Capítulo 5

CTL

5.1 Introdução

O objetivo da tese é apresentar um sistema em dedução natural para a lógica CTL. É uma lógica temporal muito indicada para a análise de programas concorrentes, uma vez que ela se baseia numa estrutura temporal em árvore, que corresponde à execução de um programa com módulos em paralelo, no qual o comportamento não é deterministico: ou seja, dado um instante num certo estado, teremos uma gama de estados possíveis para o instante seguinte.
Considere por exemplo os dois programas seguintes em paralelo:

Considere que inicialmente i=0, e que cada instrução é atômica. Quando executarmos os programas teremos várias possibilidades para a ordem em que as instruções serão executadas: P1L1-P1L2-P2L1-P2L1, P1L1-P2L1-P1L2-P2L2, P1L1-P2L1-P2L2-P1L2, P2L1-P2L2-P1L1-P1L1, P2L1-P1L1-P2L2-P1L2, P2L1-P1L1-P1L2-P2L2, (onde PiLj significa linha j do programa i).

Considerando que o estado da máquina se resume ao valor contido na variável i, as possíveis execuções desses dois programas em paralelo podem ser representadas pela árvore seguinte:

Programa 1:	Programa 2:
i=0	i=2
i=i+1	i=5

Figura 5.1: Dois programas concorrentes

PUC-Rio - Certificação Digital Nº 0016017/CA

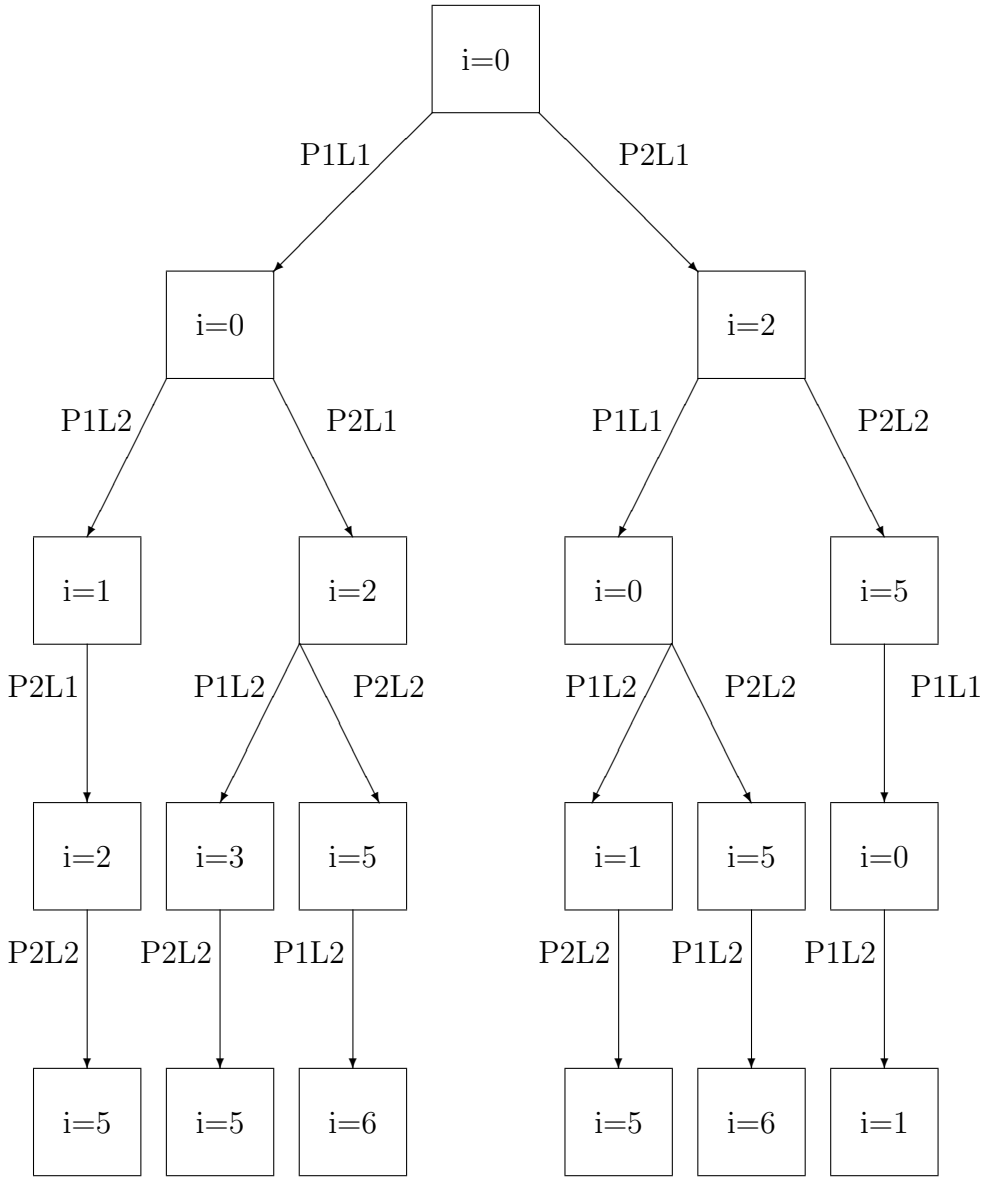


Figura 5.2: Árvore de possíveis execuções

PUC-Rio - Certificação Digital Nº 0016017/CA

CTL visa então expressar propriedades de árvores como essa. Mais precisamente a linguagem de CTL permite expressar coisas como: é possível que a execução seja tal que a condição A seja sempre válida, ou, qualquer que seja a execução a condição A será sempre válida, ou, existe uma execução na qual cedo ou tarde B será valida sendo que até lá A será valida, etc., onde A e B são fórmulas da linguagem CTL.

Por exemplo, é comum expressar propriedades ditas de segurança que afirmam que uma certa propriedade p jamais se realizará. Tais fórmulas têm a forma: $[\forall G]\neg p$. Outro exemplo é o de fórmulas expressando que uma certa propriedade p será obrigatoriamente verdadeira em algum momento do futuro. Tais fórmulas têm a forma: $[\forall F]p$.

É sempre bom mencionar a fonte de origem. CTL é uma lógica que foi inventada por Edmund M. Clarke e E. Allen Emerson em 1981 [Clarke1981]. Eles a apresentam com um objetivo bem específico: construir programas concorrentes. CTL seria então usada para gerar automaticamente o "esqueleto de sincronização"do programa. Neste esqueleto são considerados apenas os detalhes importantes para sincronização. Assim é importante identificar partes do código como seção crítica e seção não crítica. O que acontece dentro de cada parte é visto como irrelevante. O artigo é apresentado com um model checker (uma maneira de checar se uma dada estrutura é modelo de uma certa formula) e um método para testar se uma fórmula de CTL é satisfatível e gerar então um modelo finito para ela. O artigo termina então com um exemplo no qual o problema da exclusão mútua sem starvation para dois processos é resolvido em três etapas: especificação, obtenção do modelo finito, e extração do esqueleto de sincronização a partir do modelo obtido. Nesta especificação são identificadas três partes do código: seção crítica, seção não crítica, e tentativa de entrada em seção crítica. O resto da especificação consiste então em estabelecer fórmulas que traduzam a relação que queremos ter entre essas seções, como por exemplo $[\forall G](\neg(SC_1 \wedge SC_2))$ (onde SC_1 significa seção crítica do processo 1).

A linguagem usada era basicamente a mesma da aqui apresentada, com exceção de $[\exists X]$ que era um conectivo primitivo ao invés de $[\forall X]$. Também a relação R era considerada como a união de várias relações, uma para cada processo (representando as transições possíveis para cada um).

PUC-Rio - Certificação Digital Nº 0016017/CA

Entre as várias formulações de CTL, a única que não é axiomática é a de Echagüe [Echagüe1993] que foi feita para cálculo de seqüêntes, mas não teve influência sobre o nosso trabalho. Será dada então a seguir, no capítulo 2, uma apresentação mais tradicional, seguindo a apresentação de Goldblatt [Goldblatt1993], e em seguida no capítulo 3 falaremos um pouco sobre alguns artigos de interesse. Enfim será apresentada no capítulo 4 a que foi desenvolvida para dedução natural, e para a qual foram provadas correção (capítulo 4) e completude (capítulo 5). No capítulo 7 veremos como o sistema se comporta em relação à normalização das provas.

5.2 Computation Tree Logic (CTL)

CTL é uma lógica que visa o estudo de programas concorrentes, ou seja, com módulos executando em paralelo. Quando programas têm módulos que executam em paralelo, podemos ver a execução do programa como sendo não deterministica, pois a cada passo não sabemos qual dos módulos estará sendo executado. Desta forma podemos pensar na execução do programa como uma árvore que não para de se ramificar, pois a cada estado ela pode evoluir para vários estados possíveis dependendo do módulo que for executado. Cada nó da árvore representa então um estado possível do programa, sendo que o estado poderia ser representado pelo conjunto dos dados de cada processo, juntamente com o ponto de execução no qual se encontra cada um deles (do mesmo jeito que é costume fazer quando se encara um computador como uma máquina de estados). Podemos então observar certas condições interessantes e estabelecer relações entre elas. Por exemplo, podemos querer, para assegurarmos que o programa está correto, que cedo ou tarde a assertiva A seja verdadeira. Pensando na árvore diriamos: qualquer que seja o caminho percorrido A acabará sendo verdade. Ou podemos querer que tanto A quanto B sejam condições possíveis. Assim diriamos: existe um caminho que leva a A, e existe um caminho que leva a B. Traduzindo estes dois exemplos em CTL teríamos: $[\forall F]A$ para o primeiro e $[\exists F]A \wedge [\exists F]B$ para o segundo.

Segue então uma exposição de CTL baseada no livro "Logics of Time and Computation"de Robert Goldblatt [Goldblatt1993].

5.2.1 Sintaxe

A sintaxe de CTL é dada por:

PUC-Rio - Certificação Digital Nº 0016017/CA

$A := p|\ \bot|\ A_1 \rightarrow A_2|\ [\forall X]A|\ \forall(A_1 \mathcal{U} A_2)|\ \exists(A_1 \mathcal{U} A_2)$

É usual usar as seguintes abreviações:

$\neg A$ para $A \rightarrow \bot$
$\top$ para $\neg\bot$
$A_1 \vee A_2$ para $(\neg A_1) \rightarrow A_2$
$A_1 \wedge A_2$ para $\neg(A_1 \rightarrow \neg A_2)$
$A_1 \leftrightarrow A_2$ para $(A_1 \rightarrow A_2) \wedge (A_2 \rightarrow A_1)$

$[\forall F]A$ para $\forall(\top \mathcal{U} A)$
$[\exists F]A$ para $\exists(\top \mathcal{U} A)$
$[\forall G]A$ para $\neg\exists(\top \mathcal{U} \neg A)$
$[\exists G]A$ para $\neg\forall(\top \mathcal{U} \neg A)$
$[\exists X]A$ para $\neg[\forall X]\neg A$

PUC-Rio - Certificação Digital Nº 0016017/CA

5.2.2 Semântica

Considera-se um frame serial $\mathcal{F} = (S, R)$, e $\mathcal{M}$ um modelo sobre $\mathcal{F}$. Um $R - branch$ começando em s é uma seqüência infinita $s_0, ..., s_n, ...$ com $s = s_0$ e $s_n R s_{n+1}$ para todo n. Um $R - path$ é uma versão finita de um $R - branch$.

Assim sendo:

$\mathcal{M} \models_s [\forall X]A$ sse $sRt \Rightarrow \mathcal{M} \models_t A$

$\mathcal{M} \models_s \forall(A\mathcal{U}B)$ sse para todo $R - branch$ $s = s_0 R s_1 ...$ existe k tal que $\mathcal{M} \models_{s_k} B$ e $\mathcal{M} \models_{s_i} A$ para todo i tal que $0 \leq i < k$.

$\mathcal{M} \models_s \exists(A\mathcal{U}B)$ sse existe um $R - paths = s_0 ... s_k$ tal que $\mathcal{M} \models_{s_k} B$ e $\mathcal{M} \models_{s_i} A$ para todo i tal que $0 \leq i < k$.

Para os outros conectivos adota-se a interpretação tradicional.
Perceba que $[\forall X]A$ significa que para todo sucessor imediato teremos A.

As abreviações têm então o seguinte sentido:

$[\forall F]A$: para todo caminho infinito (branch) existe um mundo (estado) no qual

A é verdadeiro.
$[\exists F]A$: existe um mundo futuro (ou presente) no qual A é verdadeiro.
$[\forall G]A$: de agora em diante (para todos os caminhos) sempre A
$[\exists G]A$: existe um caminho infinito no qual sempre A
$[\exists X]A$: existe um sucessor imediato no qual A

O que se pretende encontrar então é uma lógica cujas fórmulas correspondam exatamente ao conjunto de fórmulas válidas em todos os frames seriais, usando a semântica que acaba de ser descrita. Em [Goldblatt1993] a axiomatização apresentada a seguir foi provada correta e completa em relação a esta semântica.

5.2.3 Axiomas

CTL é então a menor lógica (entende-se por lógica um conjunto de fórmulas que contém todas as tautologias proposicionais, e que seja fechado por modus ponem) da linguagem descrita que contém os seguintes axiomas (esquemas):

$K_X : [\forall X](A \to B) \to ([\forall X]A \to [\forall X]B)$
$D_X : [\exists X]\top$
$\exists\mathcal{U} : \exists(A\mathcal{U}B) \leftrightarrow (B \vee (A \wedge [\exists X]\exists(A\mathcal{U}B)))$
$\forall\mathcal{U} : \forall(A\mathcal{U}B) \leftrightarrow (B \vee (A \wedge [[\forall X]]\forall(A\mathcal{U}B)))$

e é fechada sob as regras seguintes:

$Necessitation : \vdash A \ \Rightarrow \vdash [\forall X]A$
$\exists - Ind : \vdash (B \vee (A \wedge [\exists X]C) \to C \ \Rightarrow \vdash \exists(A\mathcal{U}B) \to C$
$\forall - Ind : \vdash (B \vee (A \wedge [\forall X]C) \to C \ \Rightarrow \vdash \forall(A\mathcal{U}B) \to C$

5.3 Sistemas de Dedução Natural para Lógica Modal

Neste capítulo apresentamos a noção geral de sistemas de dedução natural rotulados, (introduzidos por [Simpson1993]), como uma forma de apresentar sistemas de dedução natural para lógica modal.

