4 Sistema dedutivo

4.1 Introdução

A lógica temporal, para além de poder ser utilizada para especificar sistemas concorrentes e reactivos, tal como se ilustrou no capítulo anterior, pode também ser utilizada para especificar propriedades sobre estes sistemas, como por exemplo *propriedades de invariância*, *animação* , *resposta*, etc….

Estas propriedades podem ser divididas em classes, segundo uma certa hierarquia ([Manna e Pnueli 90], [Manna e Pnueli 91b]). Neste capítulo consideram-se, no entanto, apenas duas dessas classes de propriedades: a classe relativa a *propriedades de invariância* (também chamadas *propriedades de segurança*) e a classe relativa a *propriedades de resposta* .

Pretende-se então introduzir um sistema dedutivo para raciocinar sobre especificações GCL, munido de um conjunto de regras que permitam estabelecer as propriedades referidas.

Com generalidade, um sistema dedutivo é composto por um conjunto de axiomas e por um conjunto de regras de inferência. Uma fórmula φ diz-se teorema nesse sistema dedutivo (o que se denota por $\vdash \varphi$), se puder ser obtida do conjunto de axiomas por aplicação das regras de inferência (cf. por exemplo [Enderton 72]).

No caso da Lógica de Certificação GNOME, as coisas não são assim tão simples. Ao tentar definir um sistema dedutivo para esta lógica, não basta escrever $\vdash \varphi$ para indicar que a fórmula φ é teorema. É necessário indicar também em que classe (de

uma certa especificação de comunidade de objectos) esta fórmula é teorema. Torna-se, então, necessário enriquecer a notação, passando a escrever $\vdash_c^{eco} \varphi$ para indicar que a fórmula φ é teorema da classe c, no contexto da especificação de comunidade de objectos *eco*. Assim, os axiomas e regras de inferência devem ser definidos para classes, no contexto de uma comunidade de objectos.

A notação escolhida para apresentar o sistema dedutivo foi a seguinte:

- axiomas:

$$\frac{}{\vdash_c^{eco} \varphi}$$

em que a fórmula φ se diz um axioma para a classe c, no contexto da especificação *eco*;

- regras de inferência:

$$\frac{\vdash_{c_1}^{eco} \varphi_1 \ \ldots \ \vdash_{c_n}^{eco} \varphi_n}{\vdash_c^{eco} \varphi}$$

em que $\vdash_{c_1}^{eco} \varphi_1 \ldots \vdash_{c_n}^{eco} \varphi_n$ se dizem as premissas da regra e $\vdash_c^{eco} \varphi$ se diz a conclusão da regra.

4.2 Axiomatização

Nesta secção apresenta-se um sistema dedutivo para GCL, adaptando alguns dos resultados apresentados em [Sernadas e Sernadas 94] para OSL.

Assume-se, de agora em diante, fixada uma especificação de comunidade de objectos $eco=\langle \Sigma, Ax \rangle$. No contexto desta especificação, a notação pode ser simplificada, passando a denotar-se a relação de demonstração por $\vdash_c$, em vez de $\vdash_c^{eco}$.

4.2.1 Axiomas

Nesta secção introduz-se o conjunto de axiomas básicos para o sistema dedutivo.

Definição 4.1 *Axiomas da especificação*

AX. $$\frac{}{\vdash_c \varphi}$$

para cada $\varphi \in Ax^c$. □

Estes axiomas resultam da especificação da classe.

Definição 4.2 *Axiomas de lógica temporal*

LPO. $\dfrac{}{\vdash_c x.q}$

para cada axioma q da lógica temporal linear, de primeira ordem, com igualdade. □

Para mais detalhes ver [Sernadas et al 92e], [Manna e Pnueli 91a], [Enderton 72] e [Goldblat 87].

Definição 4.3 *Tipos de dados*

TD. $\dfrac{}{\vdash_c x.q}$

desde que q seja uma fórmula de tipos de dados rígida, tal que θ, $td \Vdash q$, qualquer que seja a atribuição θ . □

Este conjunto de axiomas, *importa* todas as fórmulas válidas na álgebra de tipos de dados subjacente.

Definição 4.4 *Axiomas sobre acções*

AC1. $\dfrac{}{\vdash_c x.((z(x_1,\ldots,x_n)=z(x'_1,\ldots,x'_n)) \Rightarrow ((x_1=x'_1) \wedge \ldots \wedge (x_n=x'_n)))}$

para cada $z \in ACC^c_{g_1\ldots g_n,g}$;

AC2. $\dfrac{}{\vdash_c x.(\neg(z(x_1,\ldots,x_n)=z'(x'_1,\ldots,x'_{n'})))}$

para cada $z \in ACC^c_{g_1\ldots g_n,g}$, $z' \in ACC^c_{g'_1\ldots g'_n,g'}$ e $z \neq z'$;

AC3. $\dfrac{}{\vdash_c x.(\forall y(\forall_{g_1\ldots g_n \in G_N^*} (\forall_{z \in ACC^c_{g_1\ldots g_n,g}} (\exists y_1(\ldots(\exists y_n(y=z(y_1,\ldots,y_n)))\ldots)))))}$

para cada género $g \in G^{\tau}_N$. □

Estes axiomas dão uma caracterização do conjunto $\mathcal{P}op_{\tau_c}$, e traduzem o facto de as acções não serem interpretadas e serem geradas.

Definição 4.5 *Axiomas sobre vidas*

VID1. $$\frac{}{\vdash_c x.\Diamond(\bot)}$$

desde que $c \in$ CP;

VID2. $$\frac{}{\vdash_c x.((\nabla=\bot)\Rightarrow((a(x_1,\ldots,x_n)=y)\Rightarrow(\mathbf{X}(a(x_1,\ldots,x_n)=y))))}$$

desde que $c \in$ CP, $a \in ATR^{c}_{g_1\ldots g_n,g}$ e $a \neq \nabla$;

VID3. $$\frac{}{\vdash_c x.((\nabla=z(x_1,\ldots,x_n))\Rightarrow\Diamond(z(x_1,\ldots,x_n)))}$$

desde que $c \in$ CP, $z \in ACC^{c}_{g_1\ldots g_n,g}$. □

Estes axiomas traduzem as propriedades da vida de uma classe. Assim, VID1 reflecte o facto de a acção $\bot$ estar sempre activada. VID2 reflecte o facto de os atributos manterem o seu valor (exceptuando o atributo ∇) quando a acção $\bot$ ocorre. VID3 traduz o facto de uma acção só poder ocorrer quando estiver activada.

Definição 4.6 *Axiomas sobre o ambiente*

AMB1. $$\frac{}{\vdash_c x.(\neg\beta_{c',z}(\sigma(x),x_1,\ldots,x_n))}$$

desde que $\sigma:c\rightarrow c'$ seja um morfismo de classes e $z \in ACC^{c'}_{g_1\ldots g_n,\tau_{c'}}$;

AMB2. $$\frac{}{\vdash_c x.(\neg\beta_{c',z}(0,x_1,\ldots,x_n))}$$

para $z \in ACC^{c'}_{g_1\ldots g_n,\tau_{c'}}$. □

Estes axiomas traduzem as propriedades específicas do ambiente, em particular aquelas que se referem aos contextos adimissíveis. Assim, AMB2 reflecte o facto de uma instância não poder chamar um serviço de si própria. AMB3 exprime o facto de nenhum serviço da instância 0 de qualquer classe estar activado.

Definição 4.7 *Composição de morfismos*

POP. $$\frac{}{\vdash_c x.(\mu_n(\ldots(\mu_1(y))\ldots)=\mu(y))}$$

desde que $\mu=\mu_n\circ\ldots\circ\mu_1$. □

O axioma POP captura uma propriedade do functor população: a composicionalidade de morfismos.

4.2.2 Regras de inferência

Para terminar a definição do sistema dedutivo, apresenta-se, nesta secção, um conjunto de regras de inferência. Mais tarde, este conjunto de regras será estendido de modo a incluir regras para raciocinar sobre propriedades mais específicas.

Definição 4.8 *Modus Ponens*

MP. $$\frac{\vdash_c x.q \qquad \vdash_c x.(q \Rightarrow q')}{\vdash_c x.q'}$$

para $q,q' \in Q^c$. □

Definição 4.9 *Herança*

HER. $$\frac{\vdash_c \varphi}{\vdash_{c'} \sigma_L(\varphi)}$$

desde que $\sigma:c' \rightarrow c$ seja um morfismo de classes, e $\varphi \in L^c$. □

Esta regra relaciona-se com a herança de propriedades. Assim, se uma fórmula φ for teorema de uma dada classe c, e se existir um morfismo de classes $\sigma:c' \rightarrow c$, então a tradução da fórmula φ em c' será um teorema desta classe.

Definição 4.10 *Reflexão*

REF. $$\frac{\vdash_{c_1 \otimes \ldots \otimes c_n} \pi_{iL}(\varphi)}{\vdash_{c_i} \varphi}$$

para $i=1,\ldots,n$, e $\varphi \in L^{c_i}$. □

Esta regra corresponde à reflexão de uma propriedade de uma agregação nas classes que a compõem.

Note-se que as regras HER e REF combinadas dão origem ao seguinte resultado:

$\vdash_{c_1 \otimes \ldots \otimes c_n} \pi_{i_L}(\varphi)$ sse $\vdash_{c_i} \varphi$, qualquer que seja $\varphi \in L^{c_i}$.

4.2.3 Derivações

Com base no sistema dedutivo introduzido, apresentam-se agora os conceitos usuais de teorema e derivação.

Definição 4.11 *Teorema*

Seja $\varphi \in L^c$. Então a fórmula φ diz-se *teorema* de *eco* sse $\vdash_c^{eco} \varphi$. □

Definição 4.12 *Derivação*

Seja $H=\{H^c\}_{c \in |\mathcal{C}_N|}$ tal que $H^c \subseteq L^c$. O *conjunto de fórmulas derivadas* em c, a partir de H, que se denota por $Ax^{H \vdash_c^{eco}}$, define-se indutivamente do seguinte modo:

- se $\vdash_c^{eco} \varphi$ então $\varphi \in Ax^{H \vdash_c^{eco}}$;
- se $\varphi \in H^c$ então $\varphi \in Ax^{H \vdash_c^{eco}}$;
- se $x.q \in Ax^{H \vdash_c^{eco}}$ e $x.(q \Rightarrow q') \in Ax^{H \vdash_c^{eco}}$ então $x.q' \in Ax^{H \vdash_c^{eco}}$.

Os conjuntos $Ax^{H \vdash_c^{eco}}$ formam uma família indexada $Ax^{H \vdash^{eco}} = \{Ax^{H \vdash_c^{eco}}\}_{c \in |\mathcal{C}_N|}$, que se diz a *consequência* de H em *eco*.

Uma fórmula $\varphi \in Ax^{H \vdash_c^{eco}}$ diz-se *derivada* a partir de H em *eco*, o que se denota por $H \vdash_c^{eco} \varphi$. □

4.2.4 Correcção

Nesta secção prova-se que o sistema dedutivo apresentado é correcto face a semântica introduzida no capítulo anterior.

Proposição 4.13 *Correcção dos teoremas*

Seja *eco* uma especificação de comunidade de objectos. Então os teoremas de *eco* são *correctos*, i.e., se $\vdash_c^{eco} \varphi$ então $\vdash_c^{eco} \varphi$, qualquer que seja a classe $c \in |\mathcal{C}_N|$ e $\varphi \in L^c$.

prova:

Por definição, provar $\vdash_c^{eco} \varphi$ consiste em provar que $\varphi \in Ax^{\vdash_c}$, ou seja, que se $co \Vdash Ax$ então $co \Vdash_c \varphi$. Para provar o resultado enunciado basta provar que *os axiomas são correctos* (i.e., dado o axioma

$$\frac{}{\vdash_c \varphi}$$

é necessário provar que $\vdash_c^{eco} \varphi$), e que *as regras de inferência são correctas* (i.e., dada a regra de inferência

$$\frac{\vdash_{c_1} \varphi_1 \ \ldots \ \vdash_{c_n} \varphi_n}{\vdash_c \varphi}$$

é necessário provar que se $\vdash_{c_1}^{eco} \varphi_1, \ldots, \vdash_{c_n}^{eco} \varphi_n$ então $\vdash_c^{eco} \varphi$).

(i) *os axiomas são correctos*

- (AX) Seja $\varphi \in Ax^c$. Então, resulta da definição de fecho por consequência que

$\varphi \in Ax^{\vDash_c}$.

