entre duas ocorrências de a , b verifica-se mais vezes que c
 4. $a \wedge \neg b$ e $b \wedge \neg a$ são verdade alternadamente ou até c ser verdade
- (a) Para cada propriedade P_i para $1 \leq i \leq 4$ indica se é uma propriedade de segurança regular.
- (b) Para os casos afirmativos define um NFA A_i tal que $L(A_i) = \text{BadPref}(P_i)$. Nota: nas transições podes usar fórmulas lógicas em vez dos símbolos de 2^{AP} .
3. Considera o conjunto $AP = \{A, B\}$ de proposições atômicas. Especifica as seguintes propriedades como propriedades LT e indica para cada uma se é um invariante, de segurança, de vivacidade ou nenhuma delas.
- a) A não deve ocorrer nunca
 - b) A deve ocorrer exactamente uma vez
 - c) A e B devem alternar um número infinito de vezes
 - d) Deve haver um ponto a partir do qual A deve ser seguido de B
4. Seja P é uma propriedade LT sobre um conjunto AP .
- (a) Mostra que P é uma propriedade de segurança se e só se $\text{closure}(P) = P$.
 - (b) Sendo P' outra propriedade LT , mostra que

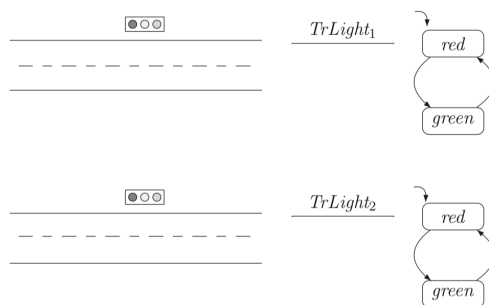
$$\text{closure}(P \cup P') = \text{closure}(P) \cup \text{closure}(P').$$

- (c) O teorema da decomposição afirma o seguinte

- $P = \text{closure}(P) \cap (P \cup (2^{AP})^\omega \setminus \text{closure}(P))$
- $\text{closure}(P)$ é uma propriedade de segurança
- $(P \cup (2^{AP})^\omega \setminus \text{closure}(P))$ é uma propriedade de vivacidade

Mostra as três afirmações anteriores.

5. Considera os seguintes sistemas de transição para semáforos de trânsito simples e independentes.



(a) Desenha o sistema de transição para a intercalagem de $T = T_1 ||| T_2$.

(b) Indica quantos caminhos infinitos existem começando no estado $\{red_1, red_2\}$.

(c) Considera $AP = \{red_1, red_2, green_1, green_2\}$ e a seguinte propriedade P :

Ambos os semáforos estão verdes um número infinito de vezes.

- Mostra que a propriedade anterior é de vivacidade.
- Indica, justificando, se o sistema T verifica a propriedade P .
- Supõe que para cada semáforo (T_1 e T_2), a ação $switch2green_i$ denota a transição entre o estado red_i e o estado $green_i$ e a ação $switch2red_i$ a transição contrária, para $i = 1, 2$. Considera a assumção de justeza (que é incondicional)

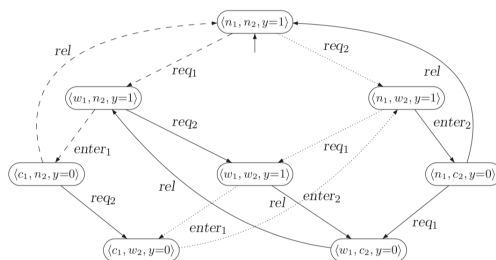
$$F = \{ \{ switch2green_1, switch2red_1 \}, \{ switch2green_2, switch2red_2 \} \}$$

. Mostra que $T \models_F P$.

6. Considera o problema de exclusão mútua com dois processos e $AP = \{w_1, c_1, w_2, c_2\}$. Mostra que as seguintes propriedades são de vivacidade e exprime-as formalmente.

- cada processo irá entrar na região crítica*
- cada processo irá entrar na região crítica um número infinito de vezes*
- cada processo em espera irá entrar na região crítica*

7. Considera o sistema de transição T_{sem} para a solução do problema de exclusão mútua com semáforo, onde as transições são etiquetadas com as ações óbvias de $Act = \{req_1, enter_1, req_2, enter_2, rel\}$. Seja $A = \{enter_2\}$.



- Mostra que a execução a tracejado que começa e termina $\langle n_1, n_2, y = 1 \rangle$ não é incondicionalmente A -justa. Mas é fortemente A -justa.
- Mostra que a execução a ponteadado que começa em $\langle n_1, n_2, y = 1 \rangle$ não é fortemente A -justa. Mas é fracamente A -justa.