PUC-Rio - Certificação Digital Nº 0016017/CA

5.3.1 Fórmulas rotuladas

O uso de rótulos em dedução natural para lógica modal não é novidade, e em [Basin1997] é exposta uma abordagem que funciona bem para lógicas modais que só utilizam os conectivos $\Box$ e $\diamond$ (além dos clássicos). Infelizmente essa solução não parece ser suficiente para tratar de noções como "until"ou outras noções específicas de modelos com estrutura em forma de árvore. O artigo "Labelled Propositional Modal Logics: Theory and Practice"[Basin1997] apresenta uma visão geral do uso de rótulos para lógicas modais.

Neste artigo o autor reune várias lógicas modais sob uma mesma abordagem, para obter um sistema em dedução natural, que é correto e completo. Para isso ele desenvolve uma lógica de base, chamada K, que contém as regras da lógica classica, (podendo então derivar todos os teoremas da lógica proposicional), à qual ele acrescenta regras de introdução e eliminação para os conectivos da lógica modal: $\Box$ e $\diamond$. Mas está lógica não trabalha diretamente com as fórmulas da lógica modal. Ela trabalha com fórmulas relacionais e com fórmulas rotuladas (labelled). As fórmulas rotuladas têm o formato: $x : A$, onde x é um rótulo, e A é uma fórmula da lógica modal. As fórmulas relacionais têm o formato xRy, onde x e y são rótulos. Informalmente uma fórmula rotulada $x : A$ tem o sentido $\mathcal{M} \models_x A$. Assim as regras do sistema K que foram acrescentadas para $\Box$ e $\diamond$, manipulam fórmulas rotuladas e fórmulas relacionais, servindo de certa maneira de interface entre as duas. O sistema K possui então as regras seguintes:

$$\begin{array}{ccc}
\begin{array}{c}[x:A]\\ \vdots \\ x:B\end{array} & \begin{array}{c}[xRy]\\ \vdots \\ y:A\end{array} & \\
\hline
x:A\to B\ {\scriptstyle \to I} & x:\Box A\ {\scriptstyle \Box I} & \dfrac{y:A \quad xRy}{x:\diamond A}\ {\scriptstyle \diamond I}
\end{array}$$

$$\begin{array}{cccc}
\begin{array}{c}[x:A\to\bot]\\ \vdots \\ y:\bot\end{array} & & & \begin{array}{c}[y:A][xRy]\\ \vdots \\ s:\diamond A \quad z:B\end{array} \\
\hline
x:A\ {\scriptstyle \bot E} & \dfrac{x:A\to B \quad x:A}{x:B}\ {\scriptstyle \to E} & \dfrac{x:\Box A \quad xRy}{y:A}\ {\scriptstyle \Box E} & z:B\ {\scriptstyle \diamond E}
\end{array}$$

PUC-Rio - Certificação Digital Nº 0016017/CA

Sendo que em $\Box I$, y é diferente de x e não ocorre em nenhuma hipótese de $y : A$ que não seja xRy; em $\diamond E$, y é diferente de x e z e não ocorre em nenhuma hipótese de $z : B$ (premissa) que não seja uma das duas indicadas, $y : A$ e xRy.

O resultado é um sistema correto e completo para a lógica K. O interessante é que de maneira incremental pode-se passar a outras lógicas modais, desde que sejam caracterisadas por teorias relacionais de Horn. Isso abrange todas as mais usuais. Estas teorias são incorporadas por meio de regras que se unem às regras já contidas em K. Assim por exemplo, se acrescentarmos a regra:

$$\overline{xRx}$$

às regras de K, obtem-se um sistema dedutivo para KT.

Isto resulta numa hierarquia de lógicas, uma vez que o acréscimo incremental de regras permite passar de uma lógica a outra. Por exemplo, acrescentando-se a regra de transitividade a KT obtem-se KT4 (S4).

O artigo mostra que todas as lógicas obtidas dessa maneira são corretas e completas em relação à semântica de Kripke associada.

PUC-Rio - Certificação Digital Nº 0016017/CA

5.3.2 Substituições

Uma propriedade desejada em sistemas de dedução natural é que as provas sejam "fechadas sob substituição". Isto significa que podemos substituir uma hipótese por uma prova desta hipótese, de tal maneira que a árvore resultante continua sendo uma prova. Porém há casos em que isso não funciona. Em lógica modal, S4 por exemplo, é comum termos a seguinte regra:

$$\dfrac{\begin{array}{c}\Box A_1, ..., \Box A_n \\ \vdots \\ B\end{array}}{\Box B}\,\Box I$$

ou seja, se todas as hipóteses de B são da forma $\Box A$, então podemos deduzir $\Box B$.

Suponha agora que substituamos $\Box A_1$ pela seguinte prova de $\Box A_1$:

$$\frac{C \to \Box A_1 \quad C}{\Box A_1} \to E$$

Teremos então a seguinte árvore:

$$\frac{\dfrac{C \to \Box A_1 \quad C}{\Box A_1} \to E \qquad \begin{matrix} \\ \\ \vdots \\ B \end{matrix} \quad , ..., \Box A_n}{\Box B} \Box I$$

que não será uma prova válida, pois a aplicação de $\Box I$ não é correta. Logo as provas deste sistema não são fechadas sob substituição.
Uma solução para este problema é encontrada em [Alechina1998], onde a regra $\Box I$ é substituida por:

$$\frac{\begin{matrix} \vdots & & \vdots & & [\Box A_1, ..., \Box A_n] \\ \Box A_1 & ... & \Box A_n & & \vdots \\ & & & & B \end{matrix}}{\Box B} \Box I$$

onde todas as hipóteses de B são eliminadas e reintroduzidas.
Neste trabalho usaremos outra solução.

5.4 O sistema $\mathcal{CN}$

O sistema $\mathcal{CN}$ de dedução natural para CTL não tem os mesmos símbolos primitivos. Aqui $\exists(A \sim B)$ (que será explicado a seguir) e $[\exists G]A$ são os conectivos primitivos, e com eles expressamos todas as modalidades de CTL.

PUC-Rio - Certificação Digital Nº 0016017/CA

5.4.1 Sintaxe

A sintaxe é dada por:

$A := p| \perp| A_1 \rightarrow A_2| [\forall X]A| [\exists G]A| \exists(A_1 \sim A_2)$

5.4.2 Semântica

Considera-se um frame serial $\mathcal{F} = (S, R)$, e $\mathcal{M}$ um modelo de $\mathcal{F}$. Um $R-branch$ começando em s é uma seqüência infinita $s_0, ..., s_n, ...$ com $s = s_0$ e $s_n R s_{n+1}$ para todo n. Um $R-path$ é uma versão finita de um $R-branch$ (como antes).

Assim sendo:

$\mathcal{M} \models_s [\forall X]A$ sse $sRt \Rightarrow \mathcal{M} \models_t A$

$\mathcal{M} \models_s [\exists G]A$ sse existe um $R-branch$ $s = s_0 R s_1 ...$ tal que $\mathcal{M} \models_{s_i} A$ para todo $i \in N$.

$\mathcal{M} \models_s \exists(A \sim B)$ sse existe um $R-path$ $s = s_0 ... s_k$ tal que $\mathcal{M} \models_k B$ e $\mathcal{M} \models_{s_i} A$ para todo i tal que $0 \leq i < k$, com $\underline{\mathbf{k > 0}}$.

Note que temos então $\mathcal{M} \models_s \exists(A \sim B) \Rightarrow \mathcal{M} \models_s A$, que é algo que não temos com $\exists(A\mathcal{U}B)$.

Desta maneira temos as seguintes abreviações:

$\exists(A\mathcal{U}B)$ para $B \vee \exists(A \sim B)$
$\forall(A\mathcal{U}B)$ para $\neg[\exists(\neg B\mathcal{U}(\neg A \wedge \neg B)) \vee [\exists G]\neg B]$

Justificação da abreviação: Para $\exists(A\mathcal{U}B)$, basta observar que $\exists(A \sim B)$ é equivalente a $A \wedge [\exists X]\exists(A\mathcal{U}B)$. Para $\forall(A\mathcal{U}B)$ vemos que uma maneira de negá-lo é negando A antes de obter B. Vemos que é o caso se $\exists(\neg B\mathcal{U}(\neg A \wedge \neg B))$ pois chegariamos em $\neg A \wedge \neg B$ (negando A) sem ter obtido ainda B. Mas há uma maneira de negar $\forall(A\mathcal{U}B)$ sem passar por $\neg A$: basta que B não se realize jamais.

5.4.3 Sistema dedutivo

Mas o sistema dedutivo não trabalha diretamente com as fórmulas que acabam de ser definidas, e sim com uma versão rotulada das fórmulas.

PUC-Rio - Certificação Digital Nº 0016017/CA

Definição

$i := i_0 \vert i_1 \vert ...$
$a := a_0 \vert a_1 \vert ...$
$l := i \vert l + a$
i é chamado de label inicial. a é chamado de elemento de label.
l é chamado de label.
L é o conjunto de todos os labels.

Uma fórmula rotulada tem então a forma A^l, onde A é uma fórmula e l é um label.

Um teorema de $\mathcal{CN}$ será então qualquer fórmula A para qual a fórmula rotulada A^i é obtida através do sistema dedutivo descrito a seguir, com todas as hipóteses canceladas.

No texto a seguir serão usados os símbolos $a, b, c, ...$ ao invés de $a_1, a_2, a_3, ...$

Informalmente, afirmar A^l significa que $\mathcal{M} \models_l A$. Quanto a $l+a$ deve ser visto como um sucessor de l, ou seja, temos sempre $(l)R(l+a)$. Se escrevermos $l+b$ também estamos afirmando que $(l)R(l+b)$. Assim $l+a, l+b, l+c, ...$ são todos sucessores de l. Só não se sabe se representam o mesmo sucessor de l. Uma notação provavelmente mais expressiva mais talvez menos prática seria $s_a(l)$, $s_b(l)$,...

Eis então as regras do sistema dedutivo.

(Atenção quanto ao uso da expressão "sub-derivação". Seu sentido está explicado na discussão ao final deste capítulo).

Regra 1:

$$\begin{array}{c} [A \rightarrow \bot^k] \\ \vdots \\ \dfrac{\bot^l}{A^k} \bot E \end{array}$$

PUC-Rio - Certificação Digital Nº 0016017/CA

Condições para aplicação: Nenhuma

Regra 2:

$$\frac{\begin{array}{c}[A^l]\\ \vdots\\ B^l\end{array}}{A \to B^l} \to I$$

Condições para aplicação: Nenhuma

Regra 3:

$$\frac{A^l \quad A \to B^l}{B^l} \to E$$

Condições para aplicação: Nenhuma

Regra 4:

$$\frac{[\forall X]A^l}{A^{l+a}} \forall E$$

Condições para aplicação: Nenhuma

Regra 5:

$$\frac{\begin{array}{c}A_1^{l_1}, ..., A_n^{l_n}\\ \vdots\\ A^{l+a}\end{array}}{[\forall X]A^l} \forall I$$

Condições para aplicação: a não ocorre em $l_1, ..., l_n$.

PUC-Rio - Certificação Digital Nº 0016017/CA

Regra 6:

$$\frac{[\exists G]A^l}{A^l}\, GE$$

Condições para aplicação: Nenhuma

Regra 7:

$$\frac{A^l \quad \exists(A \sim B)^{l+a}}{\exists(A \sim B)^l}\, \exists -$$

Condições para aplicação: Nenhuma

Regra 8:

$$\frac{A^l \quad B^{l+a}}{\exists(A \sim B)^l}\, \exists I$$

Condições para aplicação: Nenhuma

Regra 9:

$$\frac{A^l \quad [\exists G]A^{l+a}}{[\exists G]A^l}\, G-$$

Condições para aplicação: Nenhuma

PUC-Rio - Certificação Digital Nº 0016017/CA

Regra 10:

$$\dfrac{\begin{array}{cc} & A_1^{l_1}, ..., A_n^{l_n}, [[\exists G]A^{l+a}] \\ & \vdots \\ [\exists G]A^l & C^k \end{array}}{C^k} G+$$

Condições para aplicação: a não ocorre em $k, l_1, ..., l_n$.

Regra 11:

$$\dfrac{\begin{array}{ccc} & A_1^{l_1}, ..., A_n^{l_n}, [A^l, B^{l+a}] & B_1^{l'_1}, ..., B_m^{l'_m}, [A^l, \exists(A \sim B)^{l+b}] \\ & \vdots & \vdots \\ \exists(A \sim B)^l & C^k & C^k \end{array}}{C^k} \exists+$$

Condições para aplicação: nem a nem b ocorrem em $l, k, l_1, ..., l_n, l'_1, ..., l'_m$.

Regra 12:

$$\dfrac{\begin{array}{c} D \\ \neg[\forall X]\neg A^l \end{array}}{[\exists G]A^l} GInd$$

Condições para aplicação: existe uma sub-derivação de D (terminando em $\neg[\forall X]\neg A^l$) cujas hipóteses são todas ocorrências de A^l.

PUC-Rio - Certificação Digital Nº 0016017/CA

Regra 13:

$$\frac{\begin{array}{c} D \\ [\exists G]A^l \quad B^l \end{array}}{[\exists G]B^l} G =$$

Condições para aplicação: existe uma sub-derivação de D (terminando em B^l) cujas hipóteses estão contidas no conjunto $\{A^l\}$.