- (LT) Resulta da correcção do sistema dedutivo apresentado para a lógica temporal.
- (TD) Apenas se tomam como teoremas, as fórmulas válidas.
- (AC1) Sejam θ uma atribuição, $k \in \mathbb{N}_0$, $u \in \mathcal{P}op_c$ e Ω um contexto de *co* quaisquer. Suponha-se que $\theta_c(x)=u$ e que $\theta, k, u, \Omega, co \Vdash_c z(x_1,\ldots,x_n)=z(x'_1,\ldots,x'_n)$. Então $[\![z(x_1,\ldots,x_n)]\!]^{\theta}_{k,u,co}=[\![z(x'_1,\ldots,x'_n)]\!]^{\theta}_{k,u,co}$, e, por definição de interpretação de termos, $[z([\![x_1]\!]^{\theta}_{k,u,co},\ldots,[\![x_n]\!]^{\theta}_{k,u,co})]=[z([\![x'_1]\!]^{\theta}_{k,u,co},\ldots,[\![x'_n]\!]^{\theta}_{k,u,co})]$. Por definição de conjunto de acções, $[\![x_i]\!]^{\theta}_{k,u,co}=[\![x'_i]\!]^{\theta}_{k,u,co}$, para $i=1,\ldots,n$, e portanto $\theta, k, u, \Omega, co \Vdash_c ((x_1=x'_1) \wedge \ldots \wedge (x_n=x'_n))$, o que permite concluir que $co \Vdash_c x.((z(x_1,\ldots,x_n)=z(x'_1,\ldots,x'_n)) \Rightarrow ((x_1=x'_1) \wedge \ldots \wedge (x_n=x'_n)))$, ou seja

  $x.((z(x_1,\ldots,x_n)=z(x'_1,\ldots,x'_n)) \Rightarrow ((x_1=x'_1) \wedge \ldots \wedge (x_n=x'_n))) \in Ax^{\vDash_c}$.

- (AC2) A prova é semelhante à anterior e resulta das definições de interpretação e de conjunto de acções.
- (AC3) Sejam θ uma atribuição, $k \in \mathbb{N}_0$, $u \in \mathcal{P}op_c$ e Ω um contexto de *co* quaisquer. Suponha-se que $\theta_c(x)=u$. Por hipótese, tem-se que $g \in G^{\tau}_N$, logo, para que a fórmula seja bem formada é necessário que $y \in X_g$.

  Seja agora θ^0 uma atribuição y-equivalente a θ. Pretende-se provar que

  $$\theta^0, k, u, \Omega, co \Vdash_c (\forall_{g_1\ldots g_n \in G_N^*} (\forall_{z \in ACC^c_{g_1\ldots g_n,g}} (\exists y_1 \ldots (\exists y_n (y=z(y_1,\ldots,y_n))) \ldots))). \quad (1)$$

  Por definição de $\mathcal{P}op_g$, com $g \in G^{\tau}_N$, sabe-se que $\theta^0_g(y)=[z(u_1,\ldots,u_n)]$ para algum $z \in ACC^c_{g_1\ldots g_n,g}$ e $u_i \in \mathcal{P}op_{g_i}$, para $i=1,\ldots,n$. Defina-se agora uma atribuição θ^1, y_1-equivalente a θ^0, tal que $\theta^1_{g_1}(y_1)=u_1$. Com base nesta definição defina-se uma atribuição θ^2, y_2-equivalente a θ^1, tal que $\theta^2_{g_2}(y_2)=u_2$. E assim sucessivamente.

  Note-se que, a atribuição θ^n é tal que $\theta^n_{g_i}(y_i)=u_i$ e $\theta^n_g(y)=[z(u_1,\ldots,u_n)]$. Então, é fácil concluir que $\theta^n, k, u, \Omega, co \Vdash_c (y=z(y_1,\ldots,y_n))$. Como θ^n é y_n-equivalente a θ^{n-1}, resulta que $\theta^{n-1}, k, u, \Omega, co \Vdash_c (\exists y_n (y=z(y_1,\ldots,y_n)))$. Repetindo este argumento sucessivamente, conclui-se que $\theta^0, k, u, \Omega, co \Vdash_c (\exists y_1 \ldots (\exists y_n (y=z(y_1,\ldots,y_n))) \ldots)$, para algum $z \in ACC^c_{g_1\ldots g_n,g}$ e $g_1\ldots g_n \in G_N^*$. Ou seja, a condição (1) verifica-se. Como θ^0 é uma atribuição qualquer, y-equivalente a θ, conclui-se que

  $$\theta, k, u, \Omega, co \Vdash_c (\forall y (\forall_{g_1\ldots g_n \in G_N^*} (\forall_{z \in ACC^c_{g_1\ldots g_n,g}} (\exists y_1 \ldots (\exists y_n (y=z(y_1,\ldots,y_n))) \ldots))))$$

  e portanto $x.(\forall y (\forall_{g_1\ldots g_n \in G_N^*} (\forall_{z \in ACC^c_{g_1\ldots g_n,g}} (\exists y_1 \ldots (\exists y_n (y=z(y_1,\ldots,y_n))) \ldots)))) \in Ax^{\vDash_c}$.

- (VID1) Sejam θ uma atribuição, $k \in \mathbb{N}_0$, $u \in \mathcal{P}op_c$ e Ω um contexto de *co* quaisquer, e suponha-se que $\theta_c(x)=u$. Por definição de vida de uma classe, sabe-se que $p_{\Diamond(\perp)}(\Lambda(\langle c,u \rangle)_{2,k})=true_{dt}$. Então, $[\![\Diamond(\perp)]\!]^{\theta}_{k,u,co}=true_{dt}$, o que implica que $\theta, k, u, \Omega, co \Vdash_c \Diamond(\perp)$. Conclui-se então que $co \Vdash_c x.\Diamond(\perp)$ e portanto $x.\Diamond(\perp) \in Ax^{\vDash_c}$.

- (VID2), (VID3) A prova é semelhante à anterior e resulta da definição de vida de uma classe.
- (AMB1), (AMB2) A prova é semelhante à realizada para VID1, e resulta da definição de contexto de comunidade e de contexto admissível.
- (POP) Resulta trivialmente do facto de $\mathcal{P}op$ ser um functor e portanto preservar composição de morfismos.

(ii) *as regras de inferência são correctas*

- (MP) Suponha-se que $x.q \in Ax^{\models c}$ e $x.(q \Rightarrow q') \in Ax^{\models c}$, ou seja, $co \Vdash_c x.q$ e $co \Vdash_c x.(q \Rightarrow q')$. Sejam θ uma atribuição, $k \in \mathbb{N}_\circ$, $u \in \mathcal{P}op_c$ e Ω um contexto de co quaisquer, e suponha-se que $\theta_c(x)=u$. Por hipótese $\theta,k,u, \Omega, co \Vdash_c q$ e $\theta,k,u, \Omega, co \Vdash_c (q \Rightarrow q')$, logo $\theta, k,u,\Omega, co \Vdash_c q'$, o que permite concluir que $co \Vdash_c x.q'$ e portanto $x.q' \in Ax^{\models c}$.
- (HER) Suponha-se que $\varphi \in Ax^{\models c}$ e seja $u' \in \mathcal{P}op_{c'}$. Então, por hipótese, $\theta,k,\mathcal{P}op(\sigma)(u'),\Omega,co \Vdash_c \varphi$, quaisquer que sejam a atribuição θ, $k \in \mathbb{N}_\circ$ e o contexto de co Ω. Aplicando o lema **3.50** conclui-se que $\theta,k,u', \Omega, co \Vdash_{c'} \sigma_L(\varphi)$, quaisquer que sejam a atribuição θ e $k \in \mathbb{N}_\circ$. Então $co \Vdash_{c'} \sigma_L(\varphi)$, ou seja $\sigma_L(\varphi) \in Ax^{\models c'}$.
- (REF) Suponha-se que $\pi_{iL}(\varphi) \in Ax^{\models c_1 \otimes \ldots \otimes c_n}$ e seja $u_i \in \mathcal{P}op_{c_i}$. Defina-se ainda $u \in \mathcal{P}op_{c_1 \otimes \ldots \otimes c_n}$ tal que $\mathcal{P}op(\pi_i)(u)=u_i$[1]. Por hipótese, $\theta,k,u,\Omega, co \Vdash_{c_1 \otimes \ldots \otimes c_n} \pi_{iL}(\varphi)$, quaisquer que sejam a atribuição θ, $k \in \mathbb{N}_\circ$ e o contexto de co Ω. Pelo lema **3.50** conclui-se que $\theta,k,u_i,\Omega, co \Vdash_{c_i} \varphi$, quaisquer que sejam a atribuição θ e $k \in \mathbb{N}_\circ$. Então $co \Vdash_{c_i} \varphi$, ou seja $\varphi \in Ax^{\models c_i}$. □

A correcção do sistema dedutivo resulta trivialmente do resultado anterior, juntamente com a noção de derivação.

Teorema 4.14 *Correcção*

Seja eco uma especificação de comunidade de objectos, $H=\{H^c\}_{c \in |\mathcal{C}_N|}$ tal que $H^c \subseteq L^c$, $c \in |\mathcal{C}_N|$ e $\varphi \in L^c$. Se $H \vdash_c^{eco} \varphi$ então $H \models_c^{eco} \varphi$.

prova:

A prova deste teorema resulta da proposição anterior. □

4.2.5 Meta-teoremas

Muitas vezes, o cálculo de Hilbert pode ser tornado mais prático recorrendo ao uso de meta-teoremas. Introduzem-se, por isso, os dois meta-teoremas seguintes.

---

[1] Da definição de $\mathcal{P}op_{c_1 \otimes \ldots \otimes c_n}$ é fácil encontrar $u \in \mathcal{P}op_{c_1 \otimes \ldots \otimes c_n}$ tal que $\mathcal{P}op(\pi_i)(u)=u_i$.

Teorema 4.15 *Meta-teorema da dedução*

Sejam $H=\{H^c\}_{c\in|\mathcal{C}_N|}$ tal que $H^c\subseteq L^c$, $q,q' \in Q^c$ e $x\in X_c$. Então,

DED. $$\frac{H\cup\{x.q\}\vdash_c x.q'}{H\vdash_c x.(q\Rightarrow q')}$$

□

Teorema 4.16 *Meta-teorema da redução ao absurdo*

Sejam $H=\{H^c\}_{c\in|\mathcal{C}_N|}$ tal que $H^c\subseteq L^c$, $q,q' \in Q^c$ e $x\in X_c$. Então,

ABS. $$\frac{H\cup\{x.q\}\vdash_c x.q' \quad H\cup\{x.q\}\vdash_c x.(\neg q')}{H\vdash_c x.(\neg q)}$$

□

A prova de correcção destes meta-teoremas é clássica Veja-se, para um sistema dedutivo semelhante, [Enderton 72]. Note-se a importância de só admitir *Modus Ponens* sobre os elementos de H, na definição de derivação (com generalidade, os meta-teoremas apresentados apenas podem ser aplicados se não tiver sido aplicada nenhuma regra de necessitação sobre as hipóteses - cf. por exemplo [Hamilton 78]).

De agora em diante, ao apresentar derivações, não se apresentarão os detalhes sobre raciocínio em lógica temporal de primeira ordem, desde que regras sobre necessitação (para os quantificadores) não tenham sido aplicadas.

Em [Sernadas e Sernadas 94] apresenta-se ainda uma regra que permite combinar axiomas locais.

Notação:

Seja $z\in ACC^c_{g_1\ldots g_n,g}$ uma acção qualquer. Utiliza-se o termo $z(y_i)$ como abreviatura do termo $z(y_1,\ldots y_n)$. □

Teorema 4.17 *Regra de combinação*

COMB.

$$\frac{\vdash_{c_i} x_i.(((\nabla=z_i(y_i))\wedge A_i[{}^{a_i}_{t_i}])\Rightarrow(\mathbf{X}A_i)),\ \text{para } i=1,\ldots,m}{\vdash_{c_1\otimes\ldots\otimes c_m} x.((\bigwedge_{i=1}^{m}(\nabla_i=\pi_i(z_i)(y_i))\wedge B[{}^{\pi_1(a_1)}_{\pi_1(t_1)}]\ldots[{}^{\pi_m(a_m)}_{\pi_m(t_m)}])\Rightarrow(\mathbf{X}B))}$$

para cada $B\in CE^{c_1\otimes\ldots\otimes c_m}$, em que $A_i\in CE^{c_i}$, para i=1,…m.

prova *(esboço)*:

Suponha-se que c_i tem apenas dois atributos simples, a_i e b_i, para i=1,…,m.

A fórmula

$$\vdash_{c_i} x_i.(((\nabla=z_i(y_i)) \wedge A_i[{}^{a_i}_{t_i}]) \Rightarrow (\mathbf{X}A_i)) \qquad (1_i)$$

dá origem às fórmulas:

$$\vdash_{c_i} x_i.(\forall k\ (((\nabla=z_i(y_i)) \wedge a_i=k) \Rightarrow (\mathbf{X}(a_i=t_i[{}^{a_i}_{k}])))); \qquad (2_i)$$

$$\vdash_{c_i} x_i.(\forall k\ (((\nabla=z_i(y_i)) \wedge b_i=k) \Rightarrow (\mathbf{X}(b_i=k)))); \qquad (3_i)$$

Prova-se, por indução da estrutura da fórmula A_i, que as fórmulas (2_i) e (3_i) dão origem à fórmula (1_i).

