Agradecimentos

À Professora Doutora Cristina Sernadas pela sua constante disponibilidade, pelo apoio científico e por todo o estímulo ao longo da elaboração desta dissertação. Ao Professor Doutor Amílcar Sernadas pelo constante incentivo, pelo apoio e por todas as condições de trabalho que me foram proporcionadas no âmbito da secção 84. Ao Jaime e ao Carlos sempre disponíveis para troca de impressões. A todos os colegas da secção 84 por todo o apoio e, sobretudo, pela amizade. À Antónia pelo ânimo nos momentos difíceis e pela amizade de sempre. Ao Artur pela muita paciência e compreensão.

À JNICT e aos projectos PRAXIS 2/2.1/MAT/262/94 SitCalc, PCEX/P/MAT/46/96 ACL e 2/2.1/TIT/1658/95 LogComp, bem como aos projectos ESPRIT II BRA WG 6071 IS-CORE e ESPRIT IV Working Groups 22704 ASPIRE e 23531 FIREworks pelo apoio.

Índice

Capítulo 1

Introdução

1.1 Contexto

O trabalho desenvolvido na presente dissertação insere-se na área da verificação de especificações formais de sistemas e, mais concretamente, na área da verificação de especificações temporais de comunidades de objectos. Pretende contribuir para a exploração de uma nova direcção neste âmbito dado que o objectivo é ir além da tarefa tradicional de verificação, isto é, do raciocínio sobre uma dada especificação para assegurar que certas propriedades são verificadas. O que se pretende é sugerir formas de enriquecer a especificação dada, no caso de uma certa propriedade não ser verificada, de modo a que a nova especificação já satisfaça a propriedade em questão. Este tipo de problema pode ser visto como um problema de abdução e a sua resolução pode ser conseguida recorrendo a técnicas de raciocínio abdutivo.

Nesta secção faz-se uma breve descrição de diversos aspectos relevantes para enquadrar o trabalho desenvolvido nesta dissertação. Os aspectos relacionados com o raciocínio abdutivo são mais detalhados por este tópico ser menos conhecido na área em que se desenvolve este trabalho.

1.1.1 Especificação

O paradigma do desenvolvimento de sistemas centrado em objectos tem os seus antecedentes na linguagem de programação SIMULA [11] e tornou-se mais popular com o aparecimento da linguagem SMALLTALK [23]. O seu sucesso está relacionado, nomeadamente, com as vantagens que apresenta ao nível do desenvolvimento e manutenção de aplicações através da utilização intensiva da encapsulação da informação e da possibilidade de reutilização.

A noção de objecto não é, ainda hoje, um assunto completamente pacífico mas existe algum consenso relativamente a algumas das suas principais características [65]. Em [59, 57], os autores defendem que um objecto pode ser visto como uma entidade sequencial que possui um estado encapsulado (definido pelos valores dos seus atributos), cuja evolução se processa através da execução das suas acções. Uma comunidade de objectos consiste num conjunto de objectos concorrentes que comunicam entre si.

A abordagem formal à especificação de sistemas tem vindo a ser fortemente defendida por vários autores. Apresenta importantes vantagens, nomeadamente, as relacionadas com a definição de uma semântica rigorosa e com a verificação correcta dos sistemas especificados. Esta abordagem pressupõe a definição de uma linguagem formal e, para efeitos de verificação, o desenvolvimento de um sistema dedutivo. Em [50] defende-se, em particular, a utilização da lógica temporal para a especificação de sistemas concorrentes e, desde aí, muito trabalho tem vindo a ser desenvolvido tendo por objectivo a utilização da lógica temporal na especificação de sistemas concorrentes e reactivos.

Vários trabalhos, de entre os quais se podem citar como exemplo [58, 20, 18, 60, 61], têm sido elaborados no sentido de desenvolver e utilizar lógicas temporais adequadas para especificação de objectos/comunidades de objectos. No contexto dos trabalhos referidos, a especificação de um objecto inclui uma assinatura e um conjunto de fórmulas da linguagem associada ao objecto. Na assinatura são indicados os identificadores dos atributos e das acções do objecto. As fórmulas da linguagem associada ao objecto são fórmulas de uma certa lógica temporal. O comportamento do objecto é especificado através das fórmulas incluídas na sua especificação. Tipicamente, estas fórmulas expressam restrições à ocorrência das acções e estabelecem os efeitos que a ocorrência das acções tem sobre os valores dos atributos. Os objectos podem interagir entre si. Em certos trabalhos, como por exemplo [20, 18], a especificação destas interacções tem por base conceitos categoriais como morfismos e colimites. Em [60, 61] propõe-se o recurso a um certo tipo de fórmulas temporais para este fim.

1.1.2 Verificação

Uma da vantagens de se usar uma abordagem à especificação de objectos baseada numa dada lógica é a possibilidade de raciocinar sobre uma dada especificação. A tarefa de verificação está associada à noção de derivação no âmbito de um sistema dedutivo apropriado. Verificar que o comportamento do objecto determinado por uma especificação possui uma certa propriedade consiste em encontrar uma derivação da fórmula que expressa essa propriedade, a partir do conjunto das fórmulas da especificação do objecto, no contexto do cálculo adoptado.

Muito trabalho tem vindo a ser desenvolvido nesta área no âmbito da abordagem à especificação de objectos baseada na lógica temporal. Como exemplo podem citar-se [58, 19, 20, 18, 60, 61]. Na generalidade dos casos adoptam-se para o cálculo sistemas dedutivos de tipo Hilbert. Existe também algum trabalho no sentido de adoptar diferentes tipos de tableaux [37, 24, 25, 28].

Determinadas propriedades do comportamento de sistemas reactivos são particularmente relevantes. Estas propriedades são usualmente agrupadas em várias classes representando cada classe um certo tipo de requisito sobre o comportamento do sistema.

Como refere [42], a classificação de tais propriedades em propriedades de segurança (*safety*) e de animação (*liveness*) foi sugerida pela primeira vez em [34] e tem vindo a ser utilizada por vários autores em diversas situações. A caracterização destas classes pode ser dada de um modo informal dizendo que uma propriedade de segurança afirma que *nada de mau acontece* e que uma propriedade de animação afirma que *algo de bom acontecerá*. A caracterização semântica das propriedades de segurança foi apresentada em [35] e a das propriedades de animação em [2]. As referidas classes de propriedades são disjuntas (com excepção das propriedades universais que pertencem a ambas). Em [63] foram apresentadas caracterizações sintácticas, em termos de fórmulas da lógica temporal proposicional com operadores de futuro, para a classe das propriedades de segurança e para algumas subclasses de propriedades de animação. Em [38] são já considerados operadores temporais de passado.

Existe também na literatura, em [41, 42] por exemplo, uma outra classificação no âmbito da qual as propriedades são apresentadas segundo uma certa hierarquia. Esta hierarquia é constituída por propriedades de segurança e propriedades de progresso sendo que nestas últimas se distinguem ainda as propriedades de garantia, obrigação, resposta, persistência e reactividade. Existe uma caracterização sintáctica para as diferentes propriedades indicadas em termos de fórmulas da lógica temporal com operadores de futuro e passado. A cada classe está associado um conjunto de fórmulas temporais canónicas. Sendo $f, f_1, f_1' \ldots, f_n, f_n'$ fórmulas temporais que não incluem operadores temporais de futuro tem-se que: $\mathbf{G}\, f$ é fórmula canónica de segurança, $\mathbf{F}\, f$ é fórmula canónica de garantia, $\bigwedge_{1 \leq i \leq n}((\mathbf{G}\, f_i) \vee (\mathbf{F}\, f_i'))$ é fórmula canónica de obrigação, $\mathbf{G}(\mathbf{F}\, f)$ é fórmula canónica de resposta, $\mathbf{F}(\mathbf{G}\, f)$ é fórmula canónica de persistência e, por último, $\bigwedge_{1 \leq i \leq n}(\mathbf{G}(\mathbf{F}\, f_i)) \vee (\mathbf{F}(\mathbf{G}\, f_i'))$ é fórmula canónica de reactividade.

Nesta hierarquia as classes não são disjuntas. As classes das propriedades de segurança e garantia estão estritamente contidas na classe das propriedades de obrigação. Por sua vez, esta classe está estritamente contida quer na classe das propriedades de resposta quer na classe das propriedades de persistência. A classe das propriedades de reactividade contém todas as outras.

No que diz respeito às propriedades de segurança, as duas classificações mencionadas, segurança-animação e segurança-progresso, coincidem. Mas o mesmo não se passa com as de animação e progresso pois existem propriedades de progresso que não são fórmulas de animação [42].

A cada classe de propriedades está usualmente associado um método particular de verificação. Existem regras que permitem tornar mais expedita a verificação de propriedades. Estas regras permitem que a validade da fórmula que caracteriza a propriedade possa ser inferida a partir da validade de um certo número (finito) de fórmulas cuja validade é mais simples de estabelecer. Em [41], por exemplo, são apresentadas várias regras relativas a propriedades de segurança e de resposta e também a propriedades de reactividade em geral. Em particular, o livro [43] é dedicado inteiramente à verificação de propriedades de segurança.

Estas técnicas têm vindo a ser adaptadas para o caso particular da especificação de objectos/comunidades de objectos baseada na lógica temporal [53, 61]. São adoptados sistemas dedutivos de tipo Hilbert tratando-se em [61] exclusivamente os aspectos relacionados com provas de invariantes. Em [53] faz-se também referência a propriedades de resposta.

1.1.3 Raciocínio abdutivo

Raciocínio abdutivo, inferência abdutiva ou abdução são três termos diferentes usados na literatura para designar a geração de possíveis explicações que justifiquem uma dada observação no âmbito de um certo domínio. As observações que necessitam de explicação podem ser vistas como factos ou propriedades do domínio que não são explicáveis a partir do conhecimento do domínio de que se dispõe.