Regra 14:

$$\frac{\begin{array}{ccc} & D_1 & D_2 \\ \exists(A \sim B)^l & C^l & C^{l+a} \end{array}}{C^l} \exists E$$

Condições para aplicação: existe uma sub-derivação de D_1 cujas hipóteses estão contidas no conjunto $\{A^l, C^{l+a}\}$ e uma sub-derivação de D_2 cujas hipóteses estão contidas no conjunto $\{B^{l+a}\}$. Além do mais, se uma das sub-derivações consideradas for a própria árvore D_1 ou D_2, então as hipóteses do conjunto respectivo podem ser canceladas.

PUC-Rio - Certificação Digital Nº 0016017/CA

5.4.4 Comentários

Sub-derivação

Nas condições de aplicação de algumas regras é usada a expressão "sub-derivação". Este conceito, aqui, difere daquele usualmente encontrado na literatura. Em geral sub-derivação costuma designar uma derivação D' extraida de uma derivação D da seguinte forma: a partir de um certo ponto, corta-se tudo o que está abaixo. Ou seja, daquele ponto para cima a árvore fica intacta (sendo que algumas hipóteses que eram canceladas, podem deixar de ser).

Aqui sub-derivação tem um sentido mais genérico. Qualquer fragmento de derivação é uma sub-derivação, desde que a extração deste fragmento do todo não venha violar as condições de aplicação de alguma regra contida no fragmento. Assim não é necessário cortar apenas a parte da árvore que se situa abaixo de um certo ponto: pode ser cortar a parte da árvore que se situa acima de algum ponto.

Por exemplo a derivação:

$$\frac{A \quad B}{A \wedge B}$$

é uma sub derivação de:

$$\dfrac{\dfrac{A \wedge C}{\dfrac{A \qquad B}{A \wedge B}}}{B \rightarrow (A \wedge B)}$$

Até aqui a introdução deste conceito pode parecer confusa e inutil. Vejamos então um exemplo no qual a extração de uma sub-árvore não gera uma sub-derivação.

Considere a derivação seguinte:

$$\dfrac{\dfrac{\dfrac{\dfrac{p \wedge \neg\exists(\top \sim \neg p)^l}{\neg\exists(\top \sim \neg p)^l}\wedge E \quad \dfrac{[\neg p\ ^{l+a}]^1 \quad \overline{\top^l}}{\exists(\top \sim \neg p)^l}\exists I}{\dfrac{\bot}{p\ ^{l+a}}\bot E_1}\rightarrow E \quad \dfrac{\dfrac{p \wedge \neg\exists(\top \sim \neg p)^l}{\neg\exists(\top \sim \neg p)^l}\wedge E \quad \dfrac{[\exists(\top \sim \neg p)^{l+a}]^2 \quad \overline{\top^l}}{\exists(\top \sim \neg p)^l}\exists -}{\dfrac{\bot}{\neg\exists(\top \sim \neg p)^{l+a}}\rightarrow I_2}\rightarrow E}{\dfrac{p \wedge \neg\exists(\top \sim \neg p)^{l+a}}{\neg(p \wedge \neg\exists(\top \sim \neg p))^{l+a}}\wedge I} \quad \dfrac{[[\forall X]\neg(p \wedge \neg\exists(\top \sim \neg p))^l]^3}{\neg(p \wedge \neg\exists(\top \sim \neg p))^{l+a}}\forall E}{\dfrac{\dfrac{\bot}{\neg[\forall X]\neg(p \wedge \neg\exists(\top \sim \neg p))^l}\rightarrow I_3}{[\exists G](p \wedge \neg\exists(\top \sim \neg p))^l}GInd}\rightarrow E$$

O ponto crítico é a aplicação de $GInd$. Esta aplicação é correta pois a derivação em questão tem uma única hipótese (não cancelada):
$p \wedge \neg\exists(\top \sim \neg p)^l$.

Considere então a derivação obtida pelo simples acrécimo de
$A \wedge (p \wedge \neg\exists(\top \sim \neg p))^l$ acima da hipótese $p \wedge \neg\exists(\top \sim \neg p)^l$.

A árvore obtida tem agora duas hipóteses (não canceladas) distintas: $p \wedge \neg\exists(\top \sim \neg p)^l$ e $A \wedge (p \wedge \neg\exists(\top \sim \neg p))^l$. Mesmo assim a aplicação de $GInd$ está correta, pois existe uma sub-derivação (obtida simplesmente retirando o acrescimo que acabamos de colocar na derivação, e obtendo assim a derivação inicial) terminando em $\neg[\forall X]\neg(p \wedge \neg\exists(\top \sim \neg p))^l$, cuja única

PUC-Rio - Certificação Digital Nº 0016017/CA

hípotese é $p \wedge \neg\exists(\top \sim \neg p)^l$.

Enfim, eis um exemplo de árvore extraida que não é uma derivação:

$$\dfrac{\dfrac{\overset{\perp}{}}{\neg[\forall X]\neg(p \wedge \neg\exists(\top \sim \neg p))^l}\to I}{[\exists G](p \wedge \neg\exists(\top \sim \neg p))^l}\,GInd$$

A aplicação de $GInd$ é errada pois a derivação em questão não possui nenhuma sub-derivação terminando em $\neg[\forall X]\neg(p \wedge \neg\exists(\top \sim \neg p))^l$ cuja única hipótese seja $p \wedge \neg\exists(\top \sim \neg p)^l$.

Toda esta formulação das condições de aplicação não é necessaria para se obter completude ou correção. Ela serve apenas para facilitar o estudo das propriedades deste sistema. Mais precisamente ela fornece ao sistema a seguinte propriedade:

Se $\begin{matrix} D_1 \\ A \end{matrix}$ e $\begin{matrix} A & B_1 & B_2 & ... \\ & & D_2 & \\ & & C & \end{matrix}$

são duas derivações, então $\begin{matrix} & D_1 & & \\ \{A\} & B_1 & B_2 & ... \\ & & D_2 & \\ & & C & \end{matrix}$

também é uma derivação.

(Compare esta alternativa, por exemplo, com a alternativa usada em [Alechina1998] no tratamento de $\Box I$).

PUC-Rio - Certificação Digital Nº 0016017/CA

Paralelo com a lógica clássica

Algumas comparações com a lógica clássica [VanDalen1994] podem ajudar a entender as condições de aplicação de algumas regras.

A introdução de $\forall$ deve ser comparada com a introdução de $\forall$ na lógica clássica.

A regra $G+$ deve ser comparada à regra de eliminação de $\exists$ na lógica clássica.

A regra $\exists+$ deve ser comparada às regras de eliminação de $\vee$ e de eliminação de $\exists$ na lógica clássica, pois dessa maneira pode-se ver que a regra está apenas afirmando que:
$\mathcal{M} \models_s \exists(A \sim B)$ implica $(\mathcal{M} \models_s A$ e $\mathcal{M} \models_t B)$ ou $(\mathcal{M} \models_s A$ e $\mathcal{M} \models_t \exists(A \sim B))$, para algum t tal que sRt.

5.4.5 Algumas provas

Vejamos então alguns exemplos de prova.

K_X

$K_X : [\forall X](A \to B) \to ([\forall X]A \to [\forall X]B)$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{[[\forall X](A \to B)^i]^2}{A \to B^{i+a}}\forall E \quad \dfrac{[[\forall X]A^i]^1}{A^{i+a}}\forall E}{B^{i+a}} \to E}{[\forall X]B^i}\forall I}{[\forall X]A \to [\forall X]B^i} \to I_1}{[\forall X](A \to B) \to ([\forall X]A \to [\forall X]B)^i} \to I_2$$

Observe que a aplicação de $\forall I$ respeita a restrição de a não ocorrer nas hipóteses. Perceba também que embora tenhamos obtido a conclusão com label i, poderiamos ter usado qualquer outro label, como por exemplo j, ou $i + b$.

PUC-Rio - Certificação Digital Nº 0016017/CA

D_X

$D_X : [\exists X]\top$

$$\dfrac{\dfrac{\dfrac{[[\forall X]\neg\neg\bot^{i}]^{2}}{\neg\neg\bot^{i+a}}\forall E \quad \dfrac{[\bot^{i+a}]^{1}}{\neg\bot^{i+a}}\rightarrow I_1}{\bot}\rightarrow E}{\neg[\forall X]\neg\neg\bot^{i}}\rightarrow I_2$$

Observe a ocorrência de $\bot$ sem label nenhum. A rigor, deveria ser $\bot^{i+a}$. Mas pela regra $\bot E$ podemos deduzir $\bot^j$ de $\bot^i$ quaisquer que sejam i e j. Em outras palavras, quando obtemos uma contradição em um mundo específico, esta contradição se "espalha"para todos os mundos.

5.5 Completude

Nesta seção a completude do cálculo é provada. Para isso é usada a axiomatização de CTL que foi usada na exposição que fizemos de CTL. Desta maneira basta reproduzir os axiomas e as regras de inferência mencionadas: como o sistema possui modus ponem, ele será automaticamente capaz de efetuar qualquer prova que seja feita com a versão axiomática, usando a tradução aqui indicada.

Desta forma, esta parte consiste essencialmente em provas realizadas em $\mathcal{CN}$, uma para cada axioma e para cada regra de inferência.

Recapitulamos aqui os axiomas e as regras de inferência:

$K_X : [\forall X](A \rightarrow B) \rightarrow ([\forall X]A \rightarrow [\forall X]B)$
$D_X : [\exists X]\top$
$\exists\mathcal{U} : \exists(A\mathcal{U}B) \leftrightarrow (B \vee (A \wedge [\exists X]\exists(A\mathcal{U}B)))$
$\forall\mathcal{U} : \forall(A\mathcal{U}B) \leftrightarrow (B \vee (A \wedge [[\forall X]]\forall(A\mathcal{U}B)))$

$Necessitation : \vdash A \ \Rightarrow \vdash [\forall X]A$
$\exists - Ind : \vdash (B \vee (A \wedge [\exists X]C) \rightarrow C \ \Rightarrow \vdash \exists(A\mathcal{U}B) \rightarrow C$
$\forall - Ind : \vdash (B \vee (A \wedge [\forall X]C) \rightarrow C \ \Rightarrow \vdash \forall(A\mathcal{U}B) \rightarrow C$

PUC-Rio - Certificação Digital Nº 0016017/CA

5.5.1 Abreviações

Para realizar as provas algumas abreviações são úteis. Usaremos então as seguintes regras, pois tornam as provas mais legíveis.

$$\frac{A}{A \vee B} \vee I$$

$$\frac{B}{A \vee B} \vee I$$

$$\frac{\begin{array}{ccc} & [A] & [B] \\ & \vdots & \vdots \\ A \vee B & C & C \end{array}}{C} \vee E$$

$$\frac{A \wedge B}{A} \wedge E$$

$$\frac{A \wedge B}{B} \wedge E$$

$$\frac{A \quad B}{A \wedge B} \wedge I$$

Essas regras são justificadas pelas provas seguintes:

PUC-Rio - Certificação Digital Nº 0016017/CA

$$\dfrac{\dfrac{A \quad [\neg A]}{\dfrac{\bot}{B}\,\bot E}\,\to E}{\neg A \to B}\,\to I$$

$$\dfrac{B}{\neg A \to B}\,\to I$$

$$\dfrac{\dfrac{\dfrac{\dfrac{[C \to \bot] \quad \begin{array}{c}[A]\\ \vdots\\ C\end{array}}{\bot}\,\to E}{A \to \bot}\,\to I \qquad (A \to \bot) \to B}{B}\,\to E \qquad \begin{array}{c}B\\ \vdots\\ C\end{array} \qquad [C \to \bot]}{\dfrac{\bot}{C}\,\bot E}\,\to E$$

$$\dfrac{\dfrac{\dfrac{[\neg A] \quad [A]}{\bot}\,\to E}{\neg B}\,\bot E}{A \to \neg B}\,\to I \qquad \neg(A \to \neg B)}{\dfrac{\bot}{A}\,\bot E}\,\to E$$

$$\dfrac{\dfrac{[\neg B]}{A \to \neg B}\,\to I \qquad \neg(A \to \neg B)}{\dfrac{\bot}{B}\,\bot E}\,\to E$$

PUC-Rio - Certificação Digital Nº 0016017/CA

$$\dfrac{\dfrac{\dfrac{A \quad [A \to \neg B]}{\neg B} \to E \qquad B}{\bot} \to E}{\neg(A \to \neg B)} \to I$$

Passamos agora às provas.