As fórmulas (2_i) e (3_i) dão origem às seguintes fórmulas, em $c_1 \otimes \ldots \otimes c_m$:

$$\vdash_{c_1\otimes\ldots\otimes c_m} x.(\forall k\ (((\nabla_i=z_i(y_i)) \wedge \pi_i(a_i)=k) \Rightarrow (\mathbf{X}(\pi_i(a_i)=\pi_i(t_i[{}^{a_i}_{k}])))); \qquad (4_i)$$

$$\vdash_{c_1\otimes\ldots\otimes c_m} x.(\forall k\ (((\nabla_i=z_i(y_i)) \wedge \pi_i(b_i)=k) \Rightarrow (\mathbf{X}(\pi_i(b_i)=k)))); \qquad (5_i)$$

Repare-se agora que qualquer fórmula $B \in CE^{c_1\otimes\ldots\otimes c_m}$ apenas pode envolver imagens de atributos simples de cada uma das classes c_i. Prova-se, por indução na estrutura de B, que as fórmulas (4_i) e (5_i) dão origem à fórmula

$$\vdash_{c_1\otimes\ldots\otimes c_m} x.((\wedge_{i=1}^{m}(\nabla_i=\pi_i(z_i)(y_i)) \wedge B[{}^{\pi_1(a_1)}_{\pi_1(t_1)}]\ldots[{}^{\pi_m(a_m)}_{\pi_m(t_m)}]) \Rightarrow (\mathbf{X}B)) \qquad (6)$$

□

Assume-se que a_i (na premissa da regra) representa os atributos da classe c_i, seguindo uma notação semelhante à utilizada no caso dos parâmetros das acções.

Exemplo 4.18 *Utilizadores e relógios*

Recordem-se as especificações das classes *Utilizador* e *Relógio*. Recorrendo ao axioma AX, conclui-se que:

1. $\vdash_R (((r.\nabla = novo) \wedge (A_1[{}^{r.tempo}_{0}]\,[{}^{r.ph}_{AN}])) \Rightarrow (\mathbf{X}A_1))$
2. $\vdash_U (((u.\nabla = novo) \wedge (A_2[{}^{u.ta}_{0}]\,[{}^{u.tp}_{0}]\,[{}^{u.sit}_{pobre}]\,[{}^{u.ph}_{AN}])) \Rightarrow (\mathbf{X}A_2))$

quaisquer que sejam $A_1 \in CE^R$ e $A_2 \in CE^U$. A regra COMB permite concluir que

3. $\vdash_{U\otimes R} ((x.\nabla_r=novo_r) \wedge (x.\ \nabla_u=novo_u) \wedge$
   $B[{}^{x.tempo_r}_{0}]\,[{}^{x.ph_r}_{AN}][{}^{x.ta_u}_{0}]\,[{}^{u.tp_u}_{0}]\,[{}^{x.sit_u}_{pobre}]\,[{}^{x.ph_u}_{AN}]) \Rightarrow (\mathbf{X}B))$

qualquer que seja $B \in CE^{U\otimes R}$.

A fórmula *3* caracteriza o efeito conjunto das acções *novo* e *novo*, das classes *Relógio* e *Utilizador*, respectivamente, sobre constrangimentos de estado da classe

Relógio ⊗Utilizador. Esta fórmula será utilizada no exemplo **4.21**. □

4.3 Cálculo de invariância

Em geral, uma *fórmula de invariância* é da forma ($\mathbf{G}_0$A), em que A é um constrangimento de estado sobre uma dada classe. Tal fórmula traduz o facto de A ter que se verificar ao longo de uma vida (qualquer) dessa classe, ou seja, traduz o facto de A ser um *invariante* da classe.

As fórmulas de invariância não se esgotam com as fórmulas da forma anterior. Certos autores consideram também fórmulas da forma ($R_0 \Rightarrow (A\ \mathbf{U}^{?}_0\ B)$) como sendo de invariância ([Manna e Pnueli 94]). Neste caso, a fórmula caracteriza situações em que, a partir do momento em que R_0 se verifique e enquanto B não se verificar, a fórmula A terá que se verificar (poderá suceder que B nunca se verifique, situação em que A terá que se verificar *para sempre*, a partir de R_0).

Uma propriedade que possa ser especificada por uma fórmula de invariância diz-se uma propriedade de invariância.

O objectivo desta secção é apresentar um conjunto de regras que permitam provar propriedades de invariância sobre uma especificação GCL.

4.3.1 Invariantes simples

O primeiro caso considerado é das fórmulas da forma ($\mathbf{G}_0$A), aqui chamadas de *invariantes simples*.

Apresenta-se em seguida uma regra que permite estabelecer, sobre uma dada classe de uma especificação de comunidade de objectos, fórmulas da forma ($\mathbf{G}_0$A). Continua a assumir-se fixada uma especificação de comunidade de objectos *eco*.

Definição 4.19 *Regra da invariância*

INV.

I1. $\vdash_{c_1 \otimes \ldots \otimes c_n} x.(\divideontimes \Rightarrow A)$

I2. $\vdash_{c_1 \otimes \ldots \otimes c_n} x.((\bigwedge_{i=1}^{n} (\nabla_i = \pi_i(z_i)(x_i)) \wedge A) \Rightarrow (\mathbf{X}\ A))$

para cada tuplo de acções $z_1, \ldots, z_n$

$\vdash_{c_1 \otimes \ldots \otimes c_n} x.(\mathbf{G}_0 A)$

em que $A \in CE^{c_1 \otimes \ldots \otimes c_n}$. □

Se uma fórmula A for estabelecida inicialmente e for preservada por qualquer tuplo de acções, então A é invariante ao longo de qualquer vida de $c_1 \otimes \ldots \otimes c_n$.

A prova de correcção desta regra encontra-se adiante, na subsecção **4.3.3**.

Exemplo 4.20 *Relógios*

Suponha-se que se pretende provar, no contexto de uma instância da classe *Relógio*, que *enquanto essa instância estiver num estado animado o valor do seu atributo tempo é sempre superior ou igual a zero*, i.e.,

$$\vdash_{\text{Relógio}} (\mathbf{G}_0((x.ph=AN) \Rightarrow (x.tempo \geq 0))).$$

A prova realiza-se recorrendo a regra INV.

I1. $\vdash_{\text{Relógio}} (\divideontimes \Rightarrow (x.ph=AN \Rightarrow x.tempo \geq 0))$

1. $\vdash_{\text{Relógio}} (\divideontimes \Rightarrow (x.ph=PN))$ $AX^{\text{Relógio}}$
2. $\vdash_{\text{Relógio}} ((x.ph=PN) \Rightarrow (\neg(x.ph=AN)))$ TD
3. $\vdash_{\text{Relógio}} ((\neg(x.ph=AN)) \Rightarrow ((x.ph=AN) \Rightarrow (x.tempo \geq 0)))$ LPO
4. $\vdash_{\text{Relógio}} (\divideontimes \Rightarrow ((x.ph=AN) \Rightarrow (x.tempo \geq 0)))$ LPO:1,2,3

I2.a $\vdash_{\text{Relógio}} (((x.\nabla=novo) \wedge (x.ph=AN \Rightarrow x.tempo \geq 0)) \Rightarrow (\mathbf{X}(x.ph=AN \Rightarrow x.tempo \geq 0)))$

1. $\vdash_{\text{Relógio}} (((x.\nabla=novo) \wedge (A[{}^{x.tempo}_{0}][{}^{x.ph}_{AN}])) \Rightarrow (\mathbf{X}\ A))$ $AX^{\text{Relógio}}$
2. $\vdash_{\text{Relógio}} (((x.\nabla=novo) \wedge (AN=AN \Rightarrow 0=0)) \Rightarrow (\mathbf{X}\ (x.ph=AN \Rightarrow x.tempo \geq 0)))$ *Subst* :1[1]
3. $\vdash_{\text{Relógio}} (AN=AN \Rightarrow 0=0)$ TD
4. $\vdash_{\text{Relógio}} ((x.\nabla=novo) \Rightarrow (\mathbf{X}\ (x.ph=AN \Rightarrow x.tempo \geq 0)))$ LPO:2,3[2]
5. $\vdash_{\text{Relógio}} (((x.\nabla=novo) \wedge (x.ph=AN \Rightarrow x.tempo \geq 0)) \Rightarrow (\mathbf{X}(x.ph=AN \Rightarrow x.tempo \geq 0)))$ LPO:4

I2.b $\vdash_{\text{Relógio}} (((x.\nabla=obs) \wedge (x.ph=AN \Rightarrow x.tempo \geq 0)) \Rightarrow (\mathbf{X}(x.ph=AN \Rightarrow x.tempo \geq 0)))$

1. $\vdash_{\text{Relógio}} (((\nabla=obs) \wedge (x.ph=AN \Rightarrow x.tempo \geq 0)) \Rightarrow (\mathbf{X}(x.ph=AN \Rightarrow x.tempo \geq 0)))$ $AX^{\text{Relógio}}$

I2.c $\vdash_{\text{Relógio}} (((x.\nabla=tic) \wedge (x.ph=AN \Rightarrow x.tempo \geq 0)) \Rightarrow (\mathbf{X}(x.ph=AN \Rightarrow x.tempo \geq 0)))$

---

1 Este passo corresponde a fazer as substituições na fórmula apresentada no passo 1.

2 Prova-se, em lógica de primeira ordem, que a partir de $A \wedge B \Rightarrow C$ e B se deriva $A \Rightarrow C$.

1. $\vdash_{\text{Relógio}}$ $((x.\nabla=\text{tic})\wedge(x.\ ph=\text{AN} \Rightarrow\ x.\text{tempo}\geq 0))$ Hip
2. $\vdash_{\text{Relógio}}$ $(x.\nabla=\text{tic})$ LPO:1
3. $\vdash_{\text{Relógio}}$ $(x.ph=\text{AN} \Rightarrow\ x.\text{tempo}\geq 0)$ LPO:1
4. $\vdash_{\text{Relógio}}$ $(((x.\nabla=\text{tic}) \wedge (A\ [^{x.\text{tempo}}_{x.\text{tempo}+1}]\ )) \Rightarrow (\mathbf{X}A))$ $AX^{\text{Relógio}}$
5. $\vdash_{\text{Relógio}}$ $(((x.\nabla=\text{tic})\wedge(x.\ ph=\text{AN} \Rightarrow\ x.\text{tempo}+1\geq 0)) \Rightarrow$
   $(\mathbf{X}(x.ph=\text{AN} \Rightarrow\ x.\text{tempo}\geq 0)))$ *Subst* :4
6. $\vdash_{\text{Relógio}}$ $(x.\text{tempo}\geq 0\ \Rightarrow x.\text{tempo}+1\geq 0)$ TD
7. $\vdash_{\text{Relógio}}$ $(x.ph=\text{AN} \Rightarrow\ x.\text{tempo}+1\geq 0)$ LPO:3,6
8. $\vdash_{\text{Relógio}}$ $((x.\nabla=\text{tic})\wedge(x.\ ph=\text{AN} \Rightarrow\ x.\text{tempo}+1\geq 0))$ LPO:2,7
9. $\vdash_{\text{Relógio}}$ $(\mathbf{X}\ (x.ph=\text{AN} \Rightarrow\ x.\text{tempo}\geq 0))$ MP:8,5
10. $\vdash_{\text{Relógio}}$ $(((x.\nabla=\text{tic})\wedge(x.\ ph=\text{AN} \Rightarrow\ x.\text{tempo}\geq 0)) \Rightarrow$
    $(\mathbf{X}\ (x.ph=\text{AN} \Rightarrow\ x.\text{tempo}\geq 0)))$ DED:1,10

I2.d $\vdash_{\text{Relógio}}$ $(((x.\nabla=\perp)\wedge(x.ph=\text{AN} \Rightarrow\ x.\text{tempo}\geq 0)) \Rightarrow\ (\mathbf{X}\ (x.ph=\text{AN} \Rightarrow x.\text{tempo}\geq 0)))$

1. $\vdash_{\text{Relógio}}$ $(((x.\nabla=\perp)\wedge(x.ph=\text{AN} \Rightarrow\ x.\text{tempo}\geq 0)) \Rightarrow$
   $(\mathbf{X}\ (x.ph=\text{AN} \Rightarrow\ x.\text{tempo}\geq 0)))$ $AX^{\text{Relógio}}$

□

Notação:

De agora em diante, em todos os exemplos apresentados, o nome da classe em causa (e sempre que não haja conflito) será abreviado para a sua inicial. Assim, a classe *Relógio* passará a ser referenciada por R e a classe *Utilizador* por U. □

Exemplo 4.21 *Utilizadores e Relógios*

Suponha-se agora que se pretende provar que durante a vida de um relógio, *o tempo nunca decresce* , o que equivale a provar que *quaisquer duas observações consecutivas que um utilizador faça* (dadas pelos atributos *ta* e *tp*) *se tem ta≥tp*, i.e.,

$\vdash_{U\otimes R} (\mathbf{G}_0((x.ph_u=\text{AN}) \Rightarrow\ ((x.\text{rl}_u=\pi_r(x)) \Rightarrow (x.\text{ta}_u\geq x.\text{tp}_u))))$.