A inferência abdutiva é uma forma de inferência que, como é referido em [44], é já mencionada por Aristóteles. É porém atribuída ao filósofo Peirce a introdução do termo *abdução* para designar o tipo de inferência com o seguinte padrão:

$$\frac{B, \quad A \to B}{A}$$

isto é, é permitido *inferir abdutivamente* A partindo da observação de B e da aceitação de que sempre que se tem A então também se tem B [49]. Peirce distingue a inferência abdutiva da inferência dedutiva a qual segue, no contexto da lógica clássica, o conhecido padrão

$$\frac{A, \quad A \to B}{B}$$

Várias abordagens ao raciocínio abdutivo têm vindo a ser utilizadas. Nestas abordagens é distinta a forma como se representa o conhecimento sobre o domínio em questão e tais diferenças vão também condicionar a representação das observações e explicações bem como as técnicas para geração destas últimas.

Como é natural, frequentemente, as explicações não são únicas. Põe-se então o problema de saber se é possível encontrar a "melhor" explicação ou o conjunto das "melhores" explicações. Mas não existe uma única noção de "melhor" explicação e é largamente aceite a ideia de que esta noção depende fortemente não só da forma como o conhecimento sobre o domínio em causa está representado como também do domínio *per se*.

Existem fundamentalmente três abordagens ao raciocínio abdutivo: a abordagem lógica, a abordagem baseada na cobertura de conjuntos e a abordagem *knowledge level*. A primeira abordagem é sem dúvida a que tem vindo a merecer maior atenção e é aquela que se utiliza no trabalho desenvolvido nesta dissertação. Por este motivo far-se-á uma referência um pouco mais detalhada da abordagem lógica e métodos de geração e selecção de explicações a ela associados e apenas uma brevíssima referência às segunda e terceira abordagens. Uma panorâmica sobre raciocínio abdutivo pode ser encontrada em [48].

Aplicações

O raciocínio abdutivo tem vindo a ser utilizado em diversas áreas com grande ênfase na área da inteligência artificial.

Um caso clássico é a aplicação a problemas de diagnóstico. A tarefa consiste em detectar quais as causas que poderão explicar os efeitos observados num certo sistema do qual se tem uma determinada descrição. Como exemplos de trabalhos nesta área podem ser citados [52, 54, 10, 7]. Nos casos de apoio a problemas de diagnóstico médico, por exemplo, a partir da observação de certos sintomas, e utilizando conhecimento prévio sobre relações causais entre doenças e sintomas, são produzidas hipóteses sobre a presença de uma ou mais doenças. Um outro exemplo é o caso de teste de circuitos no qual sempre que se observe um comportamento anormal do circuito se pretende determinar, a partir de uma descrição do modo como funciona, diagnósticos do tipo "a componente x está defeituosa".

Um outro caso é a aplicação a problemas de planeamento. Exemplos de trabalhos neste contexto são [14, 62]. O objectivo é encontrar um plano para executar uma determinada tarefa, isto é, encontrar um certo número de acções que executadas por determinada ordem permitam, a partir de um dado estado inicial, chegar a um certo estado final. Este plano pode ser visto como uma explicação para a observação do estado final tendo em conta uma descrição do estado inicial e do conjunto das acções que se podem executar bem assim como de uma descrição dos efeitos da execução de cada acção. A explicação pretendida incluirá neste caso um conjunto de acções e, eventualmente, uma ordenação das suas ocorrências.

Ainda outro domínio é o da assimilação de conhecimento sendo [31] um exemplo de trabalho neste contexto. Neste caso, a questão está relacionada com o problema de como modificar uma base de conhecimento quando se dispõe de nova informação que não pertence a essa base. Se não é possível (ou desejável) adicionar explicitamente tal informação, a abdução pode ser utilizada para encontrar um certo conjunto de hipóteses que juntamente com o estado presente da base de conhecimento expliquem a nova informação. Ao incluir explicitamente tais hipóteses na base de conhecimento, a nova informação é assimilada implicitamente.

A interpretação de linguagem natural é mais um caso de aplicação do raciocínio abdutivo [64].

Um outro exemplo de aplicação do raciocínio abdutivo é referido em [56] no âmbito da inversão de programas imperativos.

Este tipo de inferência é também utilizado no contexto do raciocínio por omissão. Em [51] é proposta uma alternativa à lógica de omissões de Reiter [55] através de uma formulação em termos de inferência abdutiva.

O raciocínio abdutivo e a programaçao em lógica têm estreitas ligações. Um exemplo é a interpretação para a negação por falha em termos abdutivos apresentada em [16]. Em [30] é apresentada uma panorâmica sobre raciocínio abdutivo e suas ligações à programação em lógica.

Abordagem lógica

A abordagem lógica ao raciocínio abdutivo é uma das mais activas áreas de investigação neste domínio. Grande parte dos trabalhos existentes, de entre os quais se podem citar [52, 9, 10, 14, 51, 16, 62, 7, 29, 8, 33, 45], desenvolvem-se no âmbito da lógica proposicional ou de primeira ordem mas recentemente também o raciocínio abdutivo no âmbito da lógica modal tem vindo a merecer atenção [46, 47].

Este tipo de abordagem não aparece tratado na literatura de um modo uniforme mas, genericamente, pode ser descrita como se segue. O conhecimento que se tem sobre o domínio em causa é representado por uma certa apresentação de teoria proposicional ou de primeira ordem $T = (\Sigma, F)$ a qual é usualmente designada por teoria domínio. A observação para a qual se pretende encontrar uma explicação é representada por uma fórmula φ. Cada explicação é um conjunto de fórmulas escolhidas de entre um conjunto H de fórmulas ditas fórmulas abdutíveis ou hipóteses. Fixando T e H, o conjunto E é uma explicação para uma certa observação φ sempre que (i) $E \subset H$, (ii) $F \cup E$ é coerente e (iii) $F \cup E \models \varphi$, onde $\models$ é o operador de consequência semântica. Em certos trabalhos utiliza-se em vez da consequência semântica o operador de derivação $\vdash$.

Relativamente às fórmulas que fazem parte da apresentação de teoria são também impostos alguns requisitos como, por exemplo, serem cláusulas de Horn proposicionais [15] ou terem de constituir um programa lógico hierárquico [8]. Sobre as observações φ recaem também restrições como por exemplo: têm de ser conjunções de átomos ou literais por vezes com exigência de serem distintos dos que ocorrem nas fórmulas abdutíveis [8]; têm de ser fórmulas fechadas [29]; têm de ser conjunções de átomos quantificadas existencialmente [16]. Sobre as fórmulas abdutíveis podem citar-se os seguintes requisitos: têm de ser átomos que não envolvam variáveis [16]; têm de ser literais [64]; têm de ser fórmulas na forma normal prenex cuja matriz é uma conjunção de literais [9, 45].

Geração de explicações

Um problema fulcral é, obviamente, o da geração de explicações que verifiquem as requisitos mencionados.

Os métodos que mais frequentemente se encontram são os que se baseiam em alguma forma de resolução, como por exemplo resolução linear e SLD. A ideia subjacente a estes métodos reside facto de que $F \cup \{\psi\} \models \varphi$ sse $F \cup \{\neg\varphi\} \models \neg\psi$. Como exemplo pode ser referido o método apresentado em [10]. Neste caso, aplica-se a resolução linear a F e $\neg\varphi$ que naturalmente se assumem na forma clausal. Para obter uma explicação: (i) considera-se o conjunto D das cláusulas que são folhas de derivações falhadas; (ii) aplica-se o algoritmo de Skolemização inversa a $\bigwedge_{d \in D} \neg d$. A fórmula assim obtida constitui uma explicação.

Também os métodos que usam tableaux para a geração de explicações se baseiam num princípio idêntico [45, 46, 47]. As explicações são obtidas através de literais que fecham os ramos abertos de um tableaux para $F \cup \{\neg\varphi\}$ [45]. Neste caso não é necessário proceder a nennhuma transformação prévia de φ ou das fórmulas em F.

Um outro método, apresentado em [8], caracteriza a fórmula explicação ψ como consequência da observação φ e da completação F_c de F (seguindo [6]) restringida aos predicados não abdutíveis. A fórmula explicação ψ é a fórmula mais específica na linguagem dos símbolos abdutíveis tal que $F_c \cup \{\varphi\} \models \psi$ (ψ é mais específica que ψ' sse $\models \psi \Rightarrow \psi'$). Esta fórmula caracteriza todas as soluções do problema abdutivo no sentido em que contém o máximo de informação que pode ser obtido da observação. A fórmula ψ (única a menos de uma equivalência) é encontrada por reescrita e simplificação de φ usando as fórmulas da completação F_c até ser obtida uma fórmula que contenha só predicados abdutíveis.

Em [44] mostra-se como é possível utilizar métodos conhecidos de geração de implicantes e implicados primários de uma fórmula para encontar explicações.

Relativamente à coerência das explicações com a teoria dada, seria desejável que os métodos utilizados para gerar explicações gerassem apenas fórmulas/conjuntos de fórmulas que verificassem a coerência desejada. No entanto, esta condição não é verificada no caso geral. Assim, usualmente, o teste à coerência é feito após a geração das potenciais explicações para eliminar as que não verificam o requisito da coerência o qual, como é natural, está condicionado à decidibilidade da lógica subjacente. Em certos casos particulares, como por exemplo no caso proposicional, existem métodos de geração de explicações que apenas constroem fórmulas/conjuntos de fórmulas que verificam o requisito da coerência [44, 45].

Selecção de explicações

Em geral, o número de explicações para um dado problema de abdução é elevado. Segundo Peirce, explicações a serem seleccionadas como "melhores" deverão ser as mais "simples" ou mais "intuitivas". Normalmente, esta noção é concretizada através de critérios de simplicidade sintáctica ou lógica. No entanto, os critérios de selecção não são uniformes no sentido em que se utilizem todos nas mesmas situações. Existem aplicações para as quais certos critérios são mais adequados que outros.

