Interacção e Concorrência

Teste - 20 Junho, 2020 (9.30 - 11.30)

***Nota**: O teste é composto por 10 questões, 6 sobre sistemas reactivos e 4 sobre sistemas quânticos, cada uma cotada para 2 valores.*

Questão 1

Os processos $P(c) \triangleq \sum_{n\in\mathbb{N}} \overline{c}\langle n\rangle.P$ e $Q(c) \triangleq \sum_{n\in\mathbb{N}} c(n).Q$ comunicam números naturais através de uma porta c. A composição

$$(P(c) \mid Q(c))\backslash_{\{c\}}$$

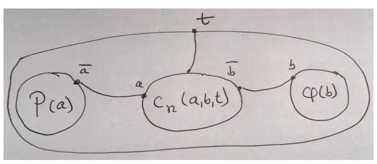
realiza a comunicação referida. Pretende-se, contudo, obter um esquema de comunicação mais sofisticado através de um processo auxiliar $C_n(a,b,t)$. Este processo é capaz de armazenar um número n e é dotado de três portas a, $\overline{b}$ e t, evoluindo de acordo com o seguinte comportamento:

- Interage com $P(a)$ sempre que este tem algum dado para transmitir na porta $\overline{a}$ e guarda o número recebido.
- Sempre que a porta t é invocada pelo ambiente, mas apenas nessa ocasião, comunica ao processo $Q(b)$ o último número lido, através da porta $\overline{b}$.

1. Desenhe o diagrama de sincronização da composição

$$(P(a) \mid C_0(a,b,t) \mid Q(b))\backslash_{\{a,b\}}$$

Sugestão de resolução



2. Especifique o processo C_n.

Sugestão de resolução

$C_n = a(m).C_m \; + \; t.\overline{b}\langle n\rangle.C_n$. Note que o último valor lido na porta a é armazenado no estado do processo.

3. Escreva na lógica modal que estudou a fórmula característica desse processo.

Sugestão de resolução

A fórmula característica deve especificar totalmente o processo: assim, a componente (1) afirma a inevitabilidade das acções iniciais a e t, enquanto (2) especifica a inevitabilidade de b após ocorrência de t. Os pontos de recursão indicam prevalência temporal, exprimindo a fórmula como uma propriedade de segurança.

$$\nu X \; (\underbrace{\langle a,t\rangle \mathsf{true} \wedge [-a,t]\mathsf{false}}_{(1)} \; \wedge \; \underbrace{[t](\langle b\rangle \mathsf{true} \wedge [-b]\mathsf{false} \wedge [b]X)}_{(2)} \; \wedge \; [a]X)$$

Questão 2

Considere o seguinte operador de renomeação de acções que é definido pela seguinte regra:

$$\frac{E \xrightarrow{a} E'}{E[f] \xrightarrow{f(a)} E'[f]}$$

onde $f : Act \longrightarrow Act$ é uma função que mapeia acções em acções sujeita às seguintes restrições: $f(\overline{a}) = \overline{f(a)}$ e $f(\tau) = \tau$.

1. Mostre que $(E+F)[f] \sim E[f]+F[f]$.

   Sugestão de resolução

   Basta mostrar que a relação
   $$\{((E+F)[f], E[f]+F[f]) \mid E,F \in \mathbb{P}\} \cup Id$$
   forma uma bissimulação. Para isso comecemos por considerar a relação
   $$R = \{((E+F)[f], E[f]+F[f]) \mid E,F \in \mathbb{P}\}$$
   e suponhamos que o processo $(E+F)[f]$ transita por y para um processo G. De acordo com a regra dada acima para definir o operador de renomeação concluimos que a acção y é da forma $f(x)$ e o processo G é da forma $H[f]$ para um processo H e uma acção x tal que
   $$E+F \xrightarrow{x} H$$
   A semântica da escolha não determinística de processos leva-nos a afirmar que existem duas possíveis razões para explicar esta transição:

   - ou $E \xrightarrow{x} H$
   - ou $F \xrightarrow{x} H$.

   No primeiro caso, se $E \xrightarrow{x} H$, então $E[f] \xrightarrow{f(x)} H[f]$, i.e. $E[f] \xrightarrow{y} G$, donde concluímos que
   $$E[f]+F[f] \xrightarrow{y} G$$
   A análise do segundo caso é similar. Como resultado, em ambos os casos teremos de adicionar o par (G,G) à relação R. A análise conversa segue os mesmos passos: suponhamos que existe a transição
   $$E[f]+F[f] \xrightarrow{y} G$$
   De novo y e G tomam a forma $y=f(x)$ e $G=H[f]$ para um processo H e uma acção x tal que

   - ou $E \xrightarrow{x} H$
   - ou $F \xrightarrow{x} H$.

   que, por sua vez, implicam $(E+F)[f] \xrightarrow{y} G$. Novamente é o par (G,G) que tem de ser adicionado a R. Concluímos então que os pares a adicionar a R para a tornar uma bissimulação são sempre pares reflexivos. Basta, pois, reunir R com a relaçao identidade Id para obter uma bissimulação, o que conclui a prova.