Em certas situações, ao longo deste exemplo, utiliza-se A como abreviatura da fórmula $(x.\ ph_u=\text{AN} \Rightarrow\ (x.\text{rl}_u=\pi_r(x) \Rightarrow x.\text{ta}_u\geq x.\text{tp}_u)$

I1. $\vdash_{U\otimes R} (\divideontimes \Rightarrow (x.ph_u=\text{AN} \Rightarrow\ (x.\text{rl}_u=\pi_r(x) \Rightarrow x.\text{ta}_u\geq x.\text{tp}_u)))$

A prova é semelhante à do exemplo anterior.

I2.a $\vdash_{U\otimes R} ((x.\nabla_u=\text{novo}_u \wedge x.\nabla_r=\text{novo}_r \wedge\ A) \Rightarrow (\mathbf{X}A))$

1. $\vdash_{U\otimes R} (x.\nabla_u=\text{novo}_u \wedge x.\nabla_r=\text{novo}_r \wedge\ A)$ Hip.
2. $\vdash_{U\otimes R} (x.\nabla_u=\text{novo}_u)$ LPO:1
3. $\vdash_{U\otimes R} (x.\nabla_r=\text{novo}_r)$ LPO:1

4. $\vdash_{U\otimes R} (x.ph_u=AN \Rightarrow ((x.rl_u=\pi_r(x) \Rightarrow x.ta_u \geq x.tp_u))$ LPO:1
5. $\vdash_U ((u.\nabla=novo \wedge (A \begin{bmatrix} u.ta \\ 0 \end{bmatrix} \begin{bmatrix} u.tp \\ 0 \end{bmatrix} \begin{bmatrix} u.sit \\ pobre \end{bmatrix} \begin{bmatrix} u.ph \\ AN \end{bmatrix})) \Rightarrow (\mathbf{X}A))$ AX^U
6. $\vdash_R ((r.\nabla=novo \wedge (A \begin{bmatrix} x.tempo \\ 0 \end{bmatrix} \begin{bmatrix} x.ph \\ AN \end{bmatrix})) \Rightarrow (\mathbf{X}A))$ AX^R
7. $\vdash_{U\otimes R} ((x.\nabla_u=novo_u \wedge x.\nabla_r=novo_r \wedge (AN=AN \Rightarrow (x.rl_u=\pi_r(x) \Rightarrow 0\geq 0))) \Rightarrow (\mathbf{X}A))$ COMB:5,6
8. $\vdash_{U\otimes R} (0\geq 0 \Rightarrow (AN=AN \Rightarrow (x.rl_u=\pi_r(x) \Rightarrow 0\geq 0)))$ LPO
9. $\vdash_{U\otimes R} 0\geq 0$ TD
10. $\vdash_{U\otimes R} (AN=AN \Rightarrow (x.rl_u=\pi_r(x) \Rightarrow 0\geq 0))$ MP:9,8
11. $\vdash_{U\otimes R} (x.\nabla_u=novo_u \wedge x.\nabla_r=novo_r \wedge (AN=AN \Rightarrow (x.rl_u=\pi_r(x) \Rightarrow 0\geq 0)))$ LPO:2,3,10
12. $\vdash_{U\otimes R} (\mathbf{X}A)$ MP:11,7
13. $\vdash_{U\otimes R} ((x.\nabla_u=novo_u \wedge x.\nabla_r=novo_r \wedge A) \Rightarrow (\mathbf{X}A))$ DED:1,12

I2.b $\vdash_{U\otimes R} ((x.\nabla_u=consultar_u \wedge x.\nabla_r=obs_r \wedge A) \Rightarrow (\mathbf{X}A))$

1. $\vdash_{U\otimes R} (x.\nabla_u=consultar_u \wedge x.\nabla_r=obs_r \wedge A)$ Hip
2. $\vdash_{U\otimes R} (x.\nabla_u=consultar_u)$ LPO:1
3. $\vdash_{U\otimes R} (x.\nabla_r=obs_r)$ LPO:1
4. $\vdash_{U\otimes R} (x.ph_u=AN \Rightarrow (x.rl_u=\pi_r(x) \Rightarrow x.ta_u \geq x.tp_u))$ LPO:1
5. $\vdash_{U\otimes R} ((x.rl_u=\pi_r(x)) \Rightarrow ((x.\nabla_u=consultar_u \wedge x.\nabla_r=obs_r \wedge (A\begin{bmatrix} x.tp_u \\ x.ta_u \end{bmatrix} \begin{bmatrix} x.ta_u \\ x.tempo_r \end{bmatrix})) \Rightarrow (\mathbf{X}A)))$ $AX^{U\otimes R}$
6. $\vdash_{U\otimes R} ((x.rl_u=\pi_r(x)) \Rightarrow ((x.\nabla_u=consultar_u \wedge x.\nabla_r=obs_r \wedge (x.ph_u=AN \Rightarrow (x.rl_u=\pi_r(x) \Rightarrow (x.tempo_r \geq x.ta_u)))) \Rightarrow (\mathbf{X}A)))$ *Subst* :5
7. $\vdash_{U\otimes R} ((x.\nabla_u=consultar_u \wedge x.\nabla_r=obs_r) \Rightarrow ((x.rl_u=\pi_r(x) \Rightarrow (x.ph_u=AN \Rightarrow (x.rl_u=\pi_r(x) \Rightarrow (x.tempo_r \geq x.ta_u)))) \Rightarrow (\mathbf{X}A)))$ LPO:6
8. $\vdash_{U\otimes R} (x.\nabla_u=consultar_u \wedge x.\nabla_r=obs_r)$ LPO:2,3
9. $\vdash_{U\otimes R} ((x.rl_u=\pi_r(x)) \Rightarrow ((x.ph_u=AN \Rightarrow (x.rl_u=\pi_r(x) \Rightarrow (x.tempo_r \geq x.ta_u))) \Rightarrow (\mathbf{X}A)))$ MP:8,7
10. $\vdash_{U\otimes R} ((x.ph_u=AN) \Rightarrow ((x.rl_u=\pi_r(x) \Rightarrow (x.tempo_r \geq x.ta_u)) \Rightarrow (\mathbf{X}A)))$ LPO:9
11. $\vdash_{U\otimes R} \mathbf{G}_0((x.ph_u=AN \wedge x.ph_r=AN) \Rightarrow (x.rl_u=\pi_r(x) \Rightarrow (x.tempo_r \geq x.ta_u)))$ *Teorema* [1]
12. $\vdash_{U\otimes R} ((x.ph_u=AN \wedge x.ph_r=AN) \Rightarrow (x.rl_u=\pi_r(x) \Rightarrow (x.tempo_r \geq x.ta_u)))$ LPO:11
13. $\vdash_U (u.\nabla=consultar \Rightarrow u.\Diamond(consultar))$ VID3
14. $\vdash_U (u.\Diamond(consultar) \Rightarrow u.ph=AN)$ AX^U,LPO
15. $\vdash_U (u.\nabla=consultar \Rightarrow u.ph=AN)$ LPO:13,14
16. $\vdash_{U\otimes R} (x.\nabla_u=consultar_u \Rightarrow x.ph_u=AN)$ HER:15
17. $\vdash_{U\otimes R} (x.ph_u=AN)$ MP:2,16
18. $\vdash_R (r.\nabla=obs \Rightarrow r.\Diamond(obs))$ VID3
19. $\vdash_R (r.\Diamond(obs) \Rightarrow r.ph=AN)$ AX^R,LPO

[1] Assume-se provado sobre a classe U ⊗R o invariante $\mathbf{G}_0((x.ph_u=AN \wedge x.ph_r=AN) \Rightarrow (x.rl_u=\pi_r(x) \Rightarrow (x.tempo_r \geq x.ta_u)))$. A prova deste invariante é semelhante à dos exemplos apresentados.

20. $\vdash_R (r.\nabla=obs \Rightarrow r.ph=AN)$ LPO:18,19
21. $\vdash_{U\otimes R} (x.\nabla_r=obs_r \Rightarrow x.ph_r=AN)$ HER:20
22. $\vdash_{U\otimes R} (x.ph_r=AN)$ MP:3,21
23. $\vdash_{U\otimes R} (x.ph_u=AN \wedge x.ph_u=AN)$ LPO:17,22
24. $\vdash_{U\otimes R} (x.rl_u=\pi_r(x) \Rightarrow (x.tempo_r \geq x.ta_u))$ MP:23,12
25. $\vdash_{U\otimes R} ((x.rl_u=\pi_r(x) \Rightarrow (x.tempo_r \geq x.ta_u)) \Rightarrow (\mathbf{X}A))$ MP:17,10
26. $\vdash_{U\otimes R} (\mathbf{X}A)$ MP:24,25
27. $\vdash_{U\otimes R} ((x.\nabla_u=consultar_u \wedge x.\nabla_r=obs_r \wedge A) \Rightarrow (\mathbf{X}A))$ DED:1,26

I2.c $\vdash_{U\otimes R} ((x.\nabla_u=consultar_u \wedge x.\nabla_r=tic_r \wedge A) \Rightarrow (\mathbf{X}A))$

1. $\vdash_{U\otimes R} (x.\nabla_u=consultar_u \wedge x.\nabla_r=tic_r \wedge A)$ Hip
2. $\vdash_{U\otimes R} (x.\nabla_u=consultar_u)$ LPO:1
3. $\vdash_{U\otimes R} (x.\nabla_r=tic_r)$ LPO:1
4. $\vdash_{U\otimes R} (x.ph_u=AN \Rightarrow (x.rl_u=\pi_r(x) \Rightarrow x.ta_u \geq x.tp_u))$ LPO:1
5. $\vdash_{U\otimes R} (x.rl_1=\pi_2(x) \Rightarrow (x.\nabla_u=consultar_u \Rightarrow x.\nabla_r=obs_r))$ $AX^{U\otimes R}$
6. $\vdash_{U\otimes R} (x.\nabla_u=consultar_u \Rightarrow (x.rl_1=\pi_2(x) \Rightarrow x.\nabla_r=obs_r))$ LPO:5
7. $\vdash_{U\otimes R} (x.rl_u=\pi_2(x) \Rightarrow x.\nabla_r=obs_r)$ MP:2,6
8. $\vdash_{U\otimes R} (x.rl_u=\pi_2(x) \Rightarrow x.\nabla_r=tic_r)$ LPO:3
9. $\vdash_{U\otimes R} (x.rl_u=\pi_2(x) \Rightarrow (x.\nabla_r=obs_r \wedge x.\nabla_r=tic_r))$ LPO:7,8
10. $\vdash_{U\otimes R} (\neg(obs_r=tic_r))$ AC2
11. $\vdash_{U\otimes R} ((\neg(obs_r=tic_r)) \Rightarrow (\neg(x.\nabla_r=obs_r \wedge x.\nabla_r=tic_r)))$ DT
12. $\vdash_{U\otimes R} (\neg(x.\nabla_r=obs_r \wedge x.\nabla_r=tic_r))$ MP:10,11
13. $\vdash_{U\otimes R} ((\neg(x.\nabla_r=obs_r \wedge x.\nabla_r=tic_r)) \Rightarrow ((x.\nabla_r=obs_r \wedge x.\nabla_r=tic_r) \Rightarrow ((x.ph_u=AN \Rightarrow (x.rl_u=\pi_r(x) \Rightarrow x.ta_u \geq x.tp_u)) \Rightarrow (\mathbf{X}A))))$ LPO
14. $\vdash_{U\otimes R} ((x.\nabla_r=obs_r \wedge x.\nabla_r=tic_r) \Rightarrow ((x.ph_u=AN \Rightarrow (x.rl_u=\pi_r(x) \Rightarrow x.ta_u \geq x.tp_u)) \Rightarrow (\mathbf{X}A)))$ MP:12,13
15. $\vdash_{U\otimes R} ((x.rl_u=\pi_2(x)) \Rightarrow ((x.ph_u=AN \Rightarrow (x.rl_u=\pi_r(x) \Rightarrow x.ta_u \geq x.tp_u)) \Rightarrow (\mathbf{X}A)))$ LPO:9,14
16. $\vdash_{U\otimes R} ((x.ph_u=AN \Rightarrow (x.rl_u=\pi_r(x) \Rightarrow x.ta_u \geq x.tp_u)) \Rightarrow (\mathbf{X}A))$ LPO:15
17. $\vdash_{U\otimes R} (\mathbf{X}A)$ MP:4,16
18. $\vdash_{U\otimes R} ((x.\nabla_u=consultar_u \wedge x.\nabla_r=tic_r \wedge A) \Rightarrow (\mathbf{X}A))$ DED:1,17

A prova para os outros casos (tuplos de acções) é semelhante. □

4.3.2 Invariantes generalizados

Considera-se agora o caso das fórmulas da forma $(R_0 \Rightarrow (A \mathbf{U}^{?}_0 B))$, aqui chamadas de *invariantes generalizados*. Esta fórmula pode se lida como *A tem que se verificar desde a condição inicial (dada por R_0) até que eventualmente a condição B se verifique*. À fórmula R_0 chama-se *requisito de configuração inicial*, e caracterizar as condições

iniciais (a partir das quais a fórmula A tem que se verificar). À negação da fórmula B chama-se *requisito de configuração* , e denota-se por R. Este requisito caracteriza as condições durante as quais a fórmula A tem que se verificar. De acordo com esta notação é possível reescrever a fórmula inicial, obtendo-se $(R_0 \Rightarrow (A\ \mathbf{U}^{?}_0\ (\neg R)))$[1].