Um dos critérios mais simples é o que se baseia na comparação da cardinalidade das explicações. No entanto, este tipo de critério não é adoptado extensivamente. Como exemplo refira-se o caso de diagnóstico de sistemas em que se pretendem justificações que impliquem a falha de um número de componentes tão pequeno quanto possível.

Em [9] são introduzidos os critérios que seguidamente se descrevem os quais são também utilizados em diversos outros trabalhos. Uma explicação E para φ é: (i) não-trivial quando não se tem $\bigwedge_{\psi\in E}\psi \Rightarrow \varphi$; (ii) básica quando qualquer explicação de $\bigwedge_{\psi\in E}\psi$ tem de ser trivial; (iii) minimal quando sempre que E' é também explicação de φ e $\bigwedge_{\psi\in E}\psi \Rightarrow \bigwedge_{\psi\in E'}\psi$ então $\bigwedge_{\psi\in E'}\psi \Rightarrow \bigwedge_{\psi\in E}\psi$.

Noutros casos são atribuídos custos quer às fórmulas da teoria domínio quer às fórmulas abdutíveis [64]. A partir destes custos é calculado o custo de cada explicação. No trabalho referido prefere-se entre duas explicações aquela a que está associado menor custo.

Outras abordagens

No âmbito da abordagem baseada na cobertura de conjuntos, e seguindo [54], é assumida a existência de: (i) um conjunto Γ cujos elementos representam causas, (ii) um conjunto Φ cujos elementos representam efeitos; (iii) uma relação $R \subset \Gamma \times \Phi$ que representa a noção de causalidade entre causas e efeitos no sentido em que se $(x, y) \in R$ tal significa que x pode causar y. Dado um conjunto de efeitos observados $\varphi \subset \Phi$ pretende-se encontar uma explicação para φ, ou seja, um conjunto de causas $\gamma \subset \Gamma$ que melhor justifiquem os efeitos em φ. O objectivo é encontrar $\gamma \subset \Gamma$ tal que (i) $\varphi \subset \{y \in \Phi : (x, y) \in R, x \in \gamma\}$ (caso em que se diz que γ é uma cobertura de φ) e (ii) γ é parcimonioso. Esta noção de parcimónia reflecte a noção intuitiva de que a explicação mais sóbria é a melhor. Em certas aplicações está associada ao conceito de cardinal mínimo e em outras à minimalidade relativamente à inclusão.

Em [1] assume-se também a existência de um conjunto Γ cujos elementos representam causas, de um conjunto Φ cujos elementos representam efeitos mas agora tem-se uma função $e : 2^\Gamma \rightarrow 2^\Phi$ que estabelece uma relação entre conjuntos de causas e conjuntos de efeitos por elas determinados. Dado $\varphi \subset \Phi$, o objectivo é novamente calcular uma explicação de φ agora com base na função e. A noção de melhor explicação está neste caso associada à minimalidade relativamente à inclusão. Para que o cálculo de γ seja exequível, e tem de verificar várias condições (e.g. ser computável).

Este tipo de abordagem é essencialmente utilizada em domínios nos quais a relação entre causas e efeitos permite a definição de uma tal relação ou função (problemas de diagnóstico, por exemplo). É também desejável que tais relações não sofram mudanças frequentes já que mesmo ligeiras modificações podem levar a uma substancial redefinição do problema.

Na abordagem *knowledge-level* a abdução é caracterizada em termos de uma lógica (modal) de crenças [36]. Para geração de explicações pode ser utilizado o procedimento do ATMS (*Assumption-based Truth Maintenance System*) [12].

1.2 Objectivos e opções

O trabalho desenvolvido nesta dissertação tem como objectivo explorar o problema da verificação de especificações de temporais de objectos/comunidades de objectos sob uma nova perspectiva: uma perspectiva abdutiva. Os trabalhos que têm vindo a ser desenvolvidos sobre o problema da verificação no contexto das especificações referidas têm por objectivo o desenvolvimento de métodos que permitam obter provas de que o comportamento do objecto/comunidade de objectos prescrito por uma dada especificação satisfaz certas propriedades. A perspectiva abdutiva que aqui se pretende explorar está relacionada com a capacidade de sugerir modificações à especificação no caso da propriedade desejada não se verificar.

Tal como é tradicional no contexto da especificação baseada em objectos, explora-se primeiro o problema a um nível local e, depois, a um nível global. Assim, o primeiro objectivo é explorar o problema da verificação, sob este novo ponto de vista, no contexto de uma especificação de objecto, isto é, explorar esta questão a um nível local. Trabalhar ao nível local corresponde assegurar que o comportamento individual do objecto verifica certas propriedades expressáveis à custa de fórmulas da linguagem associada ao objecto. O segundo objectivo é explorar o mesmo problema mas agora no âmbito de uma especificação de comunidade de objectos, ou seja, de um conjunto de objectos que comunicam entre si. Neste contexto trabalha-se a um nível global pois o objectivo é assegurar que o comportamento conjunto de vários objectos, resultante do comportamento especificado individualmente para cada um e das interacções especificadas, verifica determinadas propriedades.

A abordagem à especificação adoptada é baseada na lógica temporal linear e capitaliza no trabalho desenvolvido em [60, 61]. Trabalha-se ao nível proposicional e escolhe-se a versão ancorada da lógica temporal.

Uma especificação de objecto inclui uma assinatura, um conjunto de axiomas (fórmulas) e um conjunto de axiomas-esquema (fórmulas-esquema). A assinatura introduz os símbolos de acção (ou acções) e os símbolos de atributo (ou atributos). Assume-se que o conjunto de axiomas só contém os seguintes tipos de fórmulas: constrangimentos de estado, restrições de activação sobre acções e requisitos de justiça sobre a ocorrência das acções. Os constrangimentos de estado (fórmulas que só envolvem atributos) expressam condições iniciais. Pelo facto de se pretender especificar requisitos de justiça sobre a ocorrência de acções, motivado pelo desejo de considerar certo tipo de propriedades (propriedades de resposta, por exemplo), tornou-se necessário distinguir a noção de ocorrência de uma acção da noção de activação de uma acção. Uma acção activada num certo instante é uma acção cuja ocorrência é permitida nesse instante mas que não ocorre necessariamente nesse instante. As restrições de activação podem expressar quer condições necessárias quer condições suficientes à activação das acções. Estas condições são expressas em termos dos valores dos atributos. O requisito de justiça sobre uma acção impõe que essa acção ocorra recorrentemente se estiver activada recorrentemente. Os axiomas-esquema exprimem as modificações que a ocorrência das acções têm sobre o valor dos atributos. A utilização deste tipo de fórmulas, inspirada em [61], permite representar sucintamente o facto de os atributos cuja modificação não é explicitamente indicada não sofrerem qualquer alteração. Assume-se que existe um axioma-esquema para cada acção.

As estruturas de interpretação são sucessões de conjuntos de fórmulas (atómicas) determinando quais as acções que ocorrem e quais as que estão activadas em cada instante bem como o valor dos atributos. A estas sucessões são impostos certos requisitos: uma acção só ocorre se estiver activada e, em cada instante, só ocorre uma acção (cada objecto é uma entidade sequencial).

A especificação de comunidades de objectos tem por base o trabalho desenvolvido em [60, 61] (no qual se consideram classes de objectos) e que é aqui adaptado/simplificado para o caso em que não existe a noção de classe de objecto. A especificação de comunidade inclui, para cada objecto, uma assinatura (que, para além dos símbolos de acção e de atributo, inclui o identificador do objecto), um conjunto de axiomas e um conjunto de axiomas-esquema à semelhança do que acontece no caso local. Assume-se que a interacção entre objectos é feita através da ocorrência das respectivas acções: sob certas condições a ocorrência de uma acção de um certo objecto induz a ocorrência (simultânea) de uma acção de um outro objecto. Tal como em [60, 61], a noção de objecto composto (cuja assinatura é obtida a partir das assinaturas dos objectos envolvidos na interacção) é introduzida para permitir a especificação da comunicação entre objectos através de certas fórmulas, ditas fórmulas de interacção. Assume-se que os axiomas destes objectos compostos são exclusivamente fórmulas de interacção.

As diferentes propriedades que são consideradas estão relacionadas com a evolução do valor dos atributos e são propriedades usualmente consideradas no contexto da especificação do comportamento de sistemas reactivos. Seguindo as designações apresentadas em [41, 42] são classificadas em propriedades de segurança, propriedades de resposta, propriedades de garantia e propriedades de persistência.

1.3 Contribuições

No contexto de uma especificação de objecto, o problema da verificação sob o ponto de vista abdutivo é enquadrado na abordagem lógica ao raciocínio abdutivo da forma que seguidamente se descreve. A especificação de objecto desempenha o papel da (apresentação de) teoria T. As fórmulas que expressam as propriedades cuja verificação se quer assegurar são as observações. Os constrangimentos de estado, as restrições de activação e os requisitos de justiça constituem o conjunto de fórmulas abdutíveis H. Assim, um problema de abdução numa especificação de objecto é um requisito sobre o comportamento do objecto que não é satisfeito pelo comportamento prescrito pela especificação. Uma explicação para um problema de abdução é um conjunto de novos axiomas com o qual se enriquece a especificação de modo a que o comportamento prescrito pela nova especificação já verifique o requisito desejado e que esta seja coerente. Este novos axiomas exprimem novas restrições à evolução do objecto.

Nesta dissertação são propostas técnicas para a construção de explicações para problemas de abdução que envolvem propriedades de segurança, propriedades de resposta, propriedades de garantia e propriedades de persistência.