5.5.2 Axiomas

K_X

$K_X : [\forall X](A \to B) \to ([\forall X]A \to [\forall X]B)$

(vide seção 4.5.1)

D_X

$D_X : [\exists X]\top$

(vide seção 4.5.2)

Na sequência é importante lembrar das abreviações:

$\exists(A\mathcal{U}B)$ para $B \vee \exists(A \sim B)$
$\forall(A\mathcal{U}B)$ para $\neg(\neg A \wedge \neg B) \wedge \neg\exists(\neg B \sim (\neg A \wedge \neg B)) \wedge \neg[\exists G]\neg B$

$\exists\mathcal{U}$

$\exists\mathcal{U} : \exists(A\mathcal{U}B) \leftrightarrow (B \vee (A \wedge [\exists X]\exists(A\mathcal{U}B)))$

$\to$:

PUC-Rio - Certificação Digital Nº 0016017/CA

Como $\exists(A\mathcal{U}B)$ é $B \vee \exists(A \sim B)$, a prova pode ser feita em duas partes: $B \rightarrow B \vee (A \wedge [\exists X]\exists(A\mathcal{U}B))$ (que é evidente) e $\exists(A \sim B) \rightarrow B \vee (A \wedge [\exists X]\exists(A\mathcal{U}B))$ que segue abaixo:

PUC-Rio - Certificação Digital Nº 0016017/CA

PUC-Rio - Certificação Digital Nº 0016017/CA

$$\dfrac{\exists(A \sim B)^i \qquad \dfrac{\dfrac{[A^i]^3 \qquad \dfrac{\dfrac{\dfrac{[[\forall X]\neg(B \vee \exists(A \sim B))^i]^1}{\neg(B \vee \exists(A \sim B))^{i+a}}\forall E \quad \dfrac{[B^{i+a}]^4}{(B \vee \exists(A \sim B))^{i+a}}\vee I}{\bot}\to E}{\neg[\forall X]\neg(B \vee \exists(A \sim B))^i}\to I_1}{A \wedge \neg[\forall X]\neg(B \vee \exists(A \sim B))^i}\wedge I \qquad \dfrac{[A^i]^3 \qquad \dfrac{\dfrac{\dfrac{[[\forall X]\neg(B \vee \exists(A \sim B))^i]^2}{\neg(B \vee \exists(A \sim B))^{i+a}}\forall E \quad \dfrac{[\exists(A \sim B)^{i+b}]^5}{(B \vee \exists(A \sim B))^{i+a}}\vee I}{\bot}\to E}{\neg[\forall X]\neg(B \vee \exists(A \sim B))^i}\to I_2}{A \wedge \neg[\forall X]\neg(B \vee \exists(A \sim B))^i}\wedge I}{A \wedge \neg[\forall X]\neg(B \vee \exists(A \sim B))^i}\exists +_{3,4,5}}{B \vee (A \wedge \neg[\forall X]\neg(B \vee \exists(A \sim B)))^i}\vee I$$

$\leftarrow$:

Na prova a seguir falta $A \wedge \neg[\forall X]\neg(B \vee \exists(A \sim B)) \vdash \exists(A \sim B)$ que está explicitada logo em seguida:

PUC-Rio - Certificação Digital Nº 0016017/CA

PUC-Rio - Certificação Digital Nº 0016017/CA

$$\dfrac{B \vee (A \wedge \neg[\forall X]\neg(B \vee \exists(A \sim B)))^{i} \quad \dfrac{[B^{i}]^{1}}{B \vee \exists(a \sim B)^{i}} \vee I \qquad \begin{array}{c}[A \wedge \neg[\forall X]\neg(B \vee \exists(A \sim B))^{i}]^{2} \\ \vdots \\ \dfrac{\exists(A \sim B)^{i}}{B \vee \exists(A \sim B)^{i}} \vee I \end{array}}{B \vee \exists(A \sim B)^{i}} \vee E_{1,2}$$

$$\dfrac{\dfrac{A \wedge \neg[\forall X]\neg(B \vee \exists(A \sim B))^{i}}{\neg[\forall X]\neg(B \vee \exists(A \sim B))^{i}} \wedge E \quad \dfrac{\dfrac{\dfrac{\dfrac{\dfrac{A \wedge \neg[\forall X]\neg(B \vee \exists(A \sim B))^{i}}{A^{i}} \wedge E \quad [B^{i+a}]^{1}}{\exists(A \sim B)^{i}} \exists I \quad \dfrac{\dfrac{A \wedge \neg[\forall X]\neg(B \vee \exists(A \sim B))^{i}}{A^{i}} \wedge E \quad [\exists(A \sim B)^{i+a}]^{2}}{\exists(A \sim B)^{i}} \exists -}{\exists(A \sim B)^{i}} \vee E_{1,2} \quad [B \vee \exists(A \sim B)^{i+a}]^{3}}{\exists(A \sim B)^{i}} \quad \dfrac{\dfrac{\dfrac{\bot}{\neg(B \vee \exists(A \sim B))^{i+a}} \to I_{3}}{[\forall X]\neg(B \vee \exists(A \sim B))^{i}} \forall I \quad [\neg\exists(A \sim B)^{i}]^{4}}{\bot} \to E}{\bot} \to E}{\exists(A \sim B)^{i}} \bot E_{4}$$

$\forall \mathcal{U}$

$\forall \mathcal{U} : \forall(A \mathcal{U} B) \leftrightarrow (B \vee (A \wedge [[\forall X]] \forall(A \mathcal{U} B)))$

$\rightarrow$:

Na prova a seguir é assumido que $\neg(B \vee (A \wedge ([\forall X]\forall(A \mathcal{U} B))) \vdash \neg B$, que resulta da lógica clássica. Fora isso falta provar que $\neg(B \vee (A \wedge [\forall X]\forall(A \mathcal{U} B))^i, \forall(A \mathcal{U} B)^i \vdash \neg(\neg A \wedge \neg B) \wedge \neg\exists(\neg B \sim (\neg A \wedge \neg B)) \wedge \neg[\exists G]\neg B^{i+a}$ que está explicitada logo em seguida na forma de três provas:

PUC-Rio - Certificação Digital Nº 0016017/CA

PUC-Rio - Certificação Digital Nº 0016017/CA

$$
\dfrac{
\dfrac{
\dfrac{
\dfrac{\forall(A\mathcal{U}B)^i}{\neg(\neg A \wedge \neg B)^i}\,\wedge E
\qquad
\dfrac{[\neg A^i]^1 \qquad \dfrac{[\neg(B \vee (A \wedge [\forall X]\forall(A\mathcal{U}B))^i]^2}{\neg B^i}}{\neg A \wedge \neg B^i}\,\wedge I
}{
\dfrac{\bot}{A^i}\,\bot E_1
}\,\to E
\qquad
\dfrac{
\begin{matrix}[\neg(B \vee (A \wedge [\forall X]\forall(A\mathcal{U}B))^i]^2 \quad \forall(A\mathcal{U}B)^i \\ \vdots \\ \neg(\neg A \wedge \neg B) \wedge \neg\exists(\neg B \sim (\neg A \wedge \neg B)) \wedge \neg[\exists G]\neg B^{i+a}\end{matrix}
}{[\forall X]\forall(A\mathcal{U}B)^i}\,\forall I
}{
\dfrac{A \wedge [\forall X]\forall(A\mathcal{U}B)^i}{B \vee (A \wedge [\forall X]\forall(A\mathcal{U}B))^i}\,\vee I
}\,\wedge I
\qquad
[\neg(B \vee (A \wedge [\forall X]\forall(A\mathcal{U}B)))^i]^2
}{
\dfrac{\bot}{B \vee (A \wedge [\forall X]\forall(A\mathcal{U}B))^i}\,\bot E_2
}\,\to E
$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\neg(B \vee (A \wedge [\forall X]\forall(A\mathcal{U}B))^i}{\neg B^i} \quad \dfrac{[\neg A \wedge \neg B^{i+a}]^1}{\exists(\neg B \sim (\neg A \wedge \neg B))^i}\exists I \quad \dfrac{\forall(A\mathcal{U}B)^i}{\neg\exists(\neg B \sim (\neg A \wedge \neg B))^i}\wedge E}{\bot}\to E}{\neg(\neg A \wedge \neg B)^{i+a}}\to I_1$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\forall(A\mathcal{U}B)^i}{\neg\exists(\neg B \sim (\neg A \wedge \neg B))^i}\wedge E \quad \dfrac{\dfrac{\neg(B \vee (A \wedge [\forall X]\forall(A\mathcal{U}B))^i}{\neg B^i} \quad \dfrac{[\exists(\neg B \sim (\neg A \wedge \neg B))^{i+a}]^1}{\exists(\neg B \sim (\neg A \wedge \neg B))^i}\exists-}{\bot}\to E}{\neg\exists(\neg B \sim (\neg A \wedge \neg B))^{i+a}}\to I_1$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\forall(A\mathcal{U}B)^i}{\neg[\exists G]\neg B^i}\wedge E \quad \dfrac{\dfrac{\neg(B \vee (A \wedge [\forall X]\forall(A\mathcal{U}B))^i}{\neg B^i} \quad \dfrac{[[\exists G]\neg B^{i+a}]^1}{[\exists G]\neg B^i}G-}{\bot}\to E}{\neg[\exists G]\neg B^{i+a}}\to I_1$$

$\leftarrow$:

As três provas a seguir constituem a prova de $A \wedge [\forall X]\forall(A\mathcal{U}B) \vdash \forall(A\mathcal{U}B)$, nas quais foram omitidas (indicadas por uma linha dupla) provas do tipo $[\forall X](A \wedge B)^i \vdash [\forall X]A^i$

$$\dfrac{\dfrac{\dfrac{A \wedge [\forall X]\forall(A\mathcal{U}B)^i}{A^i}\wedge E \quad \dfrac{[\neg A \wedge \neg B^i]^1}{\neg A^i}\wedge E}{\bot}\to E}{\neg(\neg A \wedge \neg B)^i}\to I_1$$

PUC-Rio - Certificação Digital Nº 0016017/CA

PUC-Rio - Certificação Digital Nº 0016017/CA

$$\dfrac{[\exists(\neg B \sim (\neg A \wedge \neg B))^{i}]^{3} \quad \dfrac{\dfrac{[\exists(\neg B \sim (\neg A \wedge \neg B))^{i+b}]^{1} \quad \dfrac{A \wedge [\forall X]\forall(A\mathcal{U}B)^{i}}{[\forall X]\neg\exists(\neg B \sim (\neg A \wedge \neg B))^{i}}\forall E}{\neg\exists(\neg B \sim (\neg A \wedge \neg B))^{i+b}} \quad \dfrac{[\neg A \wedge \neg B^{i+a}]^{2} \quad \dfrac{A \wedge [\forall X]\forall(A\mathcal{U}B)^{i}}{[\forall X]\neg(\neg A \wedge \neg B)^{i}}\forall E}{\neg(\neg A \wedge \neg B)^{i+a}} \to E}{\bot}\to E}{\bot}\exists +_{1,2}$$

$$\dfrac{\bot}{\neg\exists(\neg B \sim (\neg A \wedge \neg B))^{i}} \to I_3$$

$$\dfrac{\dfrac{\dfrac{\dfrac{A \wedge [\forall X]\forall(A\mathcal{U}B)^{i}}{[\forall X]\neg[\exists G]\neg B^{i}}\wedge E}{\neg[\exists G]\neg B^{i+a}}\forall E \qquad \dfrac{}{[[\exists G]\neg B^{i+a}]^{1}}}{\dfrac{[[\exists G]\neg B^{i}]^{2} \qquad \bot}{\bot}\, G{+}_{1}}\to E}{\neg[\exists G]\neg B^{i}}\to I_{2}$$

Com isso, o que vem a seguir acaba de provar $B \vee (A \wedge [\forall X]\forall(A\mathcal{U}B)) \to \forall(A\mathcal{U}B)$

PUC-Rio - Certificação Digital Nº 0016017/CA

PUC-Rio - Certificação Digital Nº 0016017/CA

$$\dfrac{B \vee (A \wedge [\forall X]\forall(A\mathcal{U}B))^i \qquad \dfrac{\dfrac{\dfrac{\dfrac{[\neg A \wedge \neg B^i]^1}{\neg B^i}\wedge E \quad [B^i]^5}{\bot}\to E}{\neg(\neg A \wedge \neg B)^i}\to I_1 \qquad \dfrac{\dfrac{\dfrac{[\exists(\neg B \sim (\neg A \wedge \neg B))^i]^3[\neg B^i]^2[\neg B^i]^2}{\neg B^i}\exists+_2 \quad [B^i]^5}{\bot}\to E}{\neg\exists(\neg B \sim (\neg A \wedge \neg B))^i}\to I_3 \qquad \dfrac{\dfrac{\dfrac{[[\exists G]\neg B^i]^4}{\neg B^i}GE \quad [B^i]^5}{\bot}\to E}{\neg[\exists G]\neg B^i}\to I_4}{\forall(A\mathcal{U}B)^i}\wedge I \qquad \begin{array}{c}[A \wedge [\forall X]\forall(A\mathcal{U}B)^i]^6\\ \vdots \\ \forall(A\mathcal{U}B)^i\end{array}}{\forall(A\mathcal{U}B)^i}\vee E_{5,6}$$

5.5.3 Regras de inferência

Passamos agora às provas das regras de inferência, que são:

$Necessitation : \vdash A \ \Rightarrow \vdash [\forall X]A$
$\exists - Ind : \vdash (B \vee (A \wedge [\exists X]C) \rightarrow C \ \Rightarrow \vdash \exists(A\mathcal{U}B) \rightarrow C$
$\forall - Ind : \vdash (B \vee (A \wedge [\forall X]C) \rightarrow C \ \Rightarrow \vdash \forall(A\mathcal{U}B) \rightarrow C$

Necessitation

Para isso precisamos de um teorema:

Teorema 1

Se D é uma derivação, i um label inicial, e a um elemento de label que não ocorre em D, então a substituição de i por $i + a$ na derivação D resulta em uma derivação.

Prova

Por indução no número de aplicações de regras de inferência na derivação D.

Para provar *Necessitation* basta dizer então que se $\vdash A$, é porque existe uma prova $\begin{matrix} D \\ A^i \end{matrix}$ na qual todas as hipóteses foram canceladas.