Definição 4.22 *Regra da invariância generalizada*

ING.

G1. $\vdash_{c_1 \otimes \ldots \otimes c_n} x.(R_0 \Rightarrow A)$

G2. $\vdash_{c_1 \otimes \ldots \otimes c_n} x.(R_0 \Rightarrow R)$

G3. $\vdash_{c_1 \otimes \ldots \otimes c_n} x.((\bigwedge_{i=1}^{n} (\nabla_i = \pi_i(z_i))(x_i)) \wedge (R\ \mathbf{S}_0\ R_0) \wedge A) \Rightarrow (\mathbf{X}(R \Rightarrow A)))$

para cada tuplo de acções $z_1, \ldots, z_n$

$\vdash_{c_1 \otimes \ldots \otimes c_n} x.(R_0 \Rightarrow (A\ \mathbf{U}^{?}_0\ (\neg R)))$

em que $R, A \in CE^{c_1 \otimes \ldots \otimes c_n}$ e $R_0 \in L^{c_1 \otimes \ldots \otimes c_n}$. □

As duas primeiras premissas da regra estabelecem A e R, respectivamente. Na terceira premissa é necessário provar que, partindo de uma situação em que, para além de outras condições, A se verifica então no próximo estado, e se os requisitos de configuração (R) se mantiverem, A deverá continuar a manter-se, qualquer que seja o tuplo de acções que ocorra.

A condição $(R\ \mathbf{S}_0\ R_0)$, na terceira premissa, serve para eliminar situações em que, por algum motivo, os requisitos de configuração deixaram de se verificar, ainda que momentaneamente.

A prova de correcção desta regra encontra-se adiante, na subsecção **4.3.3**.

Em situações em que não haja requisitos de configuração, ou seja R=true, a fórmula invariante reduz-se a $(R_0 \Rightarrow (\mathbf{G}_0 A))$.

A regra seguinte serve para poder utilizar invariantes generalizados na prova de outros invariantes generalizados.

[1] Recorde-se que se encontra no apêndice B uma lista dos operadores temporais utilizados e respectiva semântica.

Definição 4.23 *Regra auxiliar*

AUX.

$$\frac{\text{A1. } \vdash_{c_1\otimes\ldots\otimes c_n} (R_0 \Rightarrow (A\ \mathbf{U}^{?}_0\ (\neg R))) \qquad \text{A2. } \vdash_{c_1\otimes\ldots\otimes c_n} (R_0 \Rightarrow R)}{\vdash_{c_1\otimes\ldots\otimes c_n} ((R\ \mathbf{S}_0\ R_0) \Rightarrow A)}$$

em que $A,R \in CE^{c_1\otimes\ldots\otimes c_n}$ e $R_0 \in L^{c_1\otimes\ldots\otimes c_n}$. □

A prova de correcção desta regra encontra-se adiante, na subsecção **4.3.3**.

Exemplo 4.24 *Relógios*

Suponha-se que se pretende provar

$\vdash_R$ (r. *ph*=AN $\Rightarrow$($\mathbf{G}_0$(r. *ph*=AN))).

pelas observações feitas à regra ING, basta provar

$\vdash_R$ (r. *ph*=AN $\Rightarrow$(r.*ph* $\mathbf{U}^{?}_0$ false)).

Escolha-se então

- r. *ph*=AN para R_0 e para φ;
- true para R.

G1. $\vdash_R$ ((r. *ph*=AN) $\Rightarrow$(r.*ph* =AN))

É imediato (é um teorema de LPO).

G2. $\vdash_R$ ((r. *ph*=AN) $\Rightarrow$true)

É imediato (é teorema de LPO).

G3.a $\vdash_R$ ((r. ∇=novo $\wedge$ (true $\mathbf{S}_0$ r. *ph*=AN) $\wedge$ r. *ph*=AN) $\Rightarrow$ ($\mathbf{X}$(true $\Rightarrow$ r.*ph* =AN)))

1.	$\vdash_R$ (r. ∇=novo $\wedge$ (true $\mathbf{S}_0$ r. *ph*=AN) $\wedge$ r. *ph*=AN)	Hip
2.	$\vdash_R$ (r. ∇=novo)	LPO:1
3.	$\vdash_R$ ((r. ∇=novo $\wedge$ (true $\Rightarrow$ AN=AN)) $\Rightarrow$ ($\mathbf{X}$(true $\Rightarrow$ r. *ph*=AN)))	AX^R
4.	$\vdash_R$ (true $\Rightarrow$ AN=AN)	TD,LPO
5.	$\vdash_R$ (r. ∇=novo $\wedge$ (true $\Rightarrow$ AN=AN))	LPO:2,4
6.	$\vdash_R$ ($\mathbf{X}$(true $\Rightarrow$ r.*ph*=AN))	MP:5,3
7.	$\vdash_R$ ((r. ∇=novo$\wedge$(true $\mathbf{S}_0$ r. *ph*=AN) $\wedge$r. *ph*=AN) $\Rightarrow$ ($\mathbf{X}$(true $\Rightarrow$ r. *ph*=AN)))	DED:1,7

A prova para os outros casos é semelhante. □

4.3.3 Correcção

Para terminar esta secção é necessário provar, tal como foi feito para a secção anterior, que as regras apresentadas são correctas face à semântica da Lógica de Certificação GNOME.

Proposição 4.25 *Correcção da regra da invariância*

A regra INV é correcta.

prova:

É um caso particular da prova de correcção da regra ING. □

Proposição 4.26 *Correcção da regra da invariância generalizada*

A regra ING é correcta.

prova:

Sejam θ uma atribuição, k∈ $\mathbb{N}_0$, u∈ $\mathcal{P}op_c$ e Ω um contexto de *co*, tais que $\theta_c(x)=u$, e suponha-se que $\theta,k,u, \Omega,co \Vdash_c R_0$ (por uma questão de simplicidade, assume-se que $c=c_1 \otimes \ldots \otimes c_n$). Pretende-se provar que $\theta,k,u, \Omega,co \Vdash_c (A \mathbf{U}^{?}_0 (\neg R))$. Há duas hipóteses a considerar: (i) existe k'>k tal que $\theta,k',u, \Omega,co \Vdash_c (\neg R)$; (ii) não existe k'>k tal que $\theta,k',u, \Omega,co \Vdash_c (\neg R)$.

Considere-se a situação (i) e escolha-se k' de tal modo que $\theta,k'',u, \Omega,co \Vdash_c R$, qualquer que seja k'' tal que $k \leq k'' < k'$. Basta então provar que $\theta,k''',u, \Omega,co \Vdash_c A$, qualquer que seja k''' tal que $k \leq k''' < k'$. Esta prova realiza-se por indução completa sobre o conjunto $K=\{p \in \mathbb{N}_0 : k \leq p < k'\}$.

- *base*: $\theta,k,u,\Omega,co \Vdash_c A$

  Resulta da primeira premissa (G1).

- *passo*: *θ,p',u, Ω,co* $\Vdash_c$ *A, qualquer que seja p'<p, implica* $\theta,p,u,\Omega,co \Vdash_c A$

  Seja p ∈ K tal que p>k, e suponha-se que $p \nabla_i (\Lambda(\langle c,u \rangle)_{2,p-1})=\pi_i(z_i)(x_i)$, para i=1,…,n. Então, $\theta,p-1,u, \Omega,co \Vdash_c (\bigwedge_{i=1}^{n} (\nabla_i=\pi_i(z_i)(x_i)))$, $\theta,p-1,u, \Omega,co \Vdash_c A$, por hipótese de indução, e $\theta,p-1,u, \Omega,co \Vdash_c (R \mathbf{S}_0 R_0)$, pelas hipóteses sobre k'. Isto implica que $\theta,p-1,u,\Omega,co \Vdash_c ((\bigwedge_{i=1}^{n} (\nabla_i=\pi_i(z_i)(x_i))) \wedge (R \mathbf{S}_0 R_0) \wedge A)$, o que, pela premissa G3, implica que $\theta,p,u,\Omega, co \Vdash_c (\mathbf{X} (R \Rightarrow A))$. Então, $\theta,p,u,\Omega, co \Vdash_c (R \Rightarrow A)$. Como p<k' então $\theta,p,u, \Omega,co \Vdash_c R$ e portanto $\theta,p,u,\Omega, co \Vdash_c A$.

Como existe k'>k tal que $\theta,k',u, \Omega,co \Vdash_c (\neg R)$ e, qualquer que seja k'' tal que $k \leq k'' k'$, se tem $\theta,k',u, \Omega,co \Vdash_c A$ então $\theta,k,u,\Omega, co \Vdash_c (A \mathbf{U}^{?}_0 (\neg R))$.

Considere-se agora a situação (ii). É necessário provar que $\theta,k',u, \Omega,co \Vdash_c A$, qualquer que seja k'≥k. Esta prova realiza-se novamente por indução completa, desta vez sobre o conjunto $K=\{p \in \mathbb{N}_0 : p \geq k\}$, e é semelhante à apresentada atrás.

Conclui-se também nesta situação que $\theta,k,u, \Omega,co \Vdash_c (A \mathbf{U}^{?}_0 (\neg R))$.

Pelo que se provou atrás conclui-se que $co \Vdash_c x.(R_0 \Rightarrow (A \mathbf{U}^{?}_0 (\neg R)))$, ou seja, que a regra ING é correcta. □

Proposição 4.27 *Correcção da regra auxiliar*

A regra AUX é correcta.

prova:

Sejam θ uma atribuição, $k \in \mathbb{N}_0$, $u \in \mathcal{P}op_c$ e Ω um contexto de *co*, e suponha-se que $\theta,k,u, \Omega,co \Vdash_c (R \mathbf{S}_0 R_0)$. É necessário provar que $\theta,k,u,\Omega, co \Vdash_c A$. Há duas situações a considerar: (i) $\theta,k,u, \Omega,co \Vdash_c R_0$; (ii) $\theta,k,u,\Omega, co \Vdash_c (\neg R_0)$.

Considere-se a situação (i). Por hipótese, a partir da premissa A1, $\theta,k,u, \Omega,co \Vdash_c (A \mathbf{U}^{?}_0 (\neg R))$, ou seja $\theta ,k,u,\Omega, co \Vdash_c ((\neg R) \vee (A \wedge (A \mathbf{U}^{?} (\neg R))))$. Mas da premissa A2 sabe-se que $\theta,k,u, \Omega,co \Vdash_c R$. Logo $\theta ,k,u,\Omega, co \Vdash_c (A \wedge (A \mathbf{U}^{?} (\neg R)))$ e portanto $\theta,k,u, \Omega,co \Vdash_c A$.

Considere-se agora a situação (ii). Como $\theta,k,u, \Omega,co \Vdash_c (R \mathbf{S}_0 R_0)$ então existe $k_1 < k$ tal que $\theta ,k_1 ,u, \Omega,co \Vdash_c R_0$ e $\theta ,k_2 ,u, \Omega,co \Vdash_c R$, qualquer que seja $k_1 < k_2 \leq k$. Por outro lado, a premissa A2 garante que $\theta,k_1 ,u, \Omega,co \Vdash_c R$ logo

$\theta,k,u, \Omega,co \Vdash_c R$, qualquer que seja k_2 tal que $k_1 \leq k_2 \leq k$. *(1)*

Pela premissa A1 sabe-se que $\theta,k_1 ,u, \Omega,co \Vdash_c (R_0 \Rightarrow (A \mathbf{U}^{?}_0 (\neg R)))$ logo $\theta,k_1 ,u, \Omega,co \Vdash_c (A \mathbf{U}^{?}_0 (\neg R))$ e portanto $\theta,k_1 ,u, \Omega,co \Vdash_c ((\neg R) \vee (A \wedge (A \mathbf{U}^{?} (\neg R))))$. Como $\theta,k_1 ,u, \Omega,co \Vdash_c R$ então $\theta,k_1 ,u, \Omega,co \Vdash_c (A \wedge (A \mathbf{U}^{?} (\neg R)))$, ou seja $\theta,k_1 ,u, \Omega,co \Vdash_c (A \mathbf{U}^{?} (\neg R))$, i.e., $\theta,k_1 ,u, \Omega,co \Vdash_c ((\mathbf{G}A) \vee (A \mathbf{U} (\neg R)))$. Se $\theta,k_1 ,u, \Omega,co \Vdash_c (\mathbf{G}A)$ então $\theta,k,u, \Omega,co \Vdash_c A$, visto que $k > k_1$. Se $\theta,k_1 ,u, \Omega,co \Vdash_c (A \mathbf{U} (\neg R))$ então existe $k_3 > k_1$ tal que $\theta,k_3 ,u, \Omega,co \Vdash_c (\neg R)$ e $\theta ,k_4 ,u, \Omega,co \Vdash_c A$, qualquer que seja $k_1 < k_4 < k_3$. De (1) sabe-se que $k_3 > k$ logo $\theta ,k,u,\Omega, co \Vdash_c A$. □

4.4 Cálculo de resposta

Uma propriedade de resposta pode ser utilizada para exprimir a *resposta* de um sistema a um dado estímulo. Uma fórmula de resposta é, em geral, da forma $(A \Rightarrow (\mathbf{F}_0 B))$, e exprime situações em que sempre A se verifique B tem que se verificar num instante futuro.