O problema da geração de explicações é resolvido tendo como base, por um lado, as técnicas propostas na literatura para a verificação de propriedades de segurança [43] e de propriedades de resposta [41] e animação [39] de sistemas reactivos concorrentes e, por outro, as técnicas abdutivas baseadas em tableaux que são apresentadas em [45] para raciocínio abdutivo em lógica proposicional. As referidas técnicas de verificação são regras que permitem concluir que as propriedades são verificadas sempre que se verificarem um certo número de propriedades mais simples (as premissas da regra). As regras de verificação referidas são aqui adaptadas para o raciocínio sobre as especificações adoptadas.

No caso de propriedades de segurança, as premissas estão relacionadas com a verificação de certas condições iniciais e com a verificação de que, após a ocorrência de cada acção, um certo constrangimento de estado é satisfeito sempre que um outro constrangimento de estado seja satisfeito quando a acção ocorre. Sempre que alguma das premissas não é verificada pela especificação, é construído um tableau para determinado conjunto de fórmulas proposicionais obtido a partir do problema em causa e dos axiomas e axiomas-esquema da especificação. A partir da análise desse tableau são construídas várias fórmulas (constrangimentos de estado ou restrições de activação, conforme o tipo de premissa) que vão assegurar a verificação da premissa em causa.

No caso das regras relativas a propriedades de resposta, garantia e persistência existem ainda outros dois tipos de premissas: restrições de activação que representam condições suficientes para a activação das acções e requisitos de justiça. Neste caso não é construído qualquer tableau e as premissas são incluídas directamente nas potenciais explicações sempre que não sejam verificadas.

Para que um conjunto de fórmulas obtido do modo descrito possa ser considerado uma explicação, há que verificar ainda que, ao enriquecer com ele a especificação dada, se obtém uma especificação coerente. Refere-se como se pode utilizar sistemas de tableaux temporais para testar a coerência de tais especificações.

É analisada a questão da selecção de explicações pois, como é habitual quando se geram explicações para problemas de abdução, as técnicas de construção conduzem geralmente a diferentes explicações. São apontados alguns critérios de selecção de explicações e, em certos casos, são indicados métodos para impedir a geração de explicações que se consideram menos boas. Um dos principais factores tidos em conta está relacionado com a preocupação em gerar explicações que não introduzam mais restrições à ocorrência das acções do que as que são necessárias para resolver o problema de abdução em causa.

O enquadramento do problema da verificação de especificações de comunidades de objectos na abordagem lógica ao raciocínio abdutivo é semelhante ao proposto para o nível local. As observações são agora requisitos sobre o comportamento conjunto de vários objectos e, por isso, expressas em termos de fórmulas da linguagem associada a objectos compostos. Por seu lado, as explicações podem neste caso incluir também a possibilidade de novas interacções entre os objectos da comunidade.

São apresentadas técnicas para a construção de explicações para problemas de abdução que envolvem propriedades de segurança, propriedades de resposta, propriedades de garantia e propriedades de persistência. As técnicas propostas para geração de explicações baseiam-se novamente nas técnicas de verificação de propriedades de segurança e de propriedades de resposta e animação de sistemas reactivos concorrentes e em técnicas abdutivas baseadas em tableaux semelhantes às utilizadas para o caso local.

São também apresentados critérios de preferência entre as explicações geradas pelas técnicas descritas.

O trabalho contido nesta dissertação é um desenvolvimento de trabalho preliminar já apresentado em [26, 27].

1.4 Estrutura da dissertação

A presente dissertação encontra-se organizada em 5 capítulos.

No Capítulo 2 apresentam-se as noções sintácticas e semânticas relacionadas com a especificação de objectos e faz-se referência à questão da verificação de especificações de objectos. No âmbito da verificação, é dada ênfase à utilização de tableaux temporais e proposicionais. Os tableaux proposicionais são descritos com algum detalhe e é provado um resultado àcerca deste tipo de tableaux que não é usualmente referido na literatura mas que é importante para a utilização destes no âmbito do raciocínio abdutivo.

No Capítulo 3 trata-se o problema da verificação de uma especificação de objecto de um ponto de vista abdutivo. Definem-se as noções de observação sobre uma especificação de objecto, de problema de abdução numa especificação de objecto e de explicação para um problema de abdução. São seguidamente descritas as técnicas que permitem encontrar explicações para os referidos problemas de abdução. São apontados vários critérios de preferência entre as várias explicações que as referidas técnicas permitem construir.

No Capítulo 4 trata-se o problema da verificação no âmbito de uma especificação de comunidade de objectos de um ponto de vista abdutivo. Apresentam-se as noções sintácticas e semânticas relativas à especificação de comunidades de objectos. Seguidamente, definem-se as noções de observação, de problema de abdução e de explicação no âmbito de uma especificação de comunidade de objectos. Por último, são descritas técnicas que permitem encontrar explicações para problemas de abdução neste contexto e critérios de preferência entre as explicações construídas.

No Capítulo 5 apresentam-se as conclusões e descrevem-se as perspectivas de trabalho futuro.

Capítulo 2

Especificação e verificação de objectos

2.1 Introdução

Neste capítulo descrevem-se as noções sintácticas e semânticas ligadas à noção de especificação de objecto adoptada nesta dissertação e faz-se referência à questão da verificação neste âmbito, isto é, ao problema de provar que uma certa especificação verifica uma dada propriedade.

A abordagem à especificação adoptada nesta dissertação tem por base o trabalho apresentado em [60, 61] o qual se desenvolve no âmbito da lógica temporal linear. São feitas, no entanto, algumas adaptações/simplificações dado que não se consideram classes de objectos (apenas objectos), trabalha-se no fragmento proposicional e adopta-se a versão ancorada da lógica temporal.

Uma especificação de objecto é constituída por uma assinatura (na qual se introduzem os símbolos de acção e os símbolos de atributo), por um conjunto de fórmulas e por um conjunto de fórmulas-esquema. As estruturas de interpretação são sucessões de conjuntos de fórmulas atómicas verificando alguns requisitos.

Faz-se referência ao problema da verificação dando ênfase à utilização de tableaux.

Os sistemas de tableaux temporais existentes na literatura podem ser utilizados para testar se uma dada propriedade é ou não uma propriedade do comportamento especificado para o objecto. Neste capítulo descreve-se sucintamente a utilização de tableaux temporais no âmbito das especificações adoptadas.

Em certos casos é possível tratar o problema da verificação através da utilização de tableaux mais simples como, por exemplo, os tableaux proposicionais. A utilização destes tableaux capitaliza em regras descritas na literatura para verificação de certas classes de propriedades. No caso particular dos invariantes ilustra-se o modo como as provas se podem conduzir recorrendo exclusivamente aos tableaux proposicionais.

Os tableaux proposicionais vão desempenhar um papel importante nos capítulos que se seguem sendo por isso descritos com algum detalhe. Em particular, na subsecção 2.5.2.3 é provado um resultado técnico essencial no âmbito da utilização deste tipo de tableaux nas técnicas de raciocínio abdutivo propostas nesta dissertação e cuja prova é algo elaborada. Este resultado é mencionado, sem prova, em [45].

Este capítulo encontra-se organizado como seguidamente se descreve. Na secção 2.2 introduzem-se as noções de assinatura de objecto, de linguagem associada a uma assinatura de objecto e algumas noções e resultados auxiliares. Na secção 2.3 introduzem-se as noções de estrutura de interpretação sobre uma assinatura de objecto e de satisfação e validade de fórmulas. Na secção 2.4 introduz-se a noção de especificação de objecto e algumas noções auxiliares. Na secção 2.5 ilustra-se a utilização de dois tipos diferentes de tableaux no âmbito da questão da verificação de especificações de objectos. Na subsecção 2.5.1 ilustra-se a utilização de tableaux temporais. A subsecção 2.5.2 é dedicada aos tableaux proposicionais. Na subsubsecção 2.5.2.1 são apresentados os conceitos básicos relativos a tableaux proposicionais. Na subsubsecção 2.5.2.2 ilustra-se a sua utilização na prova de invariantes. Na subsubsecção 2.5.2.3 prova-se um resultado sobre tableaux proposicionais (a Proposição 2.54) relevante no contexto da utilização destes tableaux nas técnicas de raciocínio abdutivo apresentadas no Capítulo 3 e no Capítulo 4. Na secção 2.6 são apresentadas as conclusões.

2.2 Assinaturas

Nesta secção apresentam-se a noções de assinatura de objecto, de linguagem associada a uma assinatura de objecto bem como algumas definições e resultados auxiliares.

A assinatura de um objecto inclui os identificadores das acções e dos atributos do objecto.

Definição 2.1 Uma *assinatura de objecto* é um par (Acc, Atr) tal que

- Acc é um conjunto finito e não vazio cujos elementos são designados por *símbolos de acção* ou *acções*;
- Atr é um conjunto finito cujos elementos são designados por *símbolos de atributo* ou *atributos*;
- $Acc \cap Atr = \emptyset$. ■

As fórmulas da linguagem associada ao objecto são agora definidas à custa dos símbolos de acção e atributo, de conectivos lógicos e de operadores temporais.

Definição 2.2 Seja $\Sigma = (Acc, Atr)$ uma assinatura de objecto. O conjunto das *fórmulas* sobre Σ, F_Σ, define-se indutivamente do seguinte modo:

- $\{\mathbf{t}, \mathbf{f}\} \cup Atr \subset F_\Sigma$;
- $\triangledown Acc = \{\triangledown a : a \in Acc\} \subset F_\Sigma$ e $\diamond Acc = \{\diamond a : a \in Acc\} \subset F_\Sigma$;

- se $f, f' \in F_\Sigma$ então $(\neg f), (f \wedge f'), (\mathbf{X}\, f), (f'\, \mathbf{U}\, f) \in F_\Sigma$. ∎

Consideram-se primitivos os conectivos $\neg$, $\wedge$ e os operadores temporais $\mathbf{X}$ e $\mathbf{U}$. Os conectivos $\Rightarrow, \vee, \Leftrightarrow$ e os operadores temporais, $\mathbf{G}$, $\mathbf{F}$ e $\mathbf{W}$ definem-se como abreviaturas. O símbolo $\triangledown$ está relacionado com a noção de ocorrência de uma acção e o símbolo $\diamond$ com a noção de activação. A razão pela qual são considerados como distintos será justificada ulteriormente.

