



1 Introdução

Considere a seguinte especificação de um processo que emula um contador, em termos de três acções: up (incremento), dw (decremento) e zr (teste para o valor 0):

$$\begin{aligned} Ct_0 &\triangleq up.Ct_1 + zr.Ct_0 \\ Ct_n &\triangleq up.Ct_{n+1} + dw.Ct_{n-1} \quad \text{para } n > 0 \end{aligned}$$

Uma possível implementação distribuída deste contador pode ser obtida pela composição paralela de pequenas células — processos do tipo C — cada uma das quais representa uma unidade. As células tem capacidade de se multiplicarem em resposta a uma operação de incremento assim como de se extinguirem na ocorrência de um decremento. Cada uma dispõe de duas portas auxiliares (\bar{d} e \bar{z}) usadas para propagação dos decrementos. O número 0 é representado por uma célula especial — o processo Z — que não admite a realização de decrementos, e, portanto, não tem as portas auxiliares referidas. O essencial na dinâmica destes processos é a estrutura de sincronizações que, para melhorar a legibilidade, se abreviou sob a forma de um operador derivado (\frown). Temos, pois,

$$\begin{aligned} C &\triangleq up.(C \frown C) + dw.P \\ P &\triangleq \bar{d}.C + \bar{z}.Z \\ Z &\triangleq up.(C \frown Z) + zr.Z \end{aligned}$$

onde o operador \frown se define como

$$\begin{aligned} E \frown F &= (\{u'/u, z'/z, d'/d\} E \mid \{u'/up, z'/zr, d'/dw\} F) \setminus A \\ \text{onde } A &= \{u', z', d'\} \end{aligned}$$

Note-se que não sendo u uma acção de E , a sua renomeação não tem significado. Por outro lado, no processo F , ao renomearmos up para u' e posteriormente incluirmos u' no conjunto das restrições, estamos a tornar interna a porta up do segundo operando de \frown , i.e. a impedir a sua utilização pelo exterior.

O número de células C activas depende do estado corrente da contagem. Inicialmente o contador pode ser inicializado a 0, caso em que é representado pelo processo $C^0 \triangleq Z$. No caso geral, representamos o estado do contador associado ao número n pelo processo $C^n \triangleq C \frown C \frown C \frown \dots \frown Z$, com exactamente n células C . A análise de algumas transições típicas ajudará a perceber a dinâmica do sistema. Note-se que a célula mais externa pode realizar um incremento ao mesmo tempo que um decremento se propaga nas células interiores.

- $C^0 = Z \xrightarrow{up} C \frown Z$.
- $C^1 = C \frown Z \xrightarrow{dw} (\bar{d}.C + \bar{z}.Z) \frown Z$. A partir daqui há apenas uma hipótese: uma transição invisível que corresponde à sincronização de \bar{z} com zr . Temos, então, $(\bar{d}.C + \bar{z}.Z) \frown Z \xrightarrow{\tau} Z \frown Z$. Mas $Z \frown Z = Z$, porque

$$\begin{aligned}
Z \frown Z &= (\{u'/u, z'/z, d'/d\} Z \mid \{u'/up, z'/zr, d'/dw\} Z) \setminus A \\
&= (\{u'/u, z'/z, d'/d\} Z) \setminus A \mid (\{u'/up, z'/zr, d'/dw\} Z) \setminus A \\
&= Z \mid \mathbf{0} \\
&= Z
\end{aligned}$$

- $C^2 = C \frown C \frown Z \xrightarrow{dw} (\bar{d}.C + \bar{z}.Z) \frown C \frown Z$. Agora a única possível transição é a sincronização de \bar{d} com dw , que origina uma transição por τ para $C \frown (\bar{d}.C + \bar{z}.Z) \frown Z$. De seguida $C \frown (\bar{d}.C + \bar{z}.Z) \frown Z \xrightarrow{\tau} C \frown Z \frown Z$ e, como vimos acima, $C \frown Z \frown Z = C \frown Z = C^1$.

2 Questões

1. Especifique este processo em mCRL2 e utilize as diferentes funcionalidades da ferramenta para observar o seu comportamento para diferentes valores de n . No relatório deve indicar claramente que ferramentas utilizou e porquê, anexando os resultados e printouts do écran que tiver obtido.
2. Mostre que $C^m = Ct_m$ para qualquer inteiro m . A prova deverá ser apresentada com o máximo detalhe e indicando sempre a razão que justifica cada passo.
3. Será que a ferramenta mCRL2 poderia ser utilizada para responder à pergunta anterior de forma automática ou semi-automática? Em caso afirmativo, faça-o e indique como procedeu e porquê. Em caso negativo, justifique.
4. Formule nas lógicas de processos que estudou (lógica de Hennessy-Milner e o μ -calculus modal) três propriedades de segurança e três propriedades de animação sobre o processo C^m . Verifique-as
 - (a) manualmente,
 - (b) por recurso ao mCRL2.
5. Especifique um processo que implemente uma *fila de espera* com as três acções habituais (*enqueue*, *dequeue* e *empty*), baseado na composição paralela de processos C capazes de armazenarem, cada um, um elemento da fila. Como no caso do contador, cada C dispõe de duas portas adicionais (\bar{e} e o) para propagação de valores ao longo da cadeia (só que agora as duas portas auxiliares têm sentidos de comunicação opostos entre si!). Igualmente deve introduzir um processo próprio (Z) para representar a fila vazia.
 - (a) Especifique este processo em mCRL2.
 - (b) Formule nas lógicas de processos que estudou duas propriedades de segurança e duas propriedades de animação sobre esse processo e verifique-as por recurso à ferramenta mCRL2.