Logo, pelo teorema 1, escolhendo a que não ocorre na derivação, substituindo i por $i + a$ e acrescentando uma ultima aplicação da regra $\forall I$ obtemos:

$$\frac{\begin{matrix} D' \\ A^{i+a} \end{matrix}}{[\forall X]A^i} \forall I$$

Como essa derivação não tem hipótese (não cancelada), temos $\vdash [\forall X]A$

PUC-Rio - Certificação Digital Nº 0016017/CA

$\exists - Ind$

$\exists - Ind : \vdash (B \vee (A \wedge [\exists X]C)) \rightarrow C \ \Rightarrow \vdash \exists(A \mathcal{U} B) \rightarrow C$

$$\dfrac{\exists(A \sim B)^{l} \qquad \dfrac{\dfrac{\dfrac{[A^{l}]^{1}}{B \vee (A \wedge [\exists X]C)^{l}} \quad \dfrac{\dfrac{[C^{l+a}]^{2}}{\neg[\forall X]\neg C^{l}}}{\neg[\forall X]\neg C^{l}}}{C^{l}} \quad \dfrac{}{B \vee (A \wedge [\exists X]C) \rightarrow C^{l}} \vdash}{C^{l}} \rightarrow E \quad \dfrac{\dfrac{\dfrac{[B^{l+a}]^{3}}{B \vee (A \wedge [\exists X]C)^{l+a}} \vee I \quad \dfrac{}{B \vee (A \wedge [\exists X]C) \rightarrow C^{l+a}} \vdash}{C^{l+a}} \rightarrow E}{C^{l}} \exists E_{1,2,3}$$

A isso acrescenta-se a prova de $B^{l} \vdash C^{l}$ para terminar a prova de $\exists - Ind$:

$$\dfrac{\dfrac{\dfrac{B^{l}}{B \vee (A \wedge [\exists X]C)^{l}} \vee I \quad \dfrac{}{(B \vee (A \wedge [\exists X]C)) \rightarrow C^{l}} \vdash}{C^{l}} \rightarrow E$$

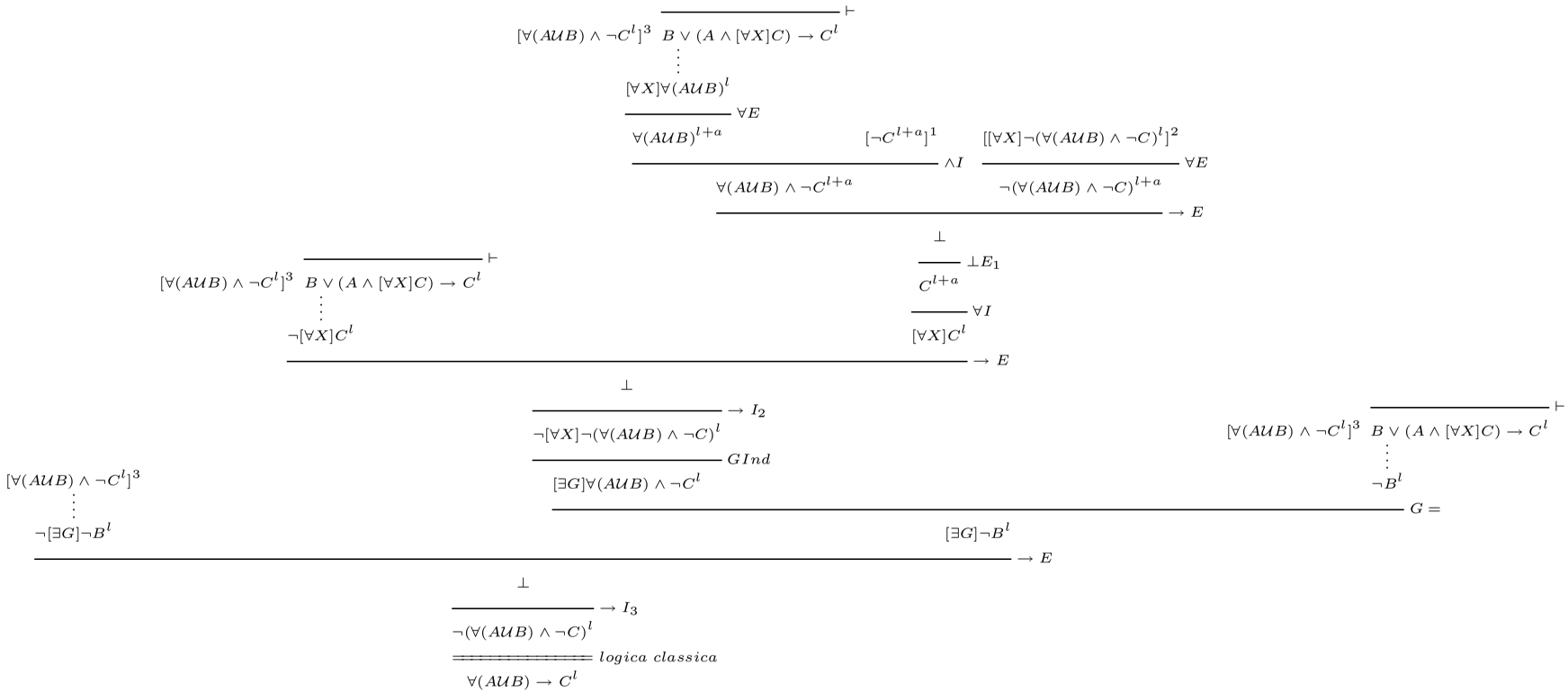
$\forall - Ind$

$\forall - Ind : \vdash (B \vee (A \wedge [\forall X]C) \rightarrow C \ \Rightarrow \vdash \forall(A \mathcal{U} B) \rightarrow C$

A estrutura geral da prova é dada por:

PUC-Rio - Certificação Digital Nº 0016017/CA

PUC-Rio - Certificação Digital Nº 0016017/CA



Só falta então explicar as quatro derivações que não foram explicitadas:

$$\begin{array}{c} \forall(A\mathcal{U}B) \wedge \neg C^l \\ \vdots \\ \neg[\exists G]\neg B^l \end{array} \qquad \forall(A\mathcal{U}B) \wedge \neg C^l \quad \dfrac{}{B \vee (A \wedge [\forall X]C) \to C^l}\vdash \quad \begin{array}{c} \vdots \\ \neg B^l \end{array}$$

$$\forall(A\mathcal{U}B) \wedge \neg C^l \quad \dfrac{}{B \vee (A \wedge [\forall X]C) \to C^l}\vdash \quad \begin{array}{c} \vdots \\ \neg[\forall X]C^l \end{array} \qquad \forall(A\mathcal{U}B) \wedge \neg C^l \quad \dfrac{}{B \vee (A \wedge [\forall X]C) \to C^l}\vdash \quad \begin{array}{c} \vdots \\ [\forall X]\forall(A\mathcal{U}B)^l \end{array}$$

As duas primeiras são evidentes. Eis então a terceira ($l.c.$ significa lógica clássica):

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\forall(A\mathcal{U}B) \wedge \neg C^l}{\neg C^l}\wedge E \quad \dfrac{}{B \vee (A \wedge [\forall X]C) \to C^l}\vdash}{\neg B \wedge \neg(A \wedge [\forall X]C)}\, l.c.}{(\neg B \wedge \neg A) \vee (\neg B \wedge \neg[\forall X]C)}\, l.c. \quad \dfrac{\forall(A\mathcal{U}B) \wedge \neg C^l}{\forall(A\mathcal{U}B)^l}\wedge E}{\neg B \wedge \neg[\forall X]C}\, l.c.}{\neg[\forall X]C^l}\, l.c.$$

A quarta, enfim, foi dividida em três partes:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\forall(A\mathcal{U}B) \wedge \neg C^l}{\neg C^l}\wedge E \quad \dfrac{}{B \vee (A \wedge [\forall X]C) \to C^l}\vdash}{\neg B \wedge \neg(A \wedge [\forall X]C)^l}\, l.c.}{\neg B^l}\wedge E \quad \dfrac{\dfrac{\dfrac{[\neg A \wedge \neg B^{l+a}]^2 \quad [\neg B^l]^1}{\exists(\neg B \sim (\neg A \wedge \neg B))^l}\exists I \quad \dfrac{\forall(A\mathcal{U}B) \wedge \neg C^l}{\forall(A\mathcal{U}B)}\wedge E}{\bot}\, l.c.}{B^l}\bot E_1}{\bot}\to E}{\neg(\neg A \wedge \neg B)^{l+a}}\to I_2$$

PUC-Rio - Certificação Digital Nº 0016017/CA

$$\dfrac{\dfrac{\dfrac{\forall(A\mathcal{U}B)\wedge\neg C^l \quad \dfrac{}{B\vee(A\wedge[\forall X]C)\to C^l}\vdash}{\neg B^l}\,l.c. \qquad \dfrac{[\exists(\neg B\sim(\neg A\wedge\neg B))^{l+a}]^1}{\exists(\neg B\sim(\neg A\wedge\neg B))^l}\exists-}{\bot}\to E}{\neg\exists(\neg B\sim(\neg A\wedge\neg B))^{l+a}}\to I_1 \qquad \dfrac{\dfrac{\forall(A\mathcal{U}B)\wedge\neg C^l}{\forall(A\mathcal{U}B)}\wedge E}{\neg\exists(\neg B\sim(\neg A\wedge\neg B))^l}\wedge E$$

$$\dfrac{\dfrac{\dfrac{\forall(A\mathcal{U}B)\wedge\neg C^l \quad \dfrac{}{B\vee(A\wedge[\forall X]C)\to C^l}\vdash}{\neg B^l}\,l.c. \qquad \dfrac{[[\exists G]\neg B^{l+a}]^1}{[\exists G]\neg B^l}G-}{\bot}\to E}{\neg[\exists G]\neg B^{l+a}}\to I_1 \qquad \dfrac{\dfrac{\forall(A\mathcal{U}B)\wedge\neg C^l}{\forall(A\mathcal{U}B)^l}\wedge E}{\neg[\exists G]\neg B^l}\wedge E$$

Isto encerra então a prova de que $\mathcal{CN}$ é completo

5.6 Correção

Nesta parte trata-se de provar que tudo que se prova em $\mathcal{CN}$ é correto, ou seja, também é verdade em CTL.

Embora a prova da completude tenha sido feita sintaticamente, (tratamos de reproduzir um sistema axiomático já existente), a prova da correção não poderia ser feita da mesma maneira. Isso porque o uso de fórmulas rotuladas permite provas não reproduzíveis em CTL. Por exemplo podemos provar que $[\forall X]A^i \vdash A^{i+a}$, o que não pode ser feito em CTL. Assim a prova a seguir será feita semanticamente, ou seja, provaremos que qualquer teorema obtido em $\mathcal{CN}$ é válido em todo frame serial.

Para isso provaremos uma propriedade mais forte, que não diz respeito unicamente a teoremas, mas diz respeito também a provas com hipóteses não canceladas. Os teoremas serão apenas um subconjunto das provas que podemos obter em $\mathcal{CN}$.

PUC-Rio - Certificação Digital Nº 0016017/CA

Para isso algumas definições são introduzidas.

5.6.1 Definições e lemas

Definição 1

$i := i_0|i_1|...$

$a := a_0|a_1|...$

$l := i|l + a$

i é chamado de label inicial. a é chamado de elemento de label.

l é chamado de label.

L é o conjunto de todos os labels.

Observe que todo l é finito, e assim L é um conjunto enumerável.

Definição 2

Uma valoração é uma função $v : L \rightarrow S$ tal que $v(l) = s$ e $v(l + a) = t$ implica sRt.

Definição 3

$\mathcal{M} \models_v A^l$ é, por definição: $\mathcal{M} \models_{v(l)} A$

Definição 4: fórmula $\exists(A \sim B)$

$\mathcal{M} \models_s \exists(A \sim B)$ significa que existe um $R - path\ s = s_0, ..., s_k$ no qual $\mathcal{M} \models_{s_i} A$ para todo $i < k$, e $\mathcal{M} \models_{s_k} B$, **com k > 0**.

Definição 5: fórmula $[\exists G]A$

$\mathcal{M} \models_s [\exists G]A$ significa que existe um $R - branchs = s_0, ..., s_n, ...$ no qual $\mathcal{M} \models_{s_i} A$ para $i \in N$

Dois lemas são usados com freqüencia na prova:

PUC-Rio - Certificação Digital Nº 0016017/CA

Lema 1

Se v é uma valoração e a não ocorre nos labels $l_1, ..., l_n$ e $v(l)Rs$, então existe uma valoração $\overline{v}$ tal que $\overline{v}(l_i) = v(l_i)$ para todo i de 1 a n, e $\overline{v}(l + a) = s$.

Lema2

Se v é uma valoração e $v(l)Rs$, então existe v' tal que $v'(l) = s$.

Prova dos lemas 1 e 2

A prova dos dois lemas é trivial usando o axioma da escolha.

5.6.2 Prova

A prova da correção propriamente dita consiste em provar que para toda derivação de $\mathcal{CN}$:

$$\begin{array}{l} A_1^{l_1}, ..., A_n^{l_n} \\ \quad D \\ \quad A^l \end{array}$$

e para todo modelo $\mathcal{M}$ sobre um frame serial $\mathcal{F} = (S, R)$ e toda valoração $v : L \to S$,

$(\mathcal{M} \models_{\mathbf{v}} \mathbf{A_i^{l_i}}$ **para todo** $\mathbf{i} \in [\mathbf{1}, \mathbf{n}])$ **implica** $\mathcal{M} \models_{\mathbf{v}} \mathbf{A^l}$

Assim vemos que uma conseqüência direta desta prova será que se A^i é teorema de $\mathcal{CN}$, então para todo $\mathcal{M}$ e toda v:

$(\mathcal{M} \models_v A_i^{l_i}$ para todo $i \in \emptyset)$ implica $\mathcal{M} \models_v A^i$.

Como a premissa é trivialmente verdadeira, isso implica que para todo $\mathcal{M}$ e para toda v, $\mathcal{M} \models_v A^i$, ou seja, $\mathcal{M} \models_{v(i)} A$.

Vemos então que se A não fosse um teorema de CTL, haveria um modelo

PUC-Rio - Certificação Digital Nº 0016017/CA

$\mathcal{M}$ com mundo s tal que $\mathcal{M} \not\models_s A$. Tomando então v tal que $v(i) = s$, teriamos $\mathcal{M} \not\models_{v(i)} A$.

Logo se A^i é teorema de $\mathcal{CN}$, A é teorema de CTL. (É neste sentido que o sistema é correto.)