No resto da subsecção assume-se fixada a assinatura de objecto $\Sigma = (Acc, Atr)$.

Definição 2.3 Consideram-se as abreviaturas que se seguem. Sendo $f, f' \in F_\Sigma$:

- $(f \vee f') =_{abv} (\neg((\neg f) \wedge (\neg f')))$;
- $(f \Rightarrow f') =_{abv} ((\neg f) \vee f')$;
- $(f \Leftrightarrow f') =_{abv} ((f \Rightarrow f') \wedge (f' \Rightarrow f))$;
- $(\mathbf{F}\, f) =_{abv} (\mathbf{t}\, \mathbf{U}\, f)$;
- $(\mathbf{G}\, f) =_{abv} (\neg(\mathbf{F}(\neg f)))$;
- $(f'\, \mathbf{W}\, f) =_{abv} ((f'\, \mathbf{U}\, f) \vee (\mathbf{G}\, f'))$. ∎

Convenciona-se que se omitem os parênteses exteriores. Introduzem-se ainda as abreviaturas que se seguem.

Definição 2.4 Dada a sequência de fórmulas $f_1 \ldots f_m$ com $f_i \in F_\Sigma$ para cada $1 \leq i \leq m$ e $m \geq 1$:

- $f_1 \wedge \ldots \wedge f_m =_{abv} f_1$ se $m = 1$;
- $f_1 \vee \ldots \vee f_m =_{abv} f_1$ se $m = 1$;
- $f_1 \wedge \ldots \wedge f_m =_{abv} (\ldots(f_1 \wedge f_2) \wedge \ldots) \wedge f_m$ se $m > 1$;
- $f_1 \vee \ldots \vee f_m =_{abv} (\ldots(f_1 \vee f_2) \vee \ldots) \vee f_m$ se $m > 1$. ∎

Seguem-se algumas definições e lemas que serão necessários ao longo da dissertação.

Definição 2.5 O conjunto das *subfórmulas* de $f \in F_\Sigma$, $Sbf(f)$, é definido indutivamente da seguinte forma:

- se $f \in \triangledown Acc \cup \diamond Acc \cup Atr \cup \{\mathbf{t}, \mathbf{f}\}$ então $Sbf(f) = \{f\}$;
- se $f = \neg f'$ ou $f = \mathbf{X}\, f'$ então $Sbf(f) = Sbf(f') \cup \{f\}$;
- se $f = f' \wedge f''$ ou $f = f'\, \mathbf{U}\, f''$ então $Sbf(f) = Sbf(f') \cup Sbf(f'') \cup \{f\}$.

A fórmula $f' \in F_\Sigma$ é *subfórmula própria* de $f \in F_\Sigma$ sse $f' \in Sbf(f)$ e $f' \neq f$. Dado $A \subseteq F_\Sigma$, $Sbf(A) = \bigcup_{f \in A} Sbf(f)$. ∎

Definição 2.6 A *complexidade* de $f \in F_\Sigma$ designa-se por $c(f)$ e define-se indutivamente do seguinte modo:

- se $f \in \nabla Acc \cup \diamond Acc \cup Atr \cup \{\mathbf{t}, \mathbf{f}\}$ então $c(f) = 1$;
- se $f = \neg f'$ ou $f = \mathbf{X}\, f'$, então $c(f) = c(f') + 1$;
- se $f = f' \wedge f''$ ou $f = f'\ \mathbf{U}\ f''$ então $c(f) = c(f') + c(f'') + 1$. ∎

Definição 2.7 O conjunto dos *constrangimentos de estado* sobre Σ, CE_Σ, define-se indutivamente do seguinte modo:

- $Atr \subset CE_\Sigma$;
- se $f, f' \in CE_\Sigma$ então $\neg f, f \wedge f' \in CE_\Sigma$.

O conjunto $CE_\Sigma^{\mathbf{tf}}$ tem definição análoga à de CE_Σ mas neste caso o primeiro requisito é substituído por $Atr \cup \{\mathbf{t}, \mathbf{f}\} \subset CE_\Sigma^{\mathbf{tf}}$. ∎

Definição 2.8 A fórmula $f \in F_\Sigma$ diz-se um *literal* sse $f \in Atr \cup \diamond Acc \cup \nabla Atr$ (caso em que se diz *literal positivo*) ou $f = \neg f'$ com $f' \in Atr \cup \diamond Acc \cup \nabla Atr$ (caso em que se diz *literal negativo*). Designa-se por L_Σ o conjunto dos literais em F_Σ, por L_Σ^+ o conjunto literais positivos em L_Σ, por L_Σ^- o conjunto dos literais negativos em L_Σ e por $L_\Sigma^{\mathbf{tf}}$ o conjunto $L_\Sigma \cup \{\mathbf{t}, \mathbf{f}, \neg\mathbf{t}, \neg\mathbf{f}\}$.

Sendo $f \in L_\Sigma$, o *conjugado* de f denota-se por $\overline{f}$ e é tal que se $f \in L_\Sigma^+$ então $\overline{f} = \neg f$ e, caso contrário, se $f = \neg f' \in L_\Sigma^-$ então $\overline{f} = f'$. Convenciona-se que $\overline{\mathbf{t}} = \mathbf{f}$ e $\overline{\mathbf{f}} = \mathbf{t}$. Dado $A \subseteq L_\Sigma$, designa-se por $\overline{A}$ o conjunto constituído pelos conjugados dos elementos de A.

$LE_\Sigma = L_\Sigma \cap CE_\Sigma$ é o conjunto dos *literais de estado* e $LE_\Sigma^{\mathbf{tf}} = L_\Sigma^{\mathbf{tf}} \cap CE_\Sigma^{\mathbf{tf}}$. ∎

Fórmulas que resultam da substituição de um atributo o por um constrangimento de estado p noutro constrangimento de estado q irão ser particularmente úteis para descrever o efeito que a ocorrência de uma dada acção tem sobre o valor desse atributo.

Definição 2.9 Sejam $o \in Atr$ e $p, q \in CE_\Sigma^{\mathbf{tf}}$. A fórmula em $CE_\Sigma^{\mathbf{tf}}$ que resulta da *substituição de o por p em q* representa-se por $q\binom{o}{p}$ e define-se do seguinte modo:

- se $q \in \{\mathbf{t}, \mathbf{f}\}$ então $q\binom{o}{p} = q$;
- se $q \in Atr$ então $q\binom{o}{p} = p$ se $q = o$ e $q\binom{o}{p} = q$ caso contrário;
- se $q = \neg q'$ então $q\binom{o}{p} = \neg q'\binom{o}{p}$;
- se $q = q' \wedge q''$ então $q\binom{o}{p} = q'\binom{o}{p} \wedge q''\binom{o}{p}$. ∎

Dado que a ocorrência de uma acção pode alterar o valor de vários atributos torna-se necessário introduzir uma generalização da Definição 2.9 na qual se considera a substituição *simultânea* dos atributos $o_1, \ldots, o_m$ pelos constrangimentos de estado $p_1, \ldots, p_m$

num dado constrangimento de estado q. Em geral tal substitução simultânea não corresponde à substituição sucessiva dos atributos o_i pelos constrangimentos de estado p_i. Por exemplo, se em p_1 ocorrer o_2 (ou seja, $o_2 \in Sbf(p_1)$) em $q(^{o_1}_{p_1})$ existem novas ocorrências de o_2 que serão substituídas por p_2 em $q(^{o_1}_{p_1})(^{o_2}_{p_2})$. Torna-se necessário então recorrer no decurso do cálculo a símbolos proposicionais auxiliares não pertencentes a Atr que irão temporariamente substituir os atributos o_i nos locais onde não se quer que p_i seja colocado. A introdução de tais símbolos não causa qualquer problema pois (ver Lema 2.11) tais símbolos não ocorrem na fórmula final se $q, p_1, \ldots, p_m \in CE^{\mathbf{tf}}_{\Sigma}$. A definição que se segue é uma adaptação da definição apresentada em [4] para substituição simultânea de variáveis por termos numa fórmula no âmbito da lógica de primeira ordem.