Certos autores assumem também um outro tipo de fórmulas de resposta, $(A \Rightarrow (A \mathbf{U}_0 B))$ ([Pnueli 86]). Nestas condições, A terá que se verificar até que B se verifique. É fácil concluir que $(A \Rightarrow (A \mathbf{U}_0 B))$ implica $(A \Rightarrow (\mathbf{F}_0 B))$.

No caso particular de especificações GCL, consideram-se propriedades de resposta que tenham em conta a *configuração* do sistema. Assim, uma propriedade de resposta é descrita por uma fórmula do tipo $((A \wedge R) \Rightarrow (R \; \mathbf{U}_0 \; (B \vee (\neg R))))$, que exprime situações que *sempre que A se verifique, sob certas condições de configuração R, ou as condições de configuração se mantêm até que B se verifique, ou as condições de configuração deixam de se verificar* .

Apresenta-se nesta secção um conjunto de regras de inferência, cuja correcção é apresentada no final do capítulo, que correspondem a uma generalização das regras propostas em [Manna e Pnueli 93b] e [Manna e Pnueli 91b] a configurações dinâmicas, devidamente adaptadas ao contexto da GCL.

No entanto, para garantir certas propriedades de resposta sobre o sistema, é necessário garantir que certas acções, que possam acontecer, *acontecem* de facto durante a vida do sistema. Ou seja, é necessário impôr sobre as acções *requisitos de justiça* .

Definição 4.28 *Requisitos de justiça*

Seja $c \in CP$. Então o conjunto Ax^c deverá incluir os seguintes axiomas:

- $\forall x.((\mathbf{G}_0(\mathbf{F}_0(\Diamond(z(x_1,\ldots,x_n))))) \Rightarrow (\mathbf{G}_0(\mathbf{F}_0(\nabla{=}z(x_1,\ldots,x_n))))))$, para cada $z \in ACC^c_{g_1\ldots g_n,g}$, tal que $z \neq \perp$. □

Cada um destes axiomas exprime que uma acção não pode estar repetidamente activada, um número infinito de vezes, e acontecer apenas num número finito. A este tipo de requisito chama-se *justiça forte* (ou *compaixão*).

Uma outra hipótese seria considerar apenas requisitos de *justiça fraca*, i.e., impedir situações em uma acção esteja continuamente activada a partir de um certo ponto e aconteça apenas um número finito de vezes. Esta condição pode ser expressa pela fórmula

$$\forall x.((\mathbf{F}_0(\mathbf{G}_0(\Diamond(z(x_1,\ldots,x_n))))) \Rightarrow (\mathbf{G}_0(\mathbf{F}_0(\nabla{=}z(x_1,\ldots,x_n))))).$$

Prova-se, no entanto, que justiça forte implica justiça fraca.

Assume-se de agora em diante que a especificação de comunidade de objectos considerada, *eco* , inclui à partida, para cada classe, axiomas de justiça forte sobre as suas acções.

4.4.1 Resposta num passo

Nesta secção introduz-se uma regra para provar propriedades de resposta que possam ser estabelecidas *num passo*, i.e., que dependam da ocorrência de uma única acção **z** para serem estabelecidas. Esta regra utiliza ainda uma fórmula φ auxiliar para caracterizar a situação que medeia entre A e A'.

Definição 4.29 *Regra de resposta num passo*

RESP

R1. $\vdash_{c_1 \otimes \ldots \otimes c_n} x.((R \wedge A) \Rightarrow (A' \vee \varphi))$

R2. $\vdash_{c_1 \otimes \ldots \otimes c_n} x.(((\bigwedge_{j=1}^{n} (\nabla_j = \pi_j(z_j)(x_j))) \wedge R \wedge \varphi) \Rightarrow (\mathbf{X}(R \Rightarrow (\varphi \vee A'))))$

para qualquer tuplo de acções $z_1, \ldots, z_n$

R3. $\vdash_{c_1 \otimes \ldots \otimes c_n} x.(((\bigwedge_{j=1}^{n} (\nabla_j = \pi_j(z_j)(x_j))) \wedge R \wedge \varphi) \Rightarrow (\mathbf{X}(R \Rightarrow A')))$

para qualquer tuplo de acções $z_1, \ldots, z_n$ tal que $z_i = \mathbf{z}$

R4. $\dfrac{\vdash_{c_1 \otimes \ldots \otimes c_n} x.((R \wedge \varphi) \Rightarrow (R \mathbf{U}_0 (A' \vee (\neg R) \vee \Diamond_i(\mathbf{z}(x_i)))))}{\vdash_{c_1 \otimes \ldots \otimes c_n} x.((R \wedge A) \Rightarrow (R \mathbf{U}_0 (A' \vee (\neg R))))}$

em que A,A',R, $\varphi \in CE^{c_1 \otimes \ldots \otimes c_n}$ e $\mathbf{z} \in ACC^{c_i}_{g_1 \ldots g_n, g}$. □

A primeira premissa da regra estabelece A' ou φ, a partir de A e R. A segunda premissa garante que qualquer tuplo de acções que preserve R deverá estabelecer A' ou, quando muito, preservar φ. A terceira premissa exige um tuplo envolvendo a acção **z** estabeleça A' a partir de φ, desde que preserve R. Finalmente, a última premissa exprime que, desde que a configuração seja preservada, num instante futuro ou A' se verifica ou a transição **z** estará activada. Esta última premissa, juntamente com as hipóteses de justiça sobre **z**, garante que a acção **z**, ocorrerá num instante futuro e portanto A' será estabelecida.

Note-se que a segunda premissa não precisa de ser provada para o caso em que o tuplo de acções envolve **z**, pois a terceira premissa implica a segunda.

Exemplo 4.30 *Relógios*

Suponha-se que se pretende provar, no contexto de uma instância da classe *Relógio*, que *se atributo tempo tiver valor 0 então alguma vez atingirá o valor 1, desde que a instância permaneça num estado animado*, i.e.,

$\vdash_R (((r.ph = AN) \wedge (r.tempo = 0)) \Rightarrow ((r.ph = AN) \mathbf{U}_0 ((r.tempo = 1) \vee (\neg(r.ph = AN)))))$

A prova realiza-se recorrendo à regra RESP, escolhendo:

- (r.tempo=0) para A;
- (r.tempo=1) para A';
- (r. *ph*=AN) para R;
- (r.tempo=0) para φ;
- tic para **z**.

R1. $\vdash_R$ ((r. *ph*=AN ∧ r.tempo=0) ⇒ (r.tempo=1 ∨ r.tempo=0))

A prova deste resultado é imediata.

R2.a $\vdash_R$ ((r. ∇=novo∧r.*ph*=AN ∧r.tempo=0) ⇒ **X**(r.*ph* =AN⇒(r.tempo=1 ∨r.tempo=0)))

1.	$\vdash_R$ (r. ∇=novo∧r.*ph*=AN ∧r.tempo=0)	Hip
2.	$\vdash_R$ (r. ∇=novo)	LPO:1
3.	$\vdash_R$ (r. *ph*=AN)	LPO:1
4.	$\vdash_R$ (r.tempo=0)	LPO:1
5.	$\vdash_R$ ((r. ∇=novo ∧ (AN=AN ⇒ (0=0 ∨ 0=1))) ⇒ (**X**(r.*ph* =AN⇒(r.tempo=1 ∨r.tempo=0))))	AX^R
6.	$\vdash_R$ (AN=AN ⇒ (0=0 ∨ 0=1))	TD,LPO
7.	$\vdash_R$ (r. ∇=novo ∧ (AN=AN ⇒ (0=0 ∨ 0=1)))	LPO:2,6
8.	$\vdash_R$ (**X**(r. *ph*=AN ⇒(r.tempo=1 ∨r.tempo=0)))	MP:7,5
9.	$\vdash_R$ ((r. ∇=novo∧r.*ph*=AN ∧r.tempo=0) ⇒ (**X**(r.*ph* =AN⇒(r.tempo=1 ∨r.tempo=0))))	DED:1,8

R2.b $\vdash_R$ ((r. ∇=obs∧r. *ph*=AN ∧r.tempo=0) ⇒ (**X**(r.*ph*=AN ⇒(r.tempo=1 ∨r.tempo=0))))

1.	$\vdash_R$ (r. ∇=obs∧r. *ph*=AN ∧r.tempo=0)	Hip
2.	$\vdash_R$ (r. ∇=obs)	LPO:1
3.	$\vdash_R$ (r. *ph*=AN)	LPO:1
4.	$\vdash_R$ (r.tempo=0)	LPO:1
5.	$\vdash_R$ ((r. ∇=obs ∧ (r. *ph* =AN⇒(r.tempo=1 ∨r.tempo=0))) ⇒ (**X**(r.*ph* =AN⇒(r.tempo=1 ∨r.tempo=0))))	AX^R
6.	$\vdash_R$ (r.tempo=0 ⇒ (r. *ph* =AN⇒(r.tempo=1 ∨r.tempo=0)))	LPO
7.	$\vdash_R$ (r. *ph*=AN ⇒(r.tempo=1 ∨r.tempo=0))	MP:4,6
8.	$\vdash_R$ ((r. ∇=obs) ∧ (r. *ph*=AN⇒ (r.tempo=1 ∨r.tempo=0)))	LPO:2,7
9.	$\vdash_R$ (**X**(r. *ph*=AN ⇒(r.tempo=1 ∨r.tempo=0))))	MP:8,5
10.	$\vdash_R$ ((r. ∇=obs∧r. *ph*=AN ∧r.tempo=0) ⇒ (**X**(r.*ph* =AN⇒(r.tempo=1 ∨r.tempo=0))))	DED:1,9

R3. $\vdash_R$ ((r. ∇=tic∧r.*ph*=AN ∧r.tempo=0) ⇒ (**X**(r.*ph* =AN⇒r.tempo=1)))

1. $\vdash_R$ (r. ∇=tic$\wedge$r.*ph*=AN $\wedge$r.tempo=0) Hip
2. $\vdash_R$ (r. ∇=tic) LPO:1
3. $\vdash_R$ (r. *ph*=AN) LPO:1
4. $\vdash_R$ (r.tempo=0) LPO:1
5. $\vdash_R$ ((r. ∇=tic$\wedge$(r.*ph*=AN $\Rightarrow$r.tempo+1=1)) $\Rightarrow$ (**X**(r. *ph*=AN $\Rightarrow$r.tempo=1))) AX^R
6. $\vdash_R$ (r.tempo=0 $\Rightarrow$ r.tempo+1=1) TD
7. $\vdash_R$ (r.tempo+1=1) MP:4,6
8. $\vdash_R$ ((r.tempo+1=1) $\Rightarrow$ (r. *ph*=AN $\Rightarrow$r.tempo+1=1)) LPO
9. $\vdash_R$ (r. *ph*=AN $\Rightarrow$r.tempo+1=1) MP:7,8
10. $\vdash_R$ (r. ∇=tic $\wedge$ (r. *ph*=AN $\Rightarrow$r.tempo+1=1)) LPO:2,9
11. $\vdash_R$ (**X**(r. *ph*=AN $\Rightarrow$r.tempo=1)) MP:5,8
12. $\vdash_R$ ((r. ∇=tic$\wedge$r.*ph*=AN $\wedge$r.tempo=0) $\Rightarrow$ (**X**(r.*ph* =AN$\Rightarrow$r.tempo=1))) DED:1,11

R4. $\vdash_R$ ((r.*ph*=AN $\wedge$r.tempo=0) $\Rightarrow$ (r. *ph*=AN **U** $_0$ (r.tempo=1 $\vee$r.$\Diamond$(tic) $\vee$(¬r. *ph*=AN))))