A prova é feita por indução no número de inferências, ou seja, é necessário percorrer cada regra e verificar que ela seja correta. São quatorze regras.

Regra 1:

$$\begin{array}{l}[A \to \bot^k] \\ \quad\vdots \\ \quad \bot^l \\ \hline A^k \end{array} \bot E$$

Condições para aplicação: Nenhuma

Prova:

$\mathcal{M} \models_{v(k)} A \to \bot \;\Rightarrow\; \mathcal{M} \models_{v(l)} \bot$. Como certamente $\mathcal{M} \not\models_{v(l)} \bot$, então $\mathcal{M} \not\models_{v(k)} A \to \bot$. Logo $\mathcal{M} \models_{v(k)} A$.

PUC-Rio - Certificação Digital Nº 0016017/CA

Regra 2:

$$\frac{\begin{array}{c}[A^l]\\ \vdots\\ B^l\end{array}}{A \to B^l} \to I$$

Condições para aplicação: Nenhuma

Prova:

$(\mathcal{M} \models_{v(l)} A \;\Rightarrow\; \mathcal{M} \models_{v(l)} B) \;\Rightarrow\; \mathcal{M} \models_{v(l)} A \to B$

Regra 3:

$$\frac{A^l \quad A \to B^l}{B^l} \to E$$

Condições para aplicação: Nenhuma

Prova:

$(\mathcal{M} \models_{v(l)} A \text{ e } \mathcal{M} \models_{v(l)} A \to B) \;\Rightarrow\; \mathcal{M} \models_{v(l)} B$

PUC-Rio - Certificação Digital Nº 0016017/CA

Regra 4:

$$\frac{[\forall X]A^l}{A^{l+a}}\,\forall E$$

Condições para aplicação: Nenhuma

Prova:

$\mathcal{M} \models_v [\forall X]A^l \;\Rightarrow\; \mathcal{M} \models_{v(l)} [\forall X]A \;\Rightarrow\; \mathcal{M} \models_{v(l+a)} A$ pois $v(l)Rv(l+a)$.

Regra 5:

$$\begin{array}{c} A_1^{l_1}, ..., A_n^{l_n} \\ \vdots \\ A^{l+a} \\ \hline [\forall X]A^l \end{array}\,\forall I$$

Condições para aplicação: a não ocorre em $l_1, ..., l_n$.

Prova:

Se não fosse verdade, existiria v tal que $\forall i(\mathcal{M} \models_v A_i^{l_i})$ e $\mathcal{M} \not\models_v [\forall X]A^l$, ou seja, teriamos $v(l)Rs$ com $\mathcal{M} \not\models_s A$. Logo, pelo Lema 1, contradiríamos a $H.I.$

PUC-Rio - Certificação Digital Nº 0016017/CA

Regra 6:

$$\frac{[\exists G]A^l}{A^l}\, GE$$

Condições para aplicação: Nenhuma

Prova:

$\mathcal{M} \models_v [\exists G]A^l \;\Rightarrow\; \mathcal{M} \models_{v(l)} [\exists G]A \;\Rightarrow\; \mathcal{M} \models_{v(l)} A$ por definição.

Regra 7:

$$\frac{A^l \quad \exists(A \sim B)^{l+a}}{\exists(A \sim B)^l}\, \exists-$$

Condições para aplicação: Nenhuma

Prova:

($\mathcal{M} \models_v A^l$ e $\mathcal{M} \models_v \exists(A \sim B)^{l+a}$) $\Rightarrow$ ($\mathcal{M} \models_{v(l)} A$ e $\mathcal{M} \models_{v(l+a)} \exists(A \sim B)$). Como $v(l)Rv(l+a)$, temos, pela def. de $\exists(A \sim B)$, que $\mathcal{M} \models_{v(l)} \exists(A \sim B)$.

PUC-Rio - Certificação Digital Nº 0016017/CA

Regra 8:

$$\frac{A^l \quad B^{l+a}}{\exists(A \sim B)^l}\,\exists I$$

Condições para aplicação: Nenhuma

Prova:

($\mathcal{M} \models_v A^l$ e $\mathcal{M} \models_v B^{l+a}$) $\Rightarrow$ ($\mathcal{M} \models_{v(l)} A$ e $\mathcal{M} \models_{v(l+a)} B$). Como $v(l)Rv(l+a)$, temos, pela def. de $\exists(A \sim B)$, que $\mathcal{M} \models_{v(l)} \exists(A \sim B)$.

Regra 9:

$$\frac{A^l \quad [\exists G]A^{l+a}}{[\exists G]A^l}\,G-$$

Condições para aplicação: Nenhuma

Prova:

($\mathcal{M} \models_v A^l$ e $\mathcal{M} \models_v [\exists G]A^{l+a}$) $\Rightarrow$ ($\mathcal{M} \models_{v(l)} A$ e $\mathcal{M} \models_{v(l+a)} [\exists G]A$). Como $v(l)Rv(l+a)$, temos, pela def. de $[\exists G]A$, que $\mathcal{M} \models_{v(l)} [\exists G]A$.

PUC-Rio - Certificação Digital Nº 0016017/CA

Regra 10:

$$\dfrac{[\exists G]A^{l} \qquad \begin{array}{c} A_1^{l_1}, ..., A_n^{l_n}, [[\exists G]A^{l+a}] \\ \vdots \\ C^{k} \end{array}}{C^{k}} G+$$

Condições para aplicação: a não ocorre em $k, l_1, ..., l_n$.

Prova:

Supomos $\mathcal{M} \models_v [\exists G]A^l$ e $\mathcal{M} \models_v A_i^{l_i}$ para $i \in [1, n]$. Logo $v(l) = s_0Rs_1R...Rs_nR...$ com $\mathcal{M} \models_{s_i} A$ para todo $i \in N$. Pelo Lema 1 temos $\overline{v}$ tal que $\overline{v}(l_i) = v(l_i), \overline{v}(k) = v(k)$ e $\overline{v}(l + a) = s_1$. Logo $\mathcal{M} \models_{\overline{v}} [\exists G]A^{l+a}$. Como também $\mathcal{M} \models_{\overline{v}} A_i^{l_i}$ pois $\overline{v}(l_i) = v(l_i)$, e usando a $H.I.$, temos $\mathcal{M} \models_{\overline{v}} C^k$. Logo $\mathcal{M} \models_{\overline{v}(k)} C \Rightarrow \mathcal{M} \models_{v(k)} C \Rightarrow \mathcal{M} \models_v C^k$.

Regra 11:

$$\dfrac{\exists(A \sim B)^{l} \qquad \begin{array}{c} A_1^{l_1}, ..., A_n^{l_n}, [A^l, B^{l+a}] \\ \vdots \\ C^{k} \end{array} \qquad \begin{array}{c} B_1^{l'_1}, ..., B_m^{l'_m}, [A^l, \exists(A \sim B)^{l+b}] \\ \vdots \\ C^{k} \end{array}}{C^{k}} \exists+$$

Condições para aplicação: nem a nem b ocorrem em $l, k, l_1, ..., l_n, l'_1, ..., l'_m$.

Prova:

Supomos que $\mathcal{M} \models_v \exists(A \sim B)^l$, $\mathcal{M} \models_v A_i^{l_i}$, e $\mathcal{M} \models_v B_j^{l_j}$. Logo $\mathcal{M} \models_{v(l)} \exists(A \sim B)$. Assim, já temos $\mathcal{M} \models_{v(l)} A$. Além disso, de duas uma (ao menos): ou existe s tal que $v(l)Rs$ e $\mathcal{M} \models_s B$, ou existe s tal que $v(l)Rs$ e $\mathcal{M} \models_s \exists(A \sim B)$.

No primeiro caso, pelo Lema 1, existe $\overline{v}$ tal que $\overline{v} = v$ em todos os labels, com exceção de $l + a$, tendo $\overline{v}(l + a) = s$. Assim temos $\mathcal{M} \models_{\overline{v}(l)} A$ e $\mathcal{M} \models_{\overline{v}(l+a)} B$. Pela $H.I.$ (a primeira das duas derivações que levam a C^k), temos então $\mathcal{M} \models_{\overline{v}(k)} C$. Como $\overline{v}(k) = v(k)$, tenho $\mathcal{M} \models_v C^k$.

PUC-Rio - Certificação Digital Nº 0016017/CA

No segundo caso, a prova é semelhante.

Regra 12:

$$\frac{\begin{array}{c} D \\ \neg[\forall X]\neg A^l \end{array}}{[\exists G]A^l}\, GInd$$

Condições para aplicação: existe uma sub-derivação de D (terminando em $\neg[\forall X]\neg A^l$) cujas hipóteses são ocorrências de A^l.

Prova:

Supomos que $\mathcal{M} \models_v A^l$. Logo pela $H.I.$ $\mathcal{M} \models_v \neg[\forall X]\neg A^l$. Logo existe s tal que $v(l)Rs$ e $\mathcal{M} \models_s A$. Pelo lema 2 temos v' tal que $v'(l) = s$. Logo $\mathcal{M} \models_{v'(l)} A$. Logo, pela $H.I.$, $\mathcal{M} \models v'(l)\neg[\forall X]\neg A$. Logo existe t tal que $v'(l)Rt$ (ou seja tal que $v(l)RsRt$) e $\mathcal{M} \models_t A$. E continuando assim podemos obter uma cadeia infinita.

Regra 13:

$$\frac{\begin{array}{cc} & D \\ [\exists G]A^l & B^l \end{array}}{[\exists G]B^l}\, G =$$

Condições para aplicação: existe uma sub-derivação de D (terminando em B^l) cujas hipóteses estão contidas no conjunto $\{A^l\}$.

Prova:

Supomos que $\mathcal{M} \models_{v(l)} [\exists G]A$. Logo existe uma sequência $v(l) = s_0Rs_1R...Rs_nR...$ com $\mathcal{M} \models_{s_i} A$ para todo $i \in N$. Como $\mathcal{M} \models_{s_0} [\exists G]A$, então $\mathcal{M} \models_{s_0} A$. Logo pela prova D, $\mathcal{M} \models_{s_0} B$. Como s_0Rs_1, pelo lema 2 temos v' tal que $v'(l) = s_1$. Assim $\mathcal{M} \models_{v'(l)} A$. Logo pela prova D, $\mathcal{M} \models_{v'(l)} B$, ou seja, $\mathcal{M} \models_{s_1} B$. E assim por diante.

PUC-Rio - Certificação Digital Nº 0016017/CA

Regra 14:

$$\frac{\begin{array}{ccc} & D_1 & D_2 \\ \exists(A \sim B)^l & C^l & C^{l+a} \end{array}}{C^l} \exists E$$

Condições para aplicação: existe uma sub-derivação de D_1 cujas hipóteses estão contidas no conjunto $\{A^l, C^{l+a}\}$ e uma sub-derivação de D_2 cujas hipóteses estão contidas no conjunto $\{B^{l+a}\}$. Além do mais, se uma das sub-derivações consideradas for a própria árvore D_1 ou D_2, então as hipóteses do conjunto respectivo podem ser canceladas.

Prova:

Supomos $\mathcal{M} \models_v \exists(A \sim B)^l$. Logo existe uma sequência $v(l) = s_0 R s_1 R ... R s_k$ tal que $\mathcal{M} \models_{s_i} A$ para $i < k$, e $\mathcal{M} \models_{s_k} B$. Pela aplicação do lema 2 obtemos v' tal que $v'(l) = s_1$. Aplicando o lema 2 sucessivamente, chegamos a $v_0(l) = s_{k-1}$, e aplicando então o lema 1 otemos $\overline{v_0}$ tal que $\overline{v_0}(l) = s_{k-1}$ e $\overline{v_0}(l+a) = s_k$. Logo $\mathcal{M} \models_{\overline{v_0}} B^{l+a}$. Por D_2 deduzimos então que $\mathcal{M} \models_{\overline{v_0}} C^{l+a}$. Logo $\mathcal{M} \models_{\overline{v_0}} C^{l+a}$ e $\mathcal{M} \models_{\overline{v_0}} A^l$. Por D_1 deduzimos então que $\mathcal{M} \models_{\overline{v_0}} C^l$, ou seja, $\mathcal{M} \models_{s_{k-1}} C$.
Da mesma forma que obtivemos $\overline{v_0}$, obtemos $\overline{v_1}$ com $\overline{v_1}(l) = s_{k-2}$ e $\overline{v_1}(l+a) = s_{k-1}$, que nos permite deduzir $\mathcal{M} \models_{s_{k-2}} C$. E continuamos assim até obter $\overline{v_{k-1}}$ tal que $\overline{v_{k-1}}(l) = s_0$ e $\overline{v_{k-1}}(l+a) = s_1$, sendo que já teremos provado que $\mathcal{M} \models_{s_1} C$, ou seja, que $\mathcal{M} \models_{\overline{v_{k-1}}} C^{l+a}$. Com $\mathcal{M} \models_{\overline{v_{k-1}}} A^l$ e D_1 obtemos então $\mathcal{M} \models_{\overline{v_{k-1}}} C^l$, ou seja, $\mathcal{M} \models_v C^l$.

5.7 Normalização

5.7.1 Noções de Teoria da Prova

O que se pretende neste capítulo é normalizar as provas. Para definir o que significa normalizar, algumas definições são necessárias.

PUC-Rio - Certificação Digital Nº 0016017/CA

Definição 1

A ocorrência α de uma fórmula é uma *fórmula máxima*, se α é a conclusão de uma regra de introdução e a premissa maior de uma regra de eliminação. Numa regra de eliminação com mais de uma premissa, é chamada de *premissa maior* aquela que contém o conectivo sendo eliminado.

Definição 2

Uma prova é normal se não contém fórmulas máximas.

O que se deseja então é mostrar que toda prova pode ser transformada numa prova normal.

Isto tenta ser feito procurando cada fórmula máxima da prova, e mostrando que existe uma redução que transforma a prova em questão numa prova sem a dita fórmula máxima.