Definição 2.10 Sejam $\Sigma_{Aux} = (Acc, Atr \cup Aux)$, $q \in CE^{\mathbf{tf}}_{\Sigma_{Aux}}$, $p_1, \ldots, p_m \in CE^{\mathbf{tf}}_{\Sigma_{Aux}}$ e $o_1, \ldots, o_m \in Atr \cup Aux$ onde $m > 0$, $o_i \neq o_j$ para quaisquer $1 \leq i, j \leq m$, $i \neq j$ e tal que $Aux \backslash Sbf(\{q, p_1, \ldots, p_m\})$ tem pelo menos $m-1$ elementos. A fórmula em $CE^{\mathbf{tf}}_{\Sigma_{Aux}}$ que resulta da *substituição simultânea de* $o_1, \ldots, o_m$ *por* $p_1, \ldots, p_m$ *em* q representa-se por $q\,^{o_1 \ldots o_m}_{p_1 \ldots p_m}$ e define-se do seguinte modo:

- $q^{o_1}_{p_1} = q(^{o_1}_{p_1})$,
- sendo $m > 1$
  - se $o_m \notin Sbf(q)$ então $q\,^{o_1 \ldots o_m}_{p_1 \ldots p_m} = q\,^{o_1 \ldots o_{m-1}}_{p_1 \ldots p_{m-1}}$;
  - se $o_m \in Sbf(q)$ então $q\,^{o_1 \ldots o_m}_{p_1 \ldots p_m} = q\,^{o_1 \ldots o_{m-1}}_{p'_1 \ldots p'_{m-1}}(^{o_m}_{p_m})(^{z}_{o_m})$ onde $z \in Aux$, $z \notin Sbf(q)$ e, para cada $1 \leq i \leq m-1$, $z \notin Sbf(p_i)$ e $p'_i = p_i(^{o_m}_{z})$. ∎

Lema 2.11 Seja $\Sigma_{Aux} = (Acc, Atr \cup Aux)$ tal que $Aux \cap Atr = \emptyset$ e Aux tem pelo menos $m-1$ elementos. Se $q \in CE^{\mathbf{tf}}_{\Sigma}$, $p_1, \ldots, p_m \in CE^{\mathbf{tf}}_{\Sigma}$ e $o_1, \ldots, o_m \in Atr$ onde $m > 0$, $o_i \neq o_j$ para quaisquer $1 \leq i, j \leq m$, $i \neq j$, então $q\,^{o_1 \ldots o_m}_{p_1 \ldots p_m} \in CE^{\mathbf{tf}}_{\Sigma}$.

Prova: Prova-se facilmente que se $z \notin Sbf(\{q, p_1, \ldots, p_m\})$ então $z \notin Sbf(q\,^{o_1 \ldots o_m}_{p_1 \ldots p_m})$. ∎

Lema 2.12 Sejam, $q, q' \in CE^{\mathbf{tf}}_{\Sigma}$, $p_1, \ldots, p_m \in CE^{\mathbf{tf}}_{\Sigma}$ e $o_1, \ldots, o_m \in Atr$ onde $m > 0$ e $o_i \neq o_j$ para quaisquer $1 \leq i, j \leq m$, $i \neq j$.

1. Se $q \in (Atr \cup \{\mathbf{t}, \mathbf{f}\}) \backslash \{o_1, \ldots, o_m\}$ então $q\,^{o_1 \ldots o_m}_{p_1 \ldots p_m} = q$.
2. Se $q = o_i$ para algum $1 \leq i \leq m$ então $q\,^{o_1 \ldots o_m}_{p_1 \ldots p_m} = p_i$.
3. $(\neg q)\,^{o_1 \ldots o_m}_{p_1 \ldots p_m} = \neg q\,^{o_1 \ldots o_m}_{p_1 \ldots p_m}$.
4. $(q \wedge q')\,^{o_1 \ldots o_m}_{p_1 \ldots p_m} = q^{o_1 \ldots o_m}_{p_1 \ldots p_m} \wedge q'\,^{o_1 \ldots o_m}_{p_1 \ldots p_m}$.

Prova: As asserções 1, 2 e 3 provam-se facilmente por indução em m. A asserção 4 prova-se também por indução em m recorrendo ainda a alguns lemas intermédios em cujas provas se usa também indução estrutural. ∎

Observação 2.13 Ao longo desta dissertação existem diversas situações em que, dado um conjunto finito e não vazio A, é necessário considerar uma sequência sobre A que enumere sem repetição todos os seus elementos. Assim, denotar-se-á por $Enm(A)$ o conjunto de todas as enumerações de A, isto é, o conjunto de todas as sequências $a_1 \ldots a_n$ onde $s : \{j \in I\!N_0 : j < n\} \to A$ é uma bijecção e $s(i) = a_{i+1}$ para todo $i \in \{j \in I\!N_0 : j < n\}$. ∎

2.3 Semântica

Nesta secção introduzem-se as noções de estrutura de interpretação sobre uma assinatura de objecto e de satisfação e validade de fórmulas. Assume-se fixada a assinatura de objecto $\Sigma = (Acc, Atr)$.

Definição 2.14 Uma *estrutura de interpretação sobre* Σ é uma função

$$\lambda : I\!N_0 \to \wp(Atr \cup \triangledown Acc \cup \diamond Acc)$$

tal que para cada $k \in I\!N_0$

- existe um e um só $a \in Acc$ tal que $\triangledown a \in \lambda(k)$;
- se $\triangledown a \in \lambda(k)$ então $\diamond a \in \lambda(k)$. ∎

Tal como é frequente na literatura, a estrutura linear do tempo é aqui representada através do conjunto $I\!N_0$.

Definição 2.15 Seja λ uma estrutura de interpretação sobre Σ. A *satisfação de* $f \in F_\Sigma$ *por* λ *em* $k \in I\!N_0$ denota-se por $\lambda, k \models f$ e define-se indutivamente do seguinte modo:

- se $f = \mathbf{t}$ então $\lambda, k \models f$;
- se $f = \mathbf{f}$ então não se tem que $\lambda, k \models f$;
- se $f \in Atr \cup \triangledown Acc \cup \diamond Acc$ então $\lambda, k \models f$ sse $f \in \lambda(k)$;
- se $f = \neg f'$ então $\lambda, k \models f$ sse não se tem que $\lambda, k \models f'$;
- se $f = f' \wedge f''$ então $\lambda, k \models f$ sse $\lambda, k \models f'$ e $\lambda, k \models f''$;
- se $f = \mathbf{X}\, f'$ então $\lambda, k \models f$ sse $\lambda, k+1 \models f'$;
- se $f = f'\ \mathbf{U}\ f''$ então $\lambda, k \models f$ sse existe $k'' \geq k$ tal que $\lambda, k'' \models f''$ e $\lambda, k' \models f'$ para todo $k \leq k' < k''$. ∎

Para cada $k \in I\!N_0$, $\lambda(k)$ caracteriza um estado do objecto, pois atribui valores aos atributos determinando quais os atributos que são satisfeitos e quais os que não são satisfeitos. Ao longo da dissertação far-se-á várias vezes referência à satisfação/verificação de uma fórmula num dado instante/estado. Tais referências devem, como é natural, ser entendidas como a satisfação da fórmula num dado $k \in I\!N_0$.

Relativamente à noção de satisfação de fórmulas por uma estrutura de interpretação, adopta-se a versão ancorada da lógica temporal [40, 13] no âmbito da qual uma fórmula temporal é satisfeita por uma estrutura de interpretação sse fôr satisfeita no instante inicial, isto é, em $k = 0$.

Definição 2.16 Sejam $f, f' \in F_\Sigma$, $A \subseteq F_\Sigma$ e λ estrutura de interpretação sobre Σ:

- λ *satisfaz* ou é *modelo* de f, $\lambda \models f$, sse $\lambda, 0 \models f$; f diz-se *possível* sse tem um modelo e *impossível* caso contrário;
- λ *satisfaz* ou é *modelo* de A, $\lambda \models A$, sse $\lambda \models f$ para todo $f \in A$; A diz-se *possível* ou *coerente* sse tem um modelo e *impossível* ou *incoerente* caso contrário;
- f diz-se *válida*, $\models f$, sse todas as estruturas de interpretação sobre Σ são modelos de f.
- f e f' dizem-se *equivalentes* sse $\models f \Leftrightarrow f'$. ■

Como é habitual, usa-se $\lambda, k \not\models f$ e $\lambda \not\models f$ sempre que não se tem que $\lambda, k \models f$ e não se tem que $\lambda \models f$, respectivamente.

Lema 2.17 Seja λ uma estrutura de interpretação sobre Σ e $k \in I\!N_0$:

(i) $\lambda, k \models f' \vee f''$ sse $\lambda, k \models f'$ ou $\lambda, k \models f''$;

(ii) $\lambda, k \models f' \Rightarrow f''$ sse se $\lambda, k \models f'$ então $\lambda, k \models f''$;

(iii) $\lambda, k \models f' \Leftrightarrow f''$ sse $\lambda, k \models f' \Rightarrow f''$ e $\lambda, k \models f'' \Rightarrow f'$;

(iv) $\lambda, k \models \mathbf{G}\, f$ sse $\lambda, k \models f$ para todo $k' \geq k$;

(v) $\lambda, k \models \mathbf{F}\, f$ sse existe $k' \geq k$ tal que $\lambda, k' \models f$;

(vi) $\lambda, k \models f'\, \mathbf{W}\, f''$ sse $\lambda, k \models f$ para todo $k' \geq k$ ou existe $k'' \geq k$ tal que $\lambda, k'' \models f''$ e $\lambda, k' \models f'$ para todo $k \leq k' < k''$.

Prova: Estes resultados resultam das Definições 2.3 e 2.15. ■

Lema 2.18 Sejam $q \in CE_\Sigma^{\mathbf{tf}}$, λ e λ' duas estruturas de interpretação sobre Σ e $k, k' \in I\!N_0$ tal que $\lambda(k) \cap Atr = \lambda'(k') \cap Atr$. Tem-se que $\lambda, k \models q$ sse $\lambda', k' \models q$.

Prova: A prova decorre por indução estrutural recorrendo à Definição 2.15. ■

2.4 Especificação

Uma especificação de objectos inclui uma assinatura de objecto, fórmulas e fórmulas-esquema que descrevem o comportamento do objecto. Antes de apresentar a noção de especificação de objecto introduz-se o conceito de esquema de valoração, semelhante ao apresentado em [61].

Definição 2.19 Sejam $a \in Acc$, $p_1, \ldots, p_m \in CE_\Sigma^{\mathbf{tf}}$ e $o_1, \ldots, o_m \in Atr$ onde $m > 0$ e $o_i \neq o_j$ para quaisquer $1 \leq i, j \leq m$, $i \neq j$.

$$\mathbf{G}((\nabla a \wedge \alpha) \Rightarrow (\mathbf{X}\,\alpha)) \text{ e } \mathbf{G}((\nabla a \wedge \alpha^{o_1 \ldots o_m}_{p_1 \ldots p_m}) \Rightarrow (\mathbf{X}\,\alpha))$$

dizem-se *esquemas de valoração* para a. S_Σ^a é o conjunto dos esquemas de valoração para a e $S_\Sigma = \bigcup_{a \in Acc} S_\Sigma^a$.