1. $\vdash_R$ (r.$\Diamond$(tic) $\Leftrightarrow$ r. *ph*=AN) AX^R
2. $\vdash_R$ (r.*ph*=AN $\vee$ (¬(r. *ph*=AN))) TD
3. $\vdash_R$ ((r.*ph*=AN $\vee$ (¬(r. *ph*=AN))) $\Rightarrow$ (r.tempo=1 $\vee$ r. *ph*=AN $\vee$ (¬(r. *ph*=AN)))) LPO
4. $\vdash_R$ (r.tempo=1 $\vee$ r. *ph*=AN $\vee$ (¬(r.*ph*=AN))) MP:2,3
5. $\vdash_R$ ((r.tempo=1 $\vee$ r. *ph*=AN $\vee$ (¬(r.*ph*=AN))) $\Rightarrow$
   ((r.tempo=1 $\vee$ r. *ph*=AN $\vee$ (¬(r. *ph*=AN))) $\vee$
   (r. *ph*=AN **U** (r.tempo=1$\vee$r. *ph*=AN $\vee$(¬r. *ph*=AN))))) LPO[1]
6. $\vdash_R$ ((r.tempo=1 $\vee$ r. *ph*=AN $\vee$ (¬(r.*ph*=AN))) $\vee$
   (r. *ph*=AN **U** (r.tempo=1$\vee$r. *ph*=AN $\vee$(¬r. *ph*=AN)))) MP:4,5
7. $\vdash_R$ (((r.tempo=1 $\vee$ r. *ph*=AN $\vee$ (¬(r.*ph*=AN))) $\vee$
   (r. *ph*=AN **U** (r.tempo=1$\vee$r. *ph*=AN $\vee$(¬r. *ph*=AN)))) $\Rightarrow$
   (r. *ph*=AN **U** $_0$ (r.tempo=1$\vee$r. *ph*=AN $\vee$(¬r. *ph*=AN)))) *Abv de* $\boldsymbol{U}_0$
8. $\vdash_R$ (r.*ph*=AN **U** $_0$ (r.tempo=1$\vee$r. *ph*=AN $\vee$(¬r. *ph*=AN))) MP:6,7
9. $\vdash_R$ (r.*ph*=AN **U** $_0$ (r.tempo=1$\vee$r. $\Diamond$(tic) $\vee$(¬r.*ph* =AN))) LPO:1,8
10. $\vdash_R$ ((r. *ph*=AN $\wedge$r.tempo=0) $\Rightarrow$
    (r. *ph*=AN **U** $_0$ (r.tempo=1 $\vee$r.$\Diamond$(tic) $\vee$(¬r. *ph*=AN)))) LPO:9

□

4.4.2 Resposta em vários passos

A regra de resposta introduzida na secção anterior permite provar propriedades de resposta que sejam estabelecidas num passo, ou seja, recorrendo apenas uma uma

[1] A fórmula (A $\Rightarrow$(A$\vee$A')) é teorema de LPO.

acção. Em geral, a prova de uma propriedade de resposta não envolve apenas uma acção. No entanto, sempre que o número de acções necessárias para estabelecer a propriedade seja pequeno, pode-se recorrer a vários lemas provados com a regra anterior e utilizar as regras seguintes para compor os resultados.

Definição 4.31 *Regra da monotonia da resposta*

M-RESP

M1. $\vdash_{c_1 \otimes \ldots \otimes c_n} (A \Rightarrow A')$

M2. $\vdash_{c_1 \otimes \ldots \otimes c_n} ((R \wedge A') \Rightarrow (R \, \mathbf{U}_0 \, (B' \vee (\neg R))))$

M3. $\vdash_{c_1 \otimes \ldots \otimes c_n} (B' \Rightarrow B)$

$$\vdash_{c_1 \otimes \ldots \otimes c_n} ((R \wedge A) \Rightarrow (R \, \mathbf{U}_0 \, (B \vee (\neg R))))$$

em que $A,A'B,B',R \in CE^{c_1 \otimes \ldots \otimes c_n}$. □

Esta regra caracteriza a monotonia das propriedades de resposta, permitindo substituir o antecedente da fórmula por uma fórmula mais forte (substituir A' por A, em que A implica A') e o consequente por uma fórmula mais fraca (substituir B' por B, em que B' implica B).

Definição 4.32 *Regra da transitividade da resposta*

T-RESP

T1. $\vdash_{c_1 \otimes \ldots \otimes c_n} ((R \wedge A) \Rightarrow (R \, \mathbf{U}_0 \, (A' \vee (\neg R))))$

T2. $\vdash_{c_1 \otimes \ldots \otimes c_n} ((R \wedge A') \Rightarrow (R \, \mathbf{U}_0 \, (A'' \vee (\neg R))))$

$$\vdash_{c_1 \otimes \ldots \otimes c_n} ((R \wedge A) \Rightarrow (R \, \mathbf{U}_0 \, (A'' \vee (\neg R))))$$

em que $A,A',A'',R \in CE^{c_1 \otimes \ldots \otimes c_n}$. □

Esta regra exprime a transitividade das propriedades de resposta.

Exemplo 4.33 *Relógios*

Suponha-se que se pretende provar que

$\vdash_R ((r.\,ph{=}AN \wedge r.tempo{=}0) \Rightarrow (r.\,ph{=}AN \, \mathbf{U}_0 \, (r.tempo{\geq}1 \vee (\neg(r.ph{=}AN)))))$.

Do exemplo **4.30** , sabe-se que

$\vdash_R ((r.\,ph{=}AN \wedge r.tempo{=}0) \Rightarrow (r.\,ph{=}AN \, \mathbf{U}_0 \, (r.tempo{=}1 \vee (\neg(r.\,ph{=}AN)))))$.

Por outro lado,

$\vdash_R ((r.tempo{=}0) \Rightarrow (r.tempo{=}0))$

é teorema de LPO e,

$\vdash_R ((r.tempo=1) \Rightarrow \quad (r.tempo \geq 1))$

resulta de TD.

Então, a regra M-RESP permite concluir o resultado desejado. □

Este exemplo prova que desde que uma instância da classe *Relógio* permaneça num estado animado, se o valor do seu atributo *tempo* for igual a 0, então esse atributo atingirá um valor superior ou igual a 1.

Exemplo 4.34 *Relógios*

Suponha-se agora que se pretende provar que

$\vdash_R ((r.ph=AN \wedge r.tempo=0) \quad \Rightarrow (r.ph=AN \mathbf{U}_0 (r.tempo=2 \vee (\neg(r. \quad ph=AN)))))$.

No exemplo **4.30** , provou-se que

$\vdash_R ((r.ph=AN \wedge r.tempo=0) \quad \Rightarrow (r.ph=AN \mathbf{U}_0 (r.tempo=1 \vee (\neg(r. \quad ph=AN)))))$.

Por um método semelhante podia também provar-se o seguinte resultado:

$\vdash_R ((r.ph=AN \wedge r.tempo=1) \quad \Rightarrow (r.ph=AN \mathbf{U}_0 (r.tempo=2 \vee (\neg(r. \quad ph=AN)))))$.

Então, a regra T-RESP permite concluir o resultado pretendido. □

Este exemplo permite concluir que desde que uma instância da classe *Relógio* permaneça num estado animado, se o valor do seu atributo *tempo* for 0, então eventualmente esse atributo atingirá o valor 2.

Para algumas propriedades, pode acontecer que o número de passos necessários não seja pequeno. Para estas situações introduz-se uma regra mais poderosa, que permite combinar os vários passos necessários.

Suponha-se então que, para estabelecer uma dada propriedade de resposta, são necessárias *r* acções, $\mathbf{z}_1,\ldots,\mathbf{z}_r$, tais que $\mathbf{z}_i \in \quad ACC^{c_i}_{g_1\ldots g_n,g}$, para i=1,…,r. A cada uma destas acções associa-se uma fórmula intermédia φ_i, fórmula essa que exprime, de alguma forma, a distância que falta para *atingir* A'.

Definição 4.35 *Regra da resposta em cadeia*

RESP *n*

para i=1,…,r:

J1. $\vdash_{c_1\otimes\ldots\otimes c_n} x.((R \wedge A) \Rightarrow \varphi)$

J2. $\vdash_{c_1\otimes\ldots\otimes c_n} x.(((\bigwedge_{j=1}^{n} (\nabla_j=\pi_j(z_j)(x_j))) \wedge \ R \ \wedge \ \varphi_i) \Rightarrow (\mathbf{X}(R \Rightarrow (\bigvee_{j\leq i} \varphi_j))))$

para qualquer tuplo de acções $z_1,\ldots,z_n$

J3. $\vdash_{c_1\otimes\ldots\otimes c_n} x.(((\bigwedge_{j=1}^{n} (\nabla_j=\pi_j(z_j)(x_j))) \wedge R \wedge \varphi_i) \Rightarrow (\mathbf{X}(R \Rightarrow (\bigvee_{j<i}\varphi_j))))$

para um tuplo de acções $z_1,\ldots,z_n$ tal que $z_k = \mathbf{z}_i$

J4. $\vdash_{c_1\otimes\ldots\otimes c_n} x.((R \wedge \varphi_i) \Rightarrow (R \ \mathbf{U}_0 \ ((\neg R) \vee \Diamond_i(\mathbf{z}_i(x_i)))))$

$\vdash_{c_1\otimes\ldots\otimes c_n} x.((R \wedge A) \Rightarrow (R \ \mathbf{U}_0 \ (A' \vee (\neg R))))$

Em que $A,A',\varphi,\varphi_1,\ldots,\varphi_n \in CE^{c_1\otimes\ldots\otimes c_n}$, e se supõe que $\varphi_0 = A'$ e que $\varphi = \varphi_0 \vee \ldots \vee \varphi_r$. □

A primeira premissa garante que pelo menos uma das asserções intermédias deve ser estabelecida. A segunda premissa garante que qualquer tuplo de acções deverá, ou preservar φ_i, ou estabelecer φ_j, para j<i. A terceira premissa exige que a transição $\mathbf{z}_i$ leve de φ_i a uma fórmula φ_j, para j<i. A quarta premissa é semelhante à quarta premissa da regra RESP. Ou seja, a segunda premissa garante que o *índice das fórmulas não aumenta* (i.e., nenhum tuplo de transições pode leva de uma fórmula φ_i a uma fórmula φ_j, com j>i), e a terceira premissa garante que as transições $\mathbf{z}_i$ *levam a que o índice das fórmulas decresca* (i.e., a partir de uma fórmula φ_i, por execução de $\mathbf{z}_i$, passa-se para uma situação em que φ_j se verifica, com j<i).

Exemplo 4.36 *Relógios*

Suponha-se que se pretende provar que *desde que uma instância da classe Relógio permaneça num estado animado, se o valor do seu atributo tempo for igual a 0, então esse atributo atingirá o valor k, para k* $\in \mathbb{N}_0$, i.e.,

$\vdash_R ((r.ph=AN \wedge r.tempo=0) \Rightarrow (r.ph=AN \ \mathbf{U}_0 \ (r.tempo=k \vee (\neg(r.ph=AN)))))$

Este resultado prova-se recorrendo à regra RESP *n*, escolhendo:

- (r.tempo=0) para A;
- (r.tempo=k) para A';
- (r.*ph*=AN) para R;
- (r.tempo=k-i) para φ_i, com i=0,…,k (note-se que φ_0=A');
- tic para $\mathbf{z}_i$, com i=1,…,k.

Suponha-se que i=1,…,k. Para cada valor de i tem-se

J1. $\vdash_R ((r.ph=AN \wedge r.tempo=0) \Rightarrow (r.tempo=k \vee \ldots \vee r.tempo=0))$

J2.a $\vdash_R ((r.\nabla=novo \wedge r.ph=AN \wedge r.tempo=k-i) \Rightarrow (\mathbf{X}(r.ph=AN \Rightarrow (\bigvee_{j\le i} r.tempo=k-j))))$

J2.b $\vdash_R ((r.\nabla=obs \wedge r.ph=AN \wedge r.tempo=k-i) \Rightarrow (\mathbf{X}(r.ph=AN \Rightarrow (\bigvee_{j\le i} r.tempo=k-j))))$

A prova destes três resultados é imediata.