Uma noção também importante será a noção de caminho. Um caminho é uma seqüência de fórmulas extraidas de uma prova. Em geral um caminho começa numa hipótese e segue passando para a conclusão α da regra da qual a tal hipótese é premissa, e em seguida passa para a conclusão da regra da qual α é hipótese, e assim por diante. Porém os caminhos não seguem essa ordem no caso das regra $\exists+,\ \exists E,\ G+\ e\ G=$, como será explicitado adiante.

Assim, ao efetuarmos a eliminação dos cortes de uma prova, não consideraremos a árvore formada pela prova, mas sim a árvore formada pelos caminhos que se encontram na prova. Teremos então o cuidado de observar que após as reduções propostas, a árvore de caminhos continuará correspondendo a uma prova.

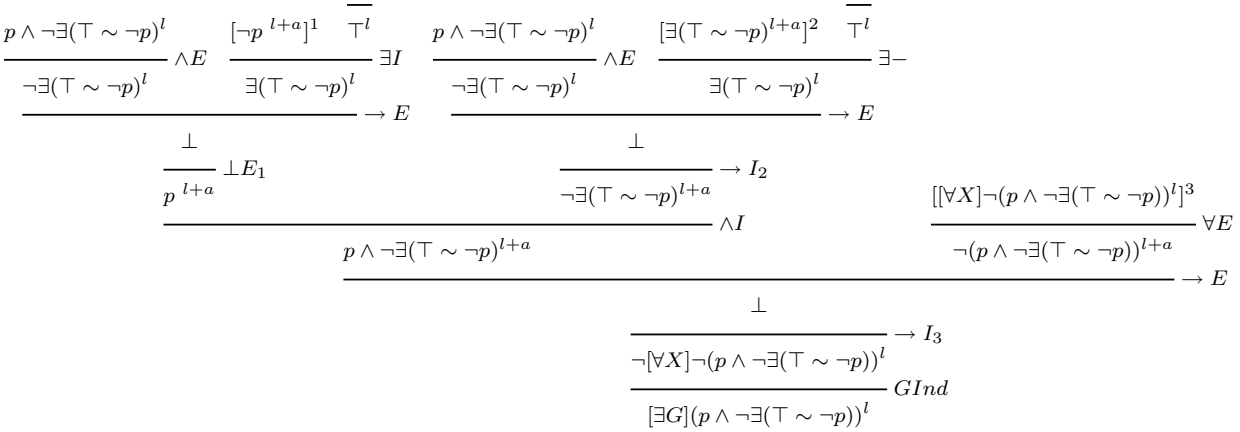
Desta forma não precisamos nos preocupar com regras permutativas [VanDalen1994].

5.7.2 Investigando $\mathcal{CN}$

Esta seção começa investigando a propriedade da sub-fórmula. Mais precisamente, é mostrado que o sistema $\mathcal{CN}$ não satisfaz a propriedade da sub-fórmula. Esta propriedade afirma que para toda prova, existe uma prova equivalente cujas fórmulas são todas sub-fórmulas das hipóteses ou da conclusão. Assim será exibido um exemplo de prova que não pode ser realizada sem passar por fórmulas que não sejam sub-fórmulas das hipóteses ou da conclusão.

PUC-Rio - Certificação Digital Nº 0016017/CA

A prova em questão é: $p \wedge \neg\exists(\top \sim \neg p) \vdash [\exists G]p$
Eis uma prova:



PUC-Rio - Certificação Digital Nº 0016017/CA

Supõe-se então que exista uma prova de $p \wedge \neg\exists(\top \sim \neg p) \vdash [\exists G]p$ que só use sub-fórmulas de $p \wedge \neg\exists(\top \sim \neg p)$ ou $[\exists G]p$. Logo esta prova não pode usar as regras $GInd$ ou $G=$, pois violariam obrigatoriamente a propriedade da sub-fórmula, uma vez que p é atômica. Vejamos então como terminaria uma prova cuja conclusão é $[\exists G]p$.

Não pode ser a conclusão de uma regra de eliminação, ou a regra teria uma premissa que não é sub-fórmula das hipóteses ou da conclusão. Se for a conclusão de uma das regras cuja conclusão é uma das premissas (mas com label diferente) então o mesmo problema existe para a tal premissa: como obtê-la? Também não provém de uma regra de introdução pois já eliminamos $GInd$ ou $G=$.

Logo não existe prova de $p \wedge \neg\exists(\top \sim \neg p) \vdash [\exists G]p$ que só use sub-fórmulas de $\{p \wedge \neg\exists(\top \sim \neg p), [\exists G]p\}$. Assim o sistema $\mathcal{CN}$ não tem a propriedade da sub-fórmula.

Para explorarmos um pouco mais o problema podemos observar se o sistema nos permite eliminar "fórmulas máximas". Pelo que acabamos de ver ele certamente não permite, mas talvez um fragmento do cálculo $\mathcal{CN}$ permita.

5.7.3 Reduções

Para verificar se as fórmulas máximas desse sistema são elimináveis, é necessário estudar um a um os conectivos $\exists(... \sim ...)$, $[\exists G]$ e $[\forall X]$.

Redução para $\forall$

A redução é semelhante à redução usada para $\forall x$ em lógica de primeira ordem [Prawitz1965]:

$$\dfrac{\dfrac{\begin{array}{c}D\\A^{l+a}\end{array}}{[\forall X]A^{l}}\,\forall I}{A^{l+b}}\,\forall E \quad \text{reduz para} \quad \begin{array}{c}D[a \leftarrow b]\\A^{l+b}\end{array}$$

Reduções para $\exists$

O tratamento deste caso é mais complexo, por causa da quantidade de regras associadas a $\exists$.

Para facilitar, quebramos a regra $\exists+$ em duas regras distintas, que chamamos de $\exists E*$ e $\exists +*$.

$$\dfrac{\exists(A \sim B)^{l} \qquad \begin{array}{c}A_1^{l_1}, ..., A_n^{l_n}, [A^{l}, B^{l+a}]\\\vdots\\C^{k}\end{array} \qquad \begin{array}{c}B_1^{l'_1}, ..., B_m^{l'_m}, [A^{l}, \exists(A \sim B)^{l+b}]\\\vdots\\C^{k}\end{array}}{C^{k}}\,\exists +$$

é substituida pelas regras

$$\dfrac{\exists(A \sim B)^{l}}{A^{l}}\,\exists E*$$

e

PUC-Rio - Certificação Digital Nº 0016017/CA

$$\dfrac{\exists(A \sim B)^{l} \qquad \begin{array}{c} A_1^{l_1}, ..., A_n^{l_n}, [B^{l+a}] \\ \vdots \\ C^{k} \end{array} \qquad \begin{array}{c} B_1^{l'_1}, ..., B_m^{l'_m}, [\exists(A \sim B)^{l+b}] \\ \vdots \\ C^{k} \end{array}}{C^{k}} \exists + *$$

Considera-se então que em toda aplicação de $\exists + *$ as hipóteses B^{l+a} e $\exists(A \sim B)^{l+b}$ ocorrem e são canceladas (se não fosse o caso teriamos uma redução evidente).

Precisamos agora definir os caminhos que ocorrem numa derivação. Em vez de definirmos textualmente dizendo algo do tipo *"Toda seqüência $A_1, A_2, ..., A_n$ onde A_i é premissa maior de A_{i+1}, ou A_i é $\exists(A \sim B)$ e A_{i+1} é uma das hipóteses canceladas numa aplicação de $\exists + *$, ou ..."*[Prawitz1965], faremos um diagrama representando os caminhos possíveis.

Uma aplicação de $\exists + *$ dá origem aos caminhos seguintes:

$$\dfrac{\exists(A \sim B)^{l}}{\begin{array}{c} B^{l+a} \\ \vdots \\ C^{k} \end{array}} \quad \text{e} \quad \dfrac{\exists(A \sim B)^{l}}{\begin{array}{c} \exists(A \sim B)^{l+a} \\ \vdots \\ C^{k} \end{array}}$$

PUC-Rio - Certificação Digital Nº 0016017/CA

Uma aplicação de $\exists E$ dá origem aos dois caminhos seguintes:

$$\dfrac{\exists(A \sim B)^l}{A^l} \qquad \begin{array}{c} \dfrac{\exists(A \sim B)^l}{B^{l+a}} \\ \vdots \\ C^{l+a} \end{array}$$
$$\vdots$$
$$C^l$$

Os caminhos gerados por $\exists E*$, $\exists -$ e $\exists I$ são evidentes.

Podemos encarar $\exists E*$ e $\exists E$ como regras de eliminação, $\exists I$ como regra de introdução, $\exists -$ como uma regra de propagação, e $\exists + *$ como uma regra de propagação e introdução.

Assim não basta apenas analisar os casos onde uma regra de introdução é seguida de uma regra de eliminação: precisamos analisar o caso onde uma regra de introdução é seguida por um número arbitrário de regras de propagação, seguidas por uma regra de eliminação, pois neste caso também teremos uma fórmula máxima.

As reduções seguintes resolvem todos os casos.

PUC-Rio - Certificação Digital Nº 0016017/CA

$\underline{\exists I \text{ seguida de } \exists + *}$

$$\dfrac{\dfrac{A^l \quad B^{l+a}}{\exists(A \sim B)^l}\exists I \qquad \begin{array}{c} A_1^{l_1}, ..., A_n^{l_n}, [B^{l+a}] \\ \vdots \\ C^k \end{array} \qquad \begin{array}{c} B_1^{l'_1}, ..., B_m^{l'_m}, [\exists(A \sim B)^{l+b}] \\ \vdots \\ C^k \end{array}}{C^k}\exists + *$$

reduz para

$$\begin{array}{c} A_1^{l_1}, ..., A_n^{l_n}, B^{l+a} \\ \vdots \\ C^k \end{array}$$

$\underline{\exists I \text{ seguida de } \exists E*}$

$$\dfrac{\dfrac{A^l \quad B^{l+a}}{\exists(A \sim B)^l}\,\exists I}{A^l}\,\exists E* \qquad \text{reduz para} \qquad A^l$$

$\underline{\exists I \text{ seguida de } \exists E}$

$$\dfrac{\dfrac{A^l \quad B^{l+a}}{\exists(A \sim B)^l}\,\exists I \qquad \begin{matrix} A^l,\ C^{l+a} \\ \vdots \\ C^l \end{matrix} \qquad \begin{matrix} B^{l+a} \\ \vdots \\ C^{l+a} \end{matrix}}{C^l}\,\exists E$$

reduz para

$$\begin{matrix} & B^{l+a} \\ & \vdots \\ A^l, & C^{l+a} \\ & \vdots \\ & C^l \end{matrix}$$

PUC-Rio - Certificação Digital Nº 0016017/CA

$\underline{\exists-\text{ seguida de } \exists+*}$

$$\dfrac{\dfrac{A^l \quad \exists(A\sim B)^{l+a}}{\exists(A\sim B)^l}\exists- \qquad \begin{array}{c} A_1^{l_1},...,A_n^{l_n},[B^{l+a}] \\ \vdots \\ C^k \end{array} \qquad \begin{array}{c} B_1^{l'_1},...,B_m^{l'_m},[\exists(A\sim B)^{l+b}] \\ D \\ C^k \end{array}}{C^k}\exists+*$$

reduz para

$$\begin{array}{c} B_1^{l'_1},...,B_m^{l'_m},\exists(A\sim B)^{l+a} \\ D[b\leftarrow a] \\ C^k \end{array}$$

pois b não ocorre em $k, l'_1, ..., l'_m$.

$\underline{\exists-\text{ seguida de } \exists E*}$

$$\dfrac{\dfrac{A^l \quad \exists(A\sim B)^{l+a}}{\exists(A\sim B)^l}\exists-}{A^l}\exists E* \qquad \text{reduz para} \qquad A^l$$

PUC-Rio - Certificação Digital Nº 0016017/CA

$\underline{\exists I \text{ seguida de um número arbitrário de } \exists -, \text{ seguidas de } \exists E}$

$$\dfrac{\dfrac{A^{l+a_1+\ldots+a_{n-3}} \quad \dfrac{\dfrac{A^{l+a_1+\ldots+a_{n-2}} \quad \dfrac{A^{l+a_1+\ldots+a_{n-1}} \quad B^{l+a_1+\ldots+a_n}}{\exists(A \sim B)^{l+a_1+\ldots+a_{n-1}}}\exists I}{\exists(A \sim B)^{l+a_1+\ldots+a_{n-2}}}\exists -}{\vdots}}{\dfrac{A^l \qquad \exists(A \sim B)^{l+a_1}}{\exists(A \sim B)^l}\exists -}$$

$$\dfrac{\exists(A \sim B)^l \qquad \begin{array}{cc} A^l & B^{l+a} \\ \vdots & \vdots \\ A^l & C^{l+a} \\ & \vdots \\ & C^l \end{array}}{}\exists E$$

reduz para

$$\begin{array}{ccc} & & B^{l+a_1+\ldots+a_n} \\ & & \vdots \\ & A^{l+a_1+\ldots+a_{n-1}} & C^{l+a_1+\ldots+a_n} \\ & \vdots & \vdots \\ A^{l+a_1+\ldots+a_{n-2}} & C^{l+a_1+\ldots+a_{n-1}} & \\ \vdots & & \\ A^l \qquad C^{l+a_1} & & \\ \vdots & & \\ C^l & & \end{array}$$

PUC-Rio - Certificação Digital Nº 0016017/CA

$\underline{\exists + * \text{ seguida de } \exists -}$

$$\dfrac{A^l \quad \dfrac{\exists(A \sim B)^l}{\exists(A \sim B)^{l+a}}\exists + *}{\exists(A \sim B)^l}\exists - \qquad \text{reduz para} \qquad \exists(A \sim B)^l$$

