Interacção e Concorrência

Teste - 7 Junho, 2022 (10:00 - 12:00)

***Nota**: O teste é composto por 10 questões, 7 sobre sistemas reactivos e 3 sobre sistemas quânticos, cada uma cotada para 2 valores.*

Questão 1

Uma relação binária S em $\mathbb{P}$ é uma *simulação fraca* sse, sempre que $(E, F) \in S$ e $a \in L \cup \{\epsilon\}$, se tem

$$E \overset{a}{\Longrightarrow} E' \quad \Rightarrow \quad F \overset{a}{\Longrightarrow} F' \ \wedge \ (E', F') \in S$$

onde L é um conjunto de identificadores de acção e $\overset{a}{\Longrightarrow}$ é a relação de transição observável definida nas aulas.

Dizemos que um processo P é *fracamente simulado* por outro processo Q, e escrevemos $P \lessapprox Q$ se existir uma simulação fraca contendo o par (P, Q).

1. Dê um exemplo concreto de dois processos P e Q que sejam fracamente similares (i.e. $P \lessapprox Q$), mas não fracamente bissimilares (i.e. $P \not\approx Q$).

   Sugestão de resolução

   $P = a.\mathbf{0}$ e $Q = \tau.a.\,\mathbf{0} + b.\mathbf{0}$

2. Mostre que a relação $\lessapprox$ é transitiva.

   Sugestão de resolução

   Queremos mostrar que se $P \lessapprox Q$ e $Q \lessapprox T$, então $P \lessapprox T$, para todo o P, Q e T. Por definição de $\lessapprox$, os factos $P \lessapprox Q$ e $Q \lessapprox T$ são testemunhados por duas relações de simulação fraca, digamos R e R', respectivamente. Para concluir, então, que $P \lessapprox T$ é suficiente mostrar que a composta $R' \cdot R$ é também uma simulação fraca. Esta prova segue passos similares à prova feita nas aulas de que a composição de duas bissimulações é ainda uma bissimulação, passos que deverão ser revisitados/adaptados para concluir esta resposta.

3. Suponha que mostrou que um processo P é fracamente simulado por outro processo Q e vice versa. Em que condições poderá concluir que $P \approx Q$? Justifique.

   Sugestão de resolução

   Para que se tivesse $P \approx Q$ seria necessário que as simulações fracas que testemunham $P \lessapprox Q$ e $Q \lessapprox P$ fossem conversas uma da outra.

Questão 2

O sistema de controlo de um cruzamento entre a rua X e a rua Y, ambas de sentido único, deve garantir o funcionamento correcto dos semáforos colocados nas duas ruas. O protocolo de funcionamento é o seguinte: o sinal está sempre verde para a rua X e vermelho para a rua Y a menos que um carro seja detectado na rua Y por um sensor. Esse evento fará as luzes trocarem e o tráfego da rua Y escoar. Algum tempo depois os semáforos voltam ao estado habitual, com o sinal verde na rua X para que o seu tráfego se possa escoar, assim se mantendo até que um novo carro seja detectado na rua Y.

1. Especifique um processo C que corresponda aos requisitos acima para o sistema de controlo do cruzamento.

   Sugestão de resolução

   Uma possível especificação do sistema de controlo seria:

$$\begin{aligned} C &= sensorY.vermelhoX.verdeY.C' \ + \ passaCarroEmX.C \\ C' &= passaCarroEmY.C' \ + \ timeout.vermelhoY.verdeX.C \end{aligned}$$

com a seguinte interpretação dos eventos: $passaCarroEmX$ (carro passa na rua X), $passaCarroEmY$ (carro passa na rua Y), $verdeX$ (semáforo da rua X passa a verde), $verdeY$ (semáforo da rua Y passa a verde), $vermelhoX$ (semáforo da rua X passa a vermelho), $vermelhoY$ (semáforo da rua Y passa a vermelho)$sensorY$ (foi activado o sensor de aproximação de carro na rua Y), $timeout$ (foi esgotado o tempo de semáforo aberto na rua Y).

2. Especifique na lógica de processos que estudou, duas propriedades não triviais que sejam válidas para o processo C e explique informalmente o seu significado.