J3. $\vdash_R ((r.\nabla=tic \wedge r.ph=AN \wedge r.tempo=k-i) \Rightarrow (\mathbf{X}(r.ph=AN \Rightarrow (\bigvee_{j<i} r.tempo=k-j))))$

1. $\vdash_R$ (r.∇ =tic$\wedge$r.*ph* =AN$\wedge$r.tempo=k-i) Hip
2. $\vdash_R$ (r.∇ =tic) Hip
3. $\vdash_R$ (r.tempo=k-i) Hip
4. $\vdash_R$ ((r.∇ =tic$\wedge$(r.*ph* =AN$\Rightarrow$($\bigvee_{j<i}$ r.tempo+1=k-j)))$\Rightarrow$
   ($\mathbf{X}$(r.*ph* =AN$\Rightarrow$($\bigvee_{j<i}$ r.tempo=k-j)))) AX^R
5. $\vdash_R$ ((r.tempo=k-i) $\Rightarrow$ (r.tempo+1=k-i+1)) TD
6. $\vdash_R$ (r.tempo+1=k-i+1) MP:3,5
7. $\vdash_R$ ((r.tempo+1=k-i+1) $\Rightarrow$ ($\bigvee_{j<i}$ r.tempo+1=k-j)) LPO[1]
8. $\vdash_R$ ($\bigvee_{j<i}$ r.tempo+1=k-j) MP:6,7
9. $\vdash_R$ (($\bigvee_{j<i}$ r.tempo+1=k-j) $\Rightarrow$ (r.*ph*=AN $\Rightarrow$($\bigvee_{j<i}$ r.tempo+1=k-j))) LPO
10. $\vdash_R$ (r.*ph*=AN $\Rightarrow$($\bigvee_{j<i}$ r.tempo+1=k-j)) MP:8,9
11. $\vdash_R$ ((r.∇=tic)$\wedge$(r.*ph*=AN $\Rightarrow$($\bigvee_{j<i}$ r.tempo+1=k-j))) LPO:2,11
12. $\vdash_R$ ($\mathbf{X}$(r.*ph*=AN $\Rightarrow$($\bigvee_{j<i}$ r.tempo=k-j))) MP:11,4
13. $\vdash_R$ ((r.∇ =tic$\wedge$r.*ph* =AN$\wedge$r.tempo=k-i) $\Rightarrow$
    ($\mathbf{X}$(r.*ph* =AN$\Rightarrow$($\bigvee_{j<i}$ r.tempo=k-j)))) MTD:1,12

J4. $\vdash_R$ ((r.*ph*=AN $\wedge$r.tempo=0) $\Rightarrow$ (r.*ph*=AN $\mathbf{U}_0$ ((¬r.*ph*=AN) $\vee$ r. $\Diamond$(tic))))

A prova deste resultado é semelhante à realizada em R4 do exemplo **4.30** . □

4.4.3 Resposta em configurações estáveis

Há uma classe de configurações nas quais as propriedades de resposta agora apresentadas se resumem às propriedades de resposta tradicionais, (A$\Rightarrow$ ($\mathbf{F}_0$A')). A essas configurações chama-se *configurações estáveis*.

Definição 4.37 *Configuração estável*

Seja R$\in$ $CE^{c_1\otimes\ldots\otimes c_n}$ um requisito de configuração. Então, R diz-se *estável* sse $\vdash_{c_1\otimes\ldots\otimes c_n}$ (R$\Rightarrow$($\mathbf{G}_0$R)). □

Ou seja, uma configuração estável é uma configuração que, uma vez estabelecida, nunca mais deixa de se verificar.

Para esta classe de configurações, introduz-se a seguinte regra.

Definição 4.38 *Regra para configurações estáveis*

RCE

---

[1] Note-se que se (r.tempo+1=k-i+1) então (r.tempo+1=k-j), com j=i-1.

E1. $\vdash_{c_1 \otimes \ldots \otimes c_n} ((R \wedge A) \Rightarrow (R \; \mathbf{U}_0 \; (A' \vee (\neg R))))$

E2. $\vdash_{c_1 \otimes \ldots \otimes c_n} (R \Rightarrow (\mathbf{G}_0 R))$

$\vdash_{c_1 \otimes \ldots \otimes c_n} ((R \wedge A) \Rightarrow (\mathbf{F}_0 A'))$

em $A, A', R \in CE^{c_1 \otimes \ldots \otimes c_n}$. □

Esta regra permite relacionar as propriedades de resposta aqui introduzidas com as propriedades de respostas tradicionais, referidas no início da secção.

Exemplo 4.39 *Relógios*

Os exemplos **4.24** e **4.36** permitem concluir que

$\vdash_R ((r.ph = AN \wedge r.tempo = 0) \Rightarrow (\mathbf{F}_0 (r.tempo = k)))$, para $k \in \mathbb{N}_0$.

ou seja, *para qualquer instância r da classe Relógio que se encontre num estado animado, se o seu atributo tempo tiver valor 0 então, num instante futuro, esse atributo terá valor k, para* $k \in \mathbb{N}_0$. □

4.4.4 Correcção

Tal como foi feito nas secções anteriores, apresenta-se agora a correcção de todas as regras introduzidas relativamente à semântica da Lógica de Certifição GNOME.

Proposição 4.40 *Correcção da regra RESP*

A regra RESP é correcta.

prova:

É um caso particular da prova da regra RESP *n*. □

Proposição 4.41 *Correcção da regra M-RESP*

A regra M-RESP é correcta.

prova:

Sejam θ uma atribuição, $k \in \mathbb{N}_0$, $u \in \mathcal{P}op_c$ e Ω um contexto de *co*, e suponha-se que $\theta, k, u, \Omega, co \Vdash_c (R \wedge A)$. Então, a partir de M1, sabe-se que $\theta, k, u, \Omega, co \Vdash_c (R \wedge A')$, o que, por M2, implica $\theta, k, u, \Omega, co \Vdash_c (R \; \mathbf{U}_0 \; (B' \vee (\neg R)))$, e portanto, existe $k' \geq k$ tal que $\theta, k', u, \Omega, co \Vdash_c (B' \vee (\neg R))$ e $\theta, k'', u, \Omega, co \Vdash_c R$, qualquer que seja k'' tal que $k \leq k'' < k'$. Então, a partir da premissa M3, obtém-se $\theta, k', u, \Omega, co \Vdash_c (B \vee (\neg R))$, o que permite concluir que $\theta, k, u, \Omega, co \Vdash_c (R \; \mathbf{U}_0 \; (B \vee (\neg R)))$ e portanto, $\theta, k, u, \Omega, co \Vdash_c ((R \wedge A) \Rightarrow (R \; \mathbf{U}_0 \; (B \vee (\neg R))))$. □

Proposição 4.42 *Correcção da regra T-RESP*

A regra T-RESP é correcta.

prova:

Sejam θ uma atribuição, $k\in \mathbb{N}_0$, $u\in \mathcal{P}op_c$ e Ω um contexto de *co*, e suponha-se que $\theta,k,u, \Omega,co\Vdash_c (R\wedge A)$. Então, por T1, tem-se $\theta,k,u, \Omega,co\Vdash_c (R\ \mathbf{U}_0\ (A'\vee(\neg R)))$, e portanto existe $k'\geq k$ tal que $\theta,k',u, \Omega,co\Vdash_c (A'\vee(\neg R))$ e $\theta,k'',u, \Omega,co\Vdash_c R$, qualquer que seja k'' tal que $k\leq k''<k'$. Se $\theta,k',u, \Omega,co\Vdash_c (\neg R)$, então $\theta,k',u, \Omega,co\Vdash_c ((\neg R)\vee A'')$ e portanto $\theta,k,u, \Omega,co\Vdash_c (R\ \mathbf{U}_0\ (A''\vee(\neg R)))$. Suponha-se então que $\theta,k',u, \Omega,co\Vdash_c R$, e portanto $\theta,k',u, \Omega,co\Vdash_c A'$. A partir da premissa T2, sabe-se que $\theta,k',u, \Omega,co\Vdash_c (R\ \mathbf{U}_0\ (A''\vee(\neg R)))$. Novamente, existe $k_1\geq k'$ tal que $\theta,k_1,u, \Omega,co\Vdash_c (A''\vee(\neg R))$ e $\theta,k_2,u, \Omega,co\Vdash_c R$, qualquer que seja $k'\leq k_2<k_1$, o que juntamente com as hipóteses anteriores implica que $\theta,k_3,u, \Omega,co\Vdash_c R$, qualquer que seja k_3 tal que $k\leq k_3<k_1$, e portanto permite concluir que $\theta,k',u, \Omega,co\Vdash_c (R\ \mathbf{U}_0\ (A''\vee(\neg R)))$. Conclui-se, em ambas as situações, que $\theta,k',u, \Omega,co\Vdash_c ((R\wedge A)\Rightarrow(R\ \mathbf{U}_0\ (A''\vee(\neg R))))$. □

Proposição 4.43 *Correcção da regra RESP*n

A regra RESP *n* é correcta.

prova:

Sejam θ uma atribuição, $k\in \mathbb{N}_0$, $u\in \mathcal{P}op_c$ e Ω contexto de *co*, tais que $\theta_c(x)=u$ e que $\theta,k,u, \Omega,co\Vdash_c (R\wedge A)$. Se existe $k'>k$ tal que $\theta,k',u, \Omega,co\Vdash_c (\neg R)$ então $\theta,k,u,\Omega,co\Vdash_c (R\ \mathbf{U}_0\ (A'\vee(\neg R)))$. Suponha-se então que $\theta,k',u, \Omega,co\Vdash_c R$, qualquer que seja $k'\geq k$. Por J1 sabe-se que que $\theta,k,u, \Omega,co\Vdash_c \varphi$, ou seja, existe $1\leq i\leq r$ tal que $\theta,k,u,\Omega,co\Vdash_c \varphi_i$.

Suponha-se agora que $p\nabla_j(\Lambda(\langle c,u\rangle)_{2,k})=\pi_j(z_j)(x_j)$, para $j=1,\ldots,n$. Há duas hipóteses a considerar:

(a) $z_j=\mathbf{z}_i$, para algum j. Então, como $\theta,k,u,\Omega,co\Vdash_c R$ e $\theta,k,u,\Omega,co\Vdash_c \varphi_i$ e ainda $\theta,k,u, \Omega,co\Vdash_c \bigwedge_{l=1}^{n}\nabla_l=\pi_l(z_l)(x_l)$, por J3, resulta que $\theta,k,u,\Omega,co\Vdash_c (\mathbf{X}(R\Rightarrow(\bigvee_{l<i}\varphi_l)))$. Como $\theta,k+1,u,\Omega,co\Vdash_c R$, resulta que $\theta,k+1,u,\Omega,co\Vdash_c (\bigvee_{l<i}\varphi_l)$. Na pior das hipóteses, $\theta,k+1,u, \Omega,co\Vdash_c \varphi_{i-1}$.

(b) Nenhum dos z_j é $\mathbf{z}_i$. Então, por um argumento semelhante ao anterior, e utilizando a premissa J2, tem-se que $\theta,k+1,u, \Omega,co\Vdash_c (\bigvee_{l\leq i}\varphi_l)$, ou seja, ou $\theta,k+1,u, \Omega,co\Vdash_c \varphi_i$, ou $\theta,k+1,u,\Omega,co\Vdash_c \varphi_l$, para $l<i$, que na pior das hipóteses se reduz a $\theta,k+1,u, \Omega,co\Vdash_c \varphi_{i-1}$, tal como na hipótese (a). Suponha-se então que $\theta,k+1,u, \Omega,co\Vdash_c \varphi_i$ e que a situação se mantém, i.e., que $\theta,k_1,u,\Omega,co\Vdash_c \varphi_i$, qualquer que seja $k_1\geq k+1$ (caso a situação não se mantenha, o *pior* que pode acontecer é $\theta,k_1,u,\Omega,co\Vdash_c \varphi_l$, para algum $k_1\geq k+1$ e $l<i$, que se resume à hipótese (a)). Mas então, pela premissa J4 (atendendo a que $\theta,k_1,u,\Omega,co\Vdash_c R$, qualquer que seja $k_1\geq k+1$), conclui-se que a transição $\mathbf{z}_i$ está recorrentemente activada o que, pelas hipóteses de justiça sobre as transições, garante que a transição $\mathbf{z}_i$ terá que ocorrer, ou seja,

existe $k_2 \geq k+1$ tal que $p \nabla_j(\Lambda(<c,u>)_{2,k_2}) = \pi_j(\mathbf{z}_i)(x_j)$. Por um argumento semelhante ao utilizado na hipótese (a), tem-se que $\theta,k_2+1,u, \Omega,co \Vdash_c \varphi_{i-1}$.

De (a) e (b) resulta que existe $k_3 \geq k$, tal que $\theta,k_3,u,\Omega,co \Vdash_c \varphi_{i-1}$. Aplicando este argumento recorrentemente conclui-se que existe $k_4 \geq k$ tal que $\theta,k_4,u,\Omega,co \Vdash_c \varphi_0$. Como $\varphi_0 = A'$ conclui-se $\theta,k,u,\Omega, co \Vdash_c (R \mathbf{U}_0 (A' \vee (\neg R)))$. □

Proposição 4.44 *Correcção da regra RCE*

A regra RCE é correcta.

prova:

Sejam θ uma atribuição, $k \in \mathbb{N}_0$, $u \in \mathcal{P}op_c$ e Ω um contexto de *co*, e suponha-se que $\theta,k,u, \Omega,co \Vdash_c (R \wedge A)$. Então, a partir de E1, sabe-se que $\theta,k,u,\Omega, co \Vdash_c (R \mathbf{U} (A \vee (\neg R)))$, ou seja que existe $k' \geq k$ tal que $\theta,k',u, \Omega,co \Vdash_c (A \vee (\neg R))$ e $\theta,k'',u, \Omega,co \Vdash_c R$, qualquer que seja k'' tal que $k \leq k'' < k'$. A partir da premissa E2, sabe-se que se $\theta,k',u, \Omega,co \Vdash_c R$ logo $\theta,k',u, \Omega,co \Vdash_c A$ o que implica que $\theta,k,u, \Omega,co \Vdash_c (\mathbf{F}_0 A)$. Conclui-se então que $\theta,k,u, \Omega,co \Vdash_c ((R \wedge A) \Rightarrow (\mathbf{F}_0 A))$. □