2. Que condição que deverá ser imposta à função f de modo a garantir a validade da equação
   $$(E \mid F)[f] \sim E[f] \mid F[f]$$
   Sugestão: Comece por identificar um contraexemplo, i.e. um par de processos e uma função f que não satisfaçam a igualdade em causa.

   Sugestão de resolução

   Considere-se $A \triangleq a.A$ e $B \triangleq \overline{b}.B$, assim como a seguinte renomeação $f = [a \mapsto c, b \mapsto c]$. Claramente os processos
   $$(A \mid B)[f] \;\text{ e }\; A[f] \mid B[f]$$
   não são bisimilares: o segundo processo, ao contrário do primeiro, pode realizar τ (por sincronização de c e $\overline{c}$). Este exemplo sugere que a equação será válida sempre que a renomeação f seja uma função injectiva.

Questão 3

Considere dois processos, P e Q, com imagem finita. Suponha que P satisfaz qualquer fórmula expressa na lógica de Hennessy-Milner que seja igualmente satisfeita por Q, e vice-versa. Será possível deduzir desse facto que qualquer fórmula expressa em μ-calculus modal que seja satisfeita por um dos processos é-o também pelo outro? Justifique adequadamente a sua resposta.

Sugestão de resolução

Se os processos P e Q têm imagem finita e são modalmente equivalentes, i.e. satisfazem exactamente as mesmas fórmulas expressas na lógica de Hennessy-Milner, então o teorema da equivalência modal para essa lógica permite concluir que P e Q são estritamente bissimilares. O μ-calculus modal satisfaz igualmente um teorema deste tipo: dois processos com imagem finita são bissimilares sse satisfizerem as mesmas fórmulas expressas no μ-calculus modal. Logo P e Q verificam exactamente as mesmas fórmulas nesta segunda lógica. Note-se que este resultado é independente que qualquer consideração sobre o poder expressivo das duas lógicas.

Questão 4

Como sabe, qualquer porta quântica unária Q origina uma porta binária C_Q em que a aplicação de Q ao segundo qubit é condicionada pelo valor do primeiro qubit. O operador correspondente pode ser escrito como

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

1. Mostre que o operador C_Q é unitário sempre que Q o fôr.

   Sugestão de resolução

   É necessário mostrar que $C_Q C_Q^\dagger = I$. Desenrolando a definição de C_Q e notando que $(U \otimes V)^\dagger = U^\dagger \otimes V^\dagger$, obtemos

   $$C_Q C_Q^\dagger \;=\; (I \otimes Q^x)(I \otimes Q^x)^\dagger \;=\; (I \otimes Q^x)(I \otimes (Q^x)^\dagger)$$

   Para $x = 0$: $(I \otimes Q^0)(I \otimes (Q^0)^\dagger) \;=\; I \otimes I \;=\; I$.
   Para $x = 1$: $(I \otimes Q)(I \otimes Q^\dagger) \;=\; I \otimes (QQ^\dagger) \;=\; I \otimes I \;=\; I$, assumindo Q unitário.

2. 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

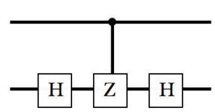
   A representação matricial de $Z = |0\rangle\langle 0| - |1\rangle\langle 1|$ é a matriz

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

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

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

3. O circuito seguinte implementa o operador $CNOT$ que constitui a versão controlada da porta X.

   Preencha as reticências na seguinte prova desse facto, completando de forma clara e completa as justificações de cada passo.

   $$\begin{aligned}
   & CNOT|x\rangle|y\rangle \\
   = & \quad \{ \; \cdots \; \} \\
   & |x\rangle \otimes X^x|y\rangle \\
   = & \quad \{ \; X = HZH \; \} \\
   & |x\rangle \otimes (HZH)^x|y\rangle \\
   = & \quad \{ \; \cdots \; \} \\
   & |x\rangle \otimes HZ^xH|y\rangle \\
   = & \quad \{ \; \cdots \; \} \\
   & I \otimes H \cdot C_Z \cdot I \otimes H
   \end{aligned}$$

   Sugestão de resolução

Primeiro passo: Definição de $CNOT$.
Segundo passo: Apesar de x tomar apenas os valores 0 ou 1, este passo é válido para qualquer x, usando $H = H^\dagger$ e H unitário. De facto, $\cdots(HZH)(HZH)\cdots = \cdots HZ(HH)ZH\cdots = \cdots HZZH\cdots$.
Terceiro passo: $I \otimes (HZ^xH) = (I \otimes H)(I \otimes Z^x)(I \otimes H)$ e definição de C_Z.

Questão 5

Em alguns textos de divulgação científica o sucesso do algoritmo de Grover é explicado por um fenómeno referido como *paralelismo quântico* que funcionaria do modo seguinte: *verificar todos os possíveis valores em paralelo e a seguir compara-los para determinar a solução.* Explique porque razão esta explicação é falaciosa e não exprime correctamente o comportamento dos algoritmos quânticos.

Sugestão de resolução

Questão aberta a explorar por cada aluno. O ponto essencial será referir que a medição de um estado quântico provoca o seu colapso, o que torna impossível uma estratégia *naíve* que procurasse calcular todas as soluções e escolher a melhor.