Sugestão de resolução

Duas propriedades válidas no processo C serão

$$[sensorY][-vermelhoX]\textsf{false} \quad \text{e} \quad [verdeY]\langle timeout\rangle\textsf{true}$$

Questão 3

---

1. Mostre, recorrendo à definição de *igualdade de processos* ($=$), que, para qualquer processo P,

$$\tau.P \;=\; P + \tau.P$$

Sugestão de resolução

Esta igualdade é estabelecida por aplicação directa da definição da igualdade entre processos: os processos em ambos os lados realizam uma transição por τ inicial, o que conduz a P and $P + P$, respectivamente, processos que são bissimilares pela lei da idempotência de $+$.

2. Use esse facto para verificar a seguinte equação entre processos:

$$\tau.(E + F) \;=\; E + \tau.(E + F)$$

Sugestão de resolução

$$\begin{array}{ll}
& \tau.(E+F) \\
= & \quad \{ \text{ alínea anterior}\} \\
& E + F + \tau.(E+F) \\
= & \quad \{ + \text{ é idempotente (aplicada duas vezes) } \} \\
& E + E + F + \tau.(E+F) + \tau.(E+F) \\
= & \quad \{ \text{ alínea anterior } \} \\
& E + \tau.(E+F) + \tau.(E+F) \\
= & \quad \{ + \text{ é idempotente}\} \\
& E + \tau.(E+F)
\end{array}$$

Questão 4

Como sabe, a partir de qualquer operador unitário U pode ser definido um outro operador C_U sobre dois qubits em que a aplicação de U ao segundo qubit é condicionada pelo valor do primeiro qubit. Recorde como exemplo a porta $CNOT$ que estudou. Na base computacional, C_U pode ser escrito como

$$C_Q|x\rangle|y\rangle \;=\; |x\rangle \otimes Q^x|y\rangle$$

com $x \in \{0, 1\}$:

1. Calcule a representação matricial de C_Z onde Z é uma das portas de Pauli definida por $Z = |0\rangle\langle 0| - |1\rangle\langle 1|$.

   Sugestão de resolução

   A representação matricial de $Z = |0\rangle\langle 0| - |1\rangle\langle 1|$ é a matriz

   $$Z \;=\; \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

   Então, usando a definição acima e notando que o produto tensorial $\otimes$ corresponde ao produto tensorial de matrizes (também dito de Kronecker), vem

   $$\begin{bmatrix} 1Z^0 & 0Z^1 \\ 0Z^0 & 1Z^1 \end{bmatrix} \;=\; \begin{bmatrix} I & 0 \\ 0 & Z \end{bmatrix} \;=\; \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$$

2. Mostre que $CNOT$ pode ser implementado com recurso a C_Z, i.e.

   $$CNOT\;|x\rangle|y\rangle \;=\; (I \otimes H) \cdot C_Z \cdot (I \otimes H)\;|x\rangle|y\rangle$$

   e desenhe o circuito correspondente à expressão $(I \otimes H) \cdot C_Z \cdot (I \otimes H)$.

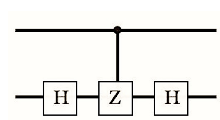
   Sugestão de resolução

   $$\begin{aligned}
   & CNOT|x\rangle|y\rangle \\
   = & \qquad \{\text{ definição de } CNOT\} \\
   & |x\rangle \otimes X^x|y\rangle \\
   = & \qquad \{\; X = HZH \;\} \\
   & |x\rangle \otimes (HZH)^x|y\rangle \\
   = & \qquad \{\; \star \,\} \\
   & |x\rangle \otimes HZ^xH|y\rangle \\
   = & \qquad \{\; I \otimes (HZ^xH) \;=\; (I \otimes H)(I \otimes Z^x)(I \otimes H) \text{ e definição de } C_Z\} \\
   & I \otimes H \cdot C_Z \cdot I \otimes H
   \end{aligned}$$

   Uma vez que H é unitário, o passo $\star$ é válido para qualquer x (mesmo se neste caso $x \in \{0, 1\}$). Por exemplo:

   $$\cdots(HZH)(HZH)\cdots \;=\; \cdots HZ(HH)ZH\cdots \;=\; \cdots HZZH\cdots$$

   O circuito será

3. Explique a razão pela qual se requer que as portas quânticas sejam implementadas por operadores unitários.

   Sugestão de resolução

   A Natureza não permite transformações arbitrárias de sistemas quânticos, mas apenas aquelas que respeitam as propriedades ligadas à medida e à sobreposição quânticas. Uma das condições fundamentais para isso é a preservação do produto interno. As transformações unitárias são exactamente aquelas que preservam o produto interno. Uma das consequências óbvias do facto de a transformação ser unitária é a sua reversibilidade.