Sendo $q \in CE_\Sigma^{\mathbf{tf}}$, a *instância-$q$* dos esquemas de valoração anteriores é, respectivamente,

$$\mathbf{G}((\nabla a \wedge q) \Rightarrow (\mathbf{X}\,q)) \text{ e } \mathbf{G}((\nabla a \wedge q^{o_1 \ldots o_m}_{p_1 \ldots p_m}) \Rightarrow (\mathbf{X}\,q)).$$

A função $\iota : \wp(S_\Sigma) \times \wp(CE_\Sigma^{\mathbf{tf}}) \to \wp(F_\Sigma)$ tal que

$$\iota(S, C) = \{f \in F_\Sigma : f \text{ é a instância-}q \text{ de } s \in S \text{ e } q \in C\}$$

para cada $S \subseteq S_\Sigma$ e $C \subseteq CE_\Sigma^{\mathbf{tf}}$ diz-se *função de instanciação*. ∎

A instância-q de um esquema de valoração para a traduz os efeitos da ocorrência dessa acção sobre o constrangimento de estado q. Suponha-se, por exemplo, que o esquema de valoração é $\mathbf{G}((\nabla a \wedge \alpha^{o_1 \ldots o_m}_{p_1 \ldots p_m}) \Rightarrow (\mathbf{X}\,\alpha))$ e $o_i \notin Sbf(q)$ qualquer que seja $1 \leq i \leq m$ ou que o esquema de valoração é $\mathbf{G}((\nabla a \wedge \alpha) \Rightarrow (\mathbf{X}\,\alpha))$. Em ambos os casos a instância-q é $\mathbf{G}((\nabla a \wedge q) \Rightarrow (\mathbf{X}\,q))$ e traduz o facto de a ocorrência de a não ter qualquer efeito sobre q. Se $q = o_i$ para algum $1 \leq i \leq m$, então a instância-q e a instância-$\neg q$ do primeiro esquema são, respectivamente, $\mathbf{G}((\nabla a \wedge p_i) \Rightarrow (\mathbf{X}\,o_i))$ e $\mathbf{G}((\nabla a \wedge (\neg p_i)) \Rightarrow (\mathbf{X}(\neg o_i)))$. Estas duas fórmulas caracterizam completamente o efeito da ocorrência de a sobre o atributo o_i.

Definição 2.20 Uma *especificação de objecto* é um tuplo $eob = (\Sigma, AxF, AxS)$ tal que

- Σ é uma assinatura de objecto;
- $AxF \subseteq F_\Sigma$ é um conjunto finito;
- $AxS \subseteq S_\Sigma$ é um conjunto finito.

As fórmulas em AxF e os esquemas em AxS dizem-se *axiomas* de eob e *axiomas esquema* de eob, respectivamente. Os axiomas de eob que são constrangimentos de estado dizem-se *condições iniciais* de eob.

Dado $F' \subseteq F_\Sigma$ finito, o *enriquecimento de eob com F'* é a especificação de objecto $eob = (\Sigma, AxF \cup F', AxS)$. ∎

Exemplo 2.21 O tuplo $eob = (\Sigma, AxF, AxS)$ com

$$\Sigma = (\{a_1, a_2\}, \{x, y, z\})$$

$$AxF = \{y, \; \mathbf{G}(\diamond a_1 \Rightarrow (\neg y)), \; \mathbf{G}(\diamond a_2 \Rightarrow z)\}$$

$$AxS = \{\mathbf{G}((\nabla a_1 \wedge \alpha^{\,x\;\;y\;\;z}_{\,\neg z\;x\;\neg z}) \Rightarrow (\mathbf{X}\,\alpha)), \; \mathbf{G}((\nabla a_2 \wedge \alpha^{\,y\;\;z}_{\,z\;\neg x}) \Rightarrow (\mathbf{X}\,\alpha))\}$$

é uma especificação de objecto. ∎

Seguem-se as noções usuais de modelo de uma especificação de objecto e de especificação coerente e incorente.

Definição 2.22 Seja $eob = (\Sigma, AxF, AxS)$ uma especificação de objecto. A estrutura de interpretação λ sobre Σ é *modelo* de *ob* sse $\lambda \models AxF \cup \iota(AxS, CE_{\Sigma}^{\mathbf{tf}})$; *eob* diz-se *coerente* sse *eob* tem pelo menos um modelo e *incoerente* caso contrário. ∎

Definição 2.23 Seja $eob = (\Sigma, AxF, AxS)$ uma especificação de objecto, $f \in F_{\Sigma}$ e $A \subseteq F_{\Sigma}$:

- f é *eob-possível* sse existe um modelo de *eob* que também é modelo de f;
- A é *eob-possível* sse existe um modelo de *eob* que também é modelo de A;
- f é *eob-válida*, $eob \models f$, sse todos os modelos de *eob* são também modelos de f. ∎

Novamente, usa-se $eob \not\models f$ sempre que não se tem que $eob \models f$.

Certas fórmulas são particularmente relevantes na descrição do comportamento dos objectos e por isso ser-lhe-ão atribuídas designações especiais.

Definição 2.24 Sejam $q \in CE_{\Sigma}^{\mathbf{tf}}$ e $a \in Acc$:

- a fórmula $(\mathbf{G}(\mathbf{F} \diamond a)) \Rightarrow (\mathbf{G}(\mathbf{F} \triangledown a))$ designa-se por *requisito de justiça para a*;
- a fórmula $\mathbf{G}(\diamond a \Rightarrow q)$ designa-se por *restrição de activação de tipo 1 para a*; a condição associada à restrição de activação $\mathbf{G}(\diamond a \Rightarrow q)$ denota-se por $cnd(\mathbf{G}(\diamond a \Rightarrow q))$ e é o constrangimento de estado q;
- a fórmula $\mathbf{G}(q \Rightarrow \diamond a)$ designa-se por *restrição de activação de tipo 2 para a*; a condição associada à restrição de activação $\mathbf{G}(q \Rightarrow \diamond a)$ denota-se por $cnd(\mathbf{G}(q \Rightarrow \diamond a))$ e é o constrangimento de estado q.

Denota-se por $RJst_{\Sigma}^{a}$ o conjunto constituído pelo requisito de justiça para a. Denota-se por $RActv1_{\Sigma}^{a}$ o conjunto das restrições de activação de tipo 1 para a e por $RActv2_{\Sigma}^{a}$ o conjunto das restrições de activação de tipo 2 para a. Consideram-se ainda os seguintes conjuntos: $RJst_{\Sigma} = \bigcup_{a \in Acc} RJst_{\Sigma}^{a}$, $RActv1_{\Sigma} = \bigcup_{a \in Acc} RActv1_{\Sigma}^{a}$, $RActv2_{\Sigma} = \bigcup_{a \in Acc} RActv2_{\Sigma}^{a}$ e $RActv_{\Sigma} = \bigcup_{a \in Acc} (RActv1_{\Sigma}^{a} \cup RActv2_{\Sigma}^{a})$. Dado o conjunto $R \subseteq RActv_{\Sigma}$ denota-se por $cnd(R)$ o conjunto $\{cnd(f) : f \in R\}$. ∎

Restrições de activação para uma acção a caracterizam condições de activação para essa acção. Para que uma acção ocorra é necessário que esteja activada mas o contrário não é necessariamente verdade. A activação de uma acção indica a disponibilidade da acção para ocorrer. Deste modo, as restrições de activação representam também restrições à ocorrência das acções. Restrições de activação de tipo 1 descrevem condições necessárias para a activação de a e restrições de activação de tipo 2 descrevem condições suficientes para a activação de a.

As restrições de activação de tipo 1 são essenciais para assegurar invariantes e outras propriedades de segurança. Se apenas se pretende assegurar que o comportamento do objecto verifica, por exemplo, um certo invariante é suficiente considerar apenas restrições de activação de tipo 1. Aliás, se apenas se consideram propriedades de segurança não é necessário introduzir o conceito de activação de uma acção como distinto do conceito de ocorrência. No entanto, uma forma de assegurar outro tipo de propriedades, como por exemplo propriedades de resposta, passa pela distinção deste dois conceitos [60].

Uma forma de garantir a verificação de propriedades de resposta é considerar restrições de activação de tipo 2 conjuntamente com a imposição de requisitos de justiça. Nestes casos é necessário garantir que certas acções que podem ocorrer durante a vida do objecto ocorrem de facto. As restrições de activação de tipo 2 exprimem condições sob as quais uma acção estará necessariamente activada. Os requisitos de justiça exprimem precisamente que uma acção não pode estar activada um número infinito de vezes e ocorrer apenas um número finito de vezes. Assim, estes dois tipos de requisitos contribuem para a garantia da verificação de propriedades de resposta. Na literatura, o requisito de justiça aqui referido aparece sob a designação de justiça forte [22, 42]. Existe também na literatura o conceito de justiça fraca o qual pode ser expresso através da fórmula temporal $(\mathbf{F}(\mathbf{G}\diamond a))\Rightarrow(\mathbf{G}(\mathbf{F}\triangledown a))$. A justiça forte implica a justiça fraca. Nesta dissertação considerar-se-á apenas justiça forte.

Mais detalhes sobre estes assuntos podem ser encontrados no Capítulo 3.