Reduções para $[\exists G]$

$\underline{G- \text{ seguida de } GE}$

$$\dfrac{A^l \quad [\exists G]A^{l+a}}{\dfrac{[\exists G]A^l}{A^l}\,GE}\,G- \qquad \text{reduz para} \qquad A^l$$

$\underline{G+ \text{ seguida de } G-}$

$$\dfrac{A^l \quad \dfrac{[\exists G]A^l}{[\exists G]A^{l+a}}\,G+}{[\exists G]A^l}\,G- \qquad \text{reduz para} \qquad [\exists G]A^l$$

$\underline{G- \text{ seguida de } G+}$

$$\dfrac{A^l \quad [\exists G]A^{l+a}}{\dfrac{[\exists G]A^l}{[\exists G]A^{l+a}}\,G+}\,G- \qquad \text{reduz para} \qquad [\exists G]A^{l+a}$$

$\underline{GInd \text{ seguida de } GE}$

PUC-Rio - Certificação Digital Nº 0016017/CA

$$\dfrac{\dfrac{\dfrac{\begin{array}{c}A^l\\ \vdots\\ \neg[\forall X]\neg A^l\end{array}}{[\exists G]A^l}\,GInd}{A^l}\,GE}{}$$

reduz para A^l

$\underline{G = \text{seguida de } GE}$

$$\dfrac{\dfrac{B^l}{[\exists G]B^l}\,G=}{B^l}\,GE$$

reduz para B^l

$\underline{GInd \text{ seguida de um número arbitrário de } G+ \text{ seguidas de } GE}$

$$\dfrac{\dfrac{\dfrac{\dfrac{\begin{array}{c}A^l\\ \vdots\\ \neg[\forall X]\neg A^l\end{array}}{[\exists G]A^l}\,GInd}{[\exists G]A^{l+a_1}}\,G+}{\begin{array}{c}\vdots\\ [\exists G]A^{l+a_1+\ldots+a_n}\end{array}}}{A^{l+a_1+\ldots+a_n}}\,GE}{\begin{array}{c}\vdots\\ C^k\end{array}}$$

reduz para

PUC-Rio - Certificação Digital Nº 0016017/CA

$$\dfrac{\begin{array}{c} \\ \\ A^{l} \\ \vdots \\ \neg[\forall X]\neg A^{l}\end{array} \qquad \begin{array}{c}\dfrac{\begin{array}{c}[A^{l+a_1+\ldots+a_{n-2}}] \\ \vdots \\ \neg[\forall X]\neg A^{l+a_1+\ldots+a_{n-2}}\end{array} \qquad \dfrac{\begin{array}{c}[A^{l+a_1+\ldots+a_{n-1}}] \\ \vdots \\ \neg[\forall X]\neg A^{l+a_1+\ldots+a_{n-1}}\end{array} \qquad \begin{array}{c}[A^{l+a_1+\ldots+a_{n}}] \\ \vdots \\ C^k\end{array}}{C^k}}{C^k} \\ \vdots \\ C^k\end{array}}{C^k}$$

<u>$G =$ seguida de um número arbitrário de $G+$ seguidas de GE</u>

$$\begin{array}{c}[\exists G]A^{l} \\ \vdots \\ \dfrac{\dfrac{B^{l}}{[\exists G]B^{l}}\,G=}{[\exists G]B^{l+a_1}}\,G+ \\ \vdots \\ \dfrac{[\exists G]B^{l+a_1+\ldots+a_n}}{B^{l+a_1+\ldots+a_n}}\,GE \\ \vdots \\ C^k\end{array}$$

reduz para

$$\begin{array}{c}\dfrac{[\exists G]A^{l}}{[\exists G]A^{l+a_1}}\,G+ \\ \vdots \\ [\exists G]A^{l+a_1+\ldots+a_n} \\ \vdots \\ B^{l+a_1+\ldots+a_n} \\ \vdots \\ C^k\end{array}$$

PUC-Rio - Certificação Digital Nº 0016017/CA

Esclarecimentos

As reduções que acabam de ser apresentadas merecem preparativos suplementares. Optou-se em apresentá-las sem os devidos preparativos para tornar a apresentação mais leve. Seguem agora alguns esclarecimentos.

Antes de mais nada é bom observar que se essas reduções fossem perfeitas o cálculo seria normalizável. Mas elas não são perfeitas. Isto acontece porque algumas regras têm condições sobre as hipóteses de alguma sub-árvore da premissa. Porém, na maioria das vezes isso não é problema já que as reduções não acrescentam hipóteses. O problema surge com a regra $G=$, que requer que suas hipóteses tenham a forma $[\exists G]A$. Assim, a redução para $GInd$ seguida de GE elimina a fórmula máxima $[\exists G]A^l$, sem considerar que essa fórmula era talvez essencial para uma aplicação da regra $G=$ que viesse abaixo. Assim sendo essa redução não é satisfatória. (Observe que as outras reduções, inclusive $G=$ seguida de GE, não apresentam esse problema). Sendo a única redução problemática, conclui-se que o cálculo seria normalizável se não tivessemos uma das três regras: $GInd$, $G=$, ou GE. Essa incompatibilidade entres essas regras nos faz pensar naquelas provas por indução nas quais devemos provar uma propriedade mais forte do que a desejada para depois derivarmos a propriedade desejada (mais fraca): essa propriedade mais forte é justamente a fórmula máxima eliminada na redução de $GInd$ seguida de GE.

Outro aspecto dessas reduções que requer esclarecimento é a escolha das váriaveis. As provas assumem que se existe uma prova de $A^l \vdash B^l$ então existe uma prova de $A^{l+a} \vdash B^{l+a}$. Para provar tal propriedade são necessários dois cuidados que não foram tomados:
primeiro que as restrições do tipo *a não pode ocorrer em l* são muito fortes e poderiam ser reformuladas para proibir a ocorrência de a numa posição específica do label l. Por exemplo, se de A^{i+a} provamos B^{i+a+a}, então seria permitido concluir $[\forall X]B^{i+a}$, pois a restrição seria siplesmente: *"a não pode ocorrer como segundo elemento de label nas hipóteses"*. O fato de ele ocorrer como primeiro elemento em A^{i+a} não tem importância.
Segundo, que é necessária uma maior liberdade na renomeação das variáveis. Para isso seria necessário uma noção de equivalência entre provas que só diferem nos nomes das variáveis. Essa consideração é semelhante ao cuidado

PUC-Rio - Certificação Digital Nº 0016017/CA

tomado em lógica clássica quando se introduz a noção de variável própria.

5.8 Conclusão

Cabe aqui mencionar uma tentativa feita para cáculo de seqüêntes [Echagüe1993], embora não tenha tido nenhuma influência sobre o nosso trabalho.

5.8.1 Cálculo de seqüêntes

O artigo se chama A Gentzen-System for Computation Tree Logic [Echagüe1993].

Para realizar o seu sistema o autor achou preferível usar outros conectivos fundamentais, e derivar os conectivos de CTL a partir deles. Assim ele não usa "until"como conectivo primitivo. Seus connectivos primitivos são $A...U_w^>...$, e $E...U_w^>...$, cujos sentidos são:

$\mathcal{M} \models_s AfU_w^>g$ sse para todo $R-branch\ s = s_0, s_1, ...$ temos: $\mathcal{M} \models_s f$ para $i \geq 1$, ou, existe $j \geq 1$ tal que $\mathcal{M} \models_{s_i} f$ para $j > i \geq 1$ e $\mathcal{M} \models_{s_j} g$

$\mathcal{M} \models_s EfU_w^>g$ sse s tem um sucessor e existe um $R - branch\ s = s_0, s_1, ...$ para o qual temos: $\mathcal{M} \models_s f$ para $i \geq 1$, ou, existe $j \geq 1$ tal que $\mathcal{M} \models_{s_i} f$ para $j > i \geq 1$ e $\mathcal{M} \models_{s_j} g$

Observe algumas diferenças: g pode não ocorrer nunca, f não precisa valer em s_0, e não adianta g valer em s_0. Também, percebe-se que o frame considerado não precisa ser serial (já que a explicação de $E...U_w^>...$ contém a frase "s tem um sucessor").

A partir desses conectivos são definidos todos os outros, inclusive $[\forall X]$.

Seu sistema é constituido então pelas regras a seguir:

$$\frac{}{f \ \Rightarrow \ f}(axi)$$

$$\frac{\Gamma_1 \ \Rightarrow \ \Delta_1, f \quad f, \Gamma_2 \ \Rightarrow \ \Delta_2}{\Gamma_1, \Gamma_2 \ \Rightarrow \ \Delta_1, \Delta_2}(cut)$$

$$\frac{\Gamma \ \Rightarrow \ \Delta}{\Gamma_1, \Gamma \ \Rightarrow \ \Delta_1, \Delta}(ext)$$

PUC-Rio - Certificação Digital Nº 0016017/CA

$$\frac{f, \Gamma \ \Rightarrow \ \Delta}{\Gamma \ \Rightarrow \ \Delta, \neg f}(\ \Rightarrow \neg)$$

$$\frac{\Gamma \ \Rightarrow \ \Delta, f}{\neg f, \Gamma \ \Rightarrow \ \Delta}(\neg \ \Rightarrow\ )$$

$$\frac{\Gamma \ \Rightarrow \ \Delta, f, g}{\Gamma \ \Rightarrow \ \Delta, f \vee g}(\ \Rightarrow \vee)$$

$$\frac{f, \Gamma \ \Rightarrow \ \Delta \quad g, \Gamma \ \Rightarrow \ \Delta}{f \vee g, \Gamma \ \Rightarrow \ \Delta}(\vee \ \Rightarrow\ )$$

$$\frac{\Gamma \ \Rightarrow \ \Delta}{AX\Gamma \ \Rightarrow \ AX \bigvee \Delta}(AX)$$

$$\frac{\Gamma \ \Rightarrow \ \Delta, AX(g \vee (f \wedge AfU^{>}_{w} g))}{\Gamma \ \Rightarrow \ \Delta, AfU^{>}_{w} g}(\ \Rightarrow AU^{>}_{w})$$

$$\frac{AX(g \vee (f \wedge AfU^{>}_{w} g)), \Gamma \ \Rightarrow \ \Delta}{AfU^{>}_{w} g, \Gamma \ \Rightarrow \ \Delta}(AU^{>}_{w} \ \Rightarrow\ )$$

$$\frac{\Gamma \ \Rightarrow \ \Delta, h \quad h \ \Rightarrow \ AX(g \vee (f \wedge h))}{\Gamma \ \Rightarrow \ \Delta, AfU^{>}_{w} g}(AU^{>}_{w} Ind)$$

$$\frac{\Gamma \ \Rightarrow \ \Delta, EX(g \vee (f \wedge (AX\bot \vee EfU^{>}_{w} g))) \ \Rightarrow \ \Delta}{\Gamma \ \Rightarrow \ \Delta, EfU^{>}_{w} g}(\ \Rightarrow EU^{>}_{w})$$

$$\frac{EX(g \vee (f \wedge (AX\bot \vee EfU^{>}_{w} g))), \Gamma \ \Rightarrow \ \Delta}{EfU^{>}_{w} g, \Gamma \ \Rightarrow \ \Delta}(EU^{>}_{w} \ \Rightarrow\ )$$

$$\frac{\Gamma \ \Rightarrow \ \Delta, h \quad h \ \Rightarrow \ EX(g \vee (f \wedge (AX\bot \vee h)))}{\Gamma \ \Rightarrow \ \Delta, EfU^{>}_{w} g}(EU^{>}_{w} Ind)$$

O autor prova então que o sistema é correto e completo, e satisfaz uma forma fraca do teorema do corte: *para toda prova existe uma prova equivalente*

PUC-Rio - Certificação Digital Nº 0016017/CA

que não usa a regra do corte. A prova apresentada é semântica, e o sistema não satisfaz a propriedade da sub-fórmula. Um outro problema que pode ser visto neste sistema é a "impureza"das regras de derivação, na medida em que várias delas mexem com vários conectivos ao mesmo tempo, ou inserem um conectivo dos dois lados do seqüênte ao mesmo tempo. Quanto à limitação da eliminação da regra do corte, o autor a atribui às regras indutivas ($(AU^{\geq}_{w}Ind)$ e $(EU^{\geq}_{w}Ind)$) pois introduzem novas fórmulas h na derivação.

5.8.2 Considerações sobre o sistema $\mathcal{CN}$

A questão da normalização fica então em aberto, embora um fragmento de $\mathcal{CN}$ seja normalizável. Para fechar essa questão algumas tentativas sem sucesso foram feitas. Na tentativa de provar que $\mathcal{CN}$ não é normalizável, tentou-se mostrar que $\mathcal{CN}$ pode ser visto como uma extensão de P, (First Order Peano arithmetic, [Prawitz1971]), pois P, que contém uma regra de indução, não é normalizável. Para isso considerou-se um frame onde a relação R é linear. Variáveis seriam representadas por labels iniciais. Por exemplo, A^i poderia ser visto como $A(x)$. Infelizmente não se conseguiu traduzir a presença de váriaveis distintas numa mesma fórmula (e P sem váriaveis é normalizável).Tentou-se então fazer o contrário: traduzir $\mathcal{CN}$ para P sem variáveis. Mas isso também não foi possível.

Pensando em termos de prova automática, resolver o problema da normalização seria um primeiro passo. Se isso não puder ser feito, um provador auxiliado pelo homem seria de grande ajuda. Talvez formar um conjunto de fórmulas A tais que $A^l \vdash \neg[\forall X]\neg A^l$, e permitir então que $G =$ fosse usada para inferir $[\exists G]B^l$ a partir de B^l sempre que a prova de B^l tivesse como única hipótese uma fórmula do conjunto formado. Uma interação homem-máquina seria útil para a formação desse conjunto. Mas isso necessitaria uma implementação e uma validação empírica, o que foge do escopo deste trabalho.

PUC-Rio - Certificação Digital Nº 0016017/CA