Observação 2.25 No que se segue trabalhar-se-á no contexto de especificações de objecto $eob = (\Sigma, AxF, AxS)$ tal que

- $AxF \subseteq CE^{\mathbf{tf}}_{\Sigma} \cup RActv_{\Sigma} \cup RJst_{\Sigma}$;
- $AxS = \bigcup_{a\in Acc}\{s_a\}$ onde $s_a \in S^a_{\Sigma}$ para todo $a \in Acc$. ■

A Observação 2.25 descreve uma situação frequente no âmbito das linguagens/lógicas de especificação de objectos. Tendo em conta que cada objecto é uma entidade cujo estado interno, caracterizado pelos valores dos seus atributos, evolui exclusivamente à custa da ocorrência das suas acções, o comportamento do objecto é usualmente descrito através do modo como as acções modificam os atributos e da imposição de restrições à ocorrência das acções.

2.5 Verificação

A verificação de que o comportamento do objecto descrito por uma dada especificação verifica uma certa propriedade consiste na derivação, no contexto de um cálculo apropriado, da fórmula que expressa essa propriedade a partir do conjunto de fórmulas incluídas na especificação.

Na subsecção 2.5.1 faz-se referência à utilização de tableaux temporais para verificação de especificações de objectos. O assunto será tratado de um modo sucinto uma vez que nesta dissertação não irá ser dada ênfase à utilização deste tipo de tableaux. Para provar propriedades expressáveis através de fórmulas temporais ou testar a coerência de uma dada especificação, pode adoptar-se qualquer um dos métodos baseados em tableaux existentes na literatura para verificação no âmbito da lógica temporal proposicional linear. A utilização de tableaux para este fim permite não só assegurar que uma certa propriedade é verificada mas também obter informação sobre porque é que uma outra propriedade não o é. Da análise de um tableaux que confirme a não verificação de uma propriedade é possível extrair estruturas de interpretação para a especificação que não satisfazem a fórmula que expressa a propriedade desejada.

Tal como já foi referido no Capítulo 1, certas classes de propriedades são particularmente relevantes no âmbito de sistemas reactivos. Existem métodos que permitem tornar mais expedita a verificação de propriedades das diferentes classes. São constituídos por regras que permitem que a validade da fórmula que caracteriza a propriedade possa ser inferida a partir da validade de outras fórmulas mais simples e cuja validade é mais simples de estabelecer. Estas técnicas são também aplicáveis no âmbito da abordagem à especificação de objectos adoptada nesta dissertação e permitem que seja possível tratar o problema da verificação trabalhando exclusivamente ou parcialmente com tableaux proposicionais. No caso da prova de invariantes e outras propriedades de segurança, por exemplo, cada uma das premissas das regras é uma fórmula cuja prova envolve apenas ou raciocínio sobre o estado inicial ou raciocínio sobre dois estados consecutivos genéricos. Nestes casos pode trabalhar-se exclusivamente com tableaux proposicionais porque permitem não só a prova das premissas relativas ao estado inicial, como seria de esperar, mas também, devido ao modo como os efeitos das acções sobre os atributos são especificados, a prova das outras premissas. Noutros casos, como por exemplo o caso da prova de propriedades de resposta, apenas parte das premissas são do tipo referido. Os tableaux proposicionais podem ser usados para a prova de todas essas premissas e só será necessário recorrer aos tableaux temporais para as outras. Estes tópicos são ilustrados na subsecção 2.5.2. Os tableaux proposicionais são aí apresentados com algum detalhe dado a papel relevante que vão desempenhar nos Capítulos 3 e 4.

2.5.1 Tableaux temporais

Nesta subsecção faz-se referência à utilização de tableaux para a lógica temporal proposicional linear no âmbito da verificação das especificações de objectos consideradas nesta dissertação.

Recordem-se, em primeiro lugar, noções sintácticas e semânticas da lógica temporal proposicional linear. Mais detalhes podem ser encontrados, por exemplo, em [13]. Sendo SP um conjunto (numerável) de símbolos proposicionais, o conjunto das $LTPL(SP)$-fórmulas, $F_{LTPL(SP)}$, define-se indutivamente: $\{\mathbf{t}, \mathbf{f}\} \cup SP$ está contido em $F_{LTPL(SP)}$ e se f, f' pertencem a $F_{LTPL(SP)}$ então $(\neg f), (f \wedge f')$, $(\mathbf{X}\, f), (f' \,\mathbf{U}\, f)$ também pertencem a $F_{LTPL(SP)}$. Uma $LTPL(SP)$-estrutura de interpretação é uma função $\tau : I\!N_0 \to \wp(SP)$. As noções $LPTL(SP)$-satisfação em $k \in I\!N_0$, de modelo, $LPTL(SP)$-possibilidade e $LPTL(SP)$-impossibilidade de fórmulas ou conjuntos de fórmulas são como as apresentadas nas Definições 2.15 e 2.16.

A designação tableau temporal é usualmente utilizada de uma forma genérica quando se fala em algoritmos para testar a satisfação de uma fórmula f no âmbito da lógica temporal. Existem dois tipos de tableaux temporais os quais são designados em [32] por tableaux declarativos e tableaux incrementais. Em ambos os casos são construídos e manipulados grafos cujos nós são conjuntos de fórmulas obtidos segundo certas regras. Certos caminhos dos grafos representam modelos de f. A diferença está em que no caso dos tableaux declarativos se constroem todos os nós que é possível obter através das regras enquanto que no caso dos tableaux incrementais apenas se constroem os nós que se podem obter partindo de um certo conjunto de nós iniciais. A construção de tableaux declarativos é geralmente mais simples de descrever e os tableaux analisam-se mais facilmente. Por outro lado, os tableaux incrementais são mais eficientes e portanto mais apropriados para implementação.

Descrições de tableaux para a lógica temporal podem ser encontradas, por exemplo, em [66, 13, 5, 32, 43]. Nestes trabalhos são considerados diferentes fragmentos da lógica temporal os quais vão desde o fragmento da lógica temporal linear comprendendo apenas os operadores de futuro **X** e **F** [5], até à lógica temporal linear com todos os operadores de passado e futuro [32, 43] ou à lógica temporal ramificada [13].

Dos resultados de correcção e completude associados a estes tableaux resulta que dada uma fórmula $f \in LPTL(SP)$ é possível, em tempo finito, construir um tableau para f e decidir se f é ou não $LPTL(SP)$-possível. No caso de f ser $LPTL(SP)$-possível é ainda possível extrair do tableau modelos de f.

No que se segue assume-se fixada a assinatura de objecto $\Sigma = (Acc, Atr)$ e a especificação de objecto $eob = (\Sigma, AxF, AxS)$. Assume-se ainda que o conjunto de símbolos proposicionais é o conjunto $SP_\Sigma = \nabla Acc \cup \diamond Acc \cup Atr$.

O lema e a proposição que seguem mostram o modo como os tableaux temporais contribuem para verificação de especificações de objectos como as consideradas nesta dissertação. Para verificar se uma fórmula f é eob-válida basta testar se uma conjunção f' das fórmulas em $V_{eob} \cup \{\neg f\}$ é ou não possível onde V_{eob} é um determinado conjunto de fórmulas obtido a partir de AxF e AxS. O teste à possibilidade de f' é conduzido através da construção de um tableau temporal para f'. Se f' é possível então f não é eob-válida. Os modelos de f' que podem ser obtidos a partir do tableau são modelos de eob que não verificam f. Estes modelos podem ser analisados para descobrir quais as razões que conduzem à não verificação de f.

A coerência das especificações também pode ser testada recorrendo aos tableaux temporais testando a possibilidade de uma conjunção das fórmulas em V_{eob}.

Lema 2.26 Sejam $a \in Acc$, $s \in S^a_\Sigma$ e λ uma estrutura de interpretação sobre Σ.

1. Se $s = \mathbf{G}((\nabla a \wedge \alpha^{o_1 \ldots o_m}_{p_1 \ldots p_m}) \Rightarrow (\mathbf{X}\,\alpha)) \in S^a_\Sigma$ com $m \geq 1$ então tem-se que

$$\lambda \models (\bigcup_{1 \leq j \leq m} \{\mathbf{G}(\nabla a \Rightarrow (p_j \Leftrightarrow (\mathbf{X}\, o_j)))\}) \cup (\bigcup_{o \in Atr \setminus \{o_1,\ldots,o_m\}} \{\mathbf{G}(\nabla a \Rightarrow (o \Leftrightarrow (\mathbf{X}\, o)))\} \text{ sse } \lambda \models \iota(\{s\}, CE^{\mathbf{tf}}_\Sigma).$$

2. Se $s = \mathbf{G}((\nabla a \wedge \alpha) \Rightarrow (\mathbf{X}\,\alpha))$ então tem-se que

$$\lambda \models \bigcup_{o \in Atr}\{\mathbf{G}(\nabla a \Rightarrow (o \Leftrightarrow (\mathbf{X}\,o)))\} \text{ sse}$$
$$\lambda \models \iota(\{s\}, CE_\Sigma^{\mathbf{tf}}).$$

Prova: (1) (a) Suponha-se que $\lambda \models \iota(\{s\}, CE_\Sigma^{\mathbf{tf}})$. Então, em particular, para todo $o \in Atr$ tem-se que $\lambda \models \mathbf{G}((\nabla a \wedge o_{p_1\ldots p_m}^{o_1\ldots o_m}) \Rightarrow (\mathbf{X}\,o))$ e $\lambda \models \mathbf{G}((\nabla a \wedge (\neg o)_{p_1\ldots p_m}^{o_1\ldots o_m}) \Rightarrow (\mathbf{X}(\neg o)))$. Pelo Lema 2.12, se $o \in Atr \backslash \{o_1, \ldots, o_m\}$, então $o_{p_1\ldots p_m}^{o_1\ldots o_m} = o$ e $(\neg o)_{p_1\ldots p_m}^{o_1\ldots o_m} = \neg o$ e se $o = o_j$ para algum $1 \leq j \leq m$ então $o_{p_1\ldots p_m}^{o_1\ldots o_m} = p_j$ e $(\neg o)_{p_1\ldots p_m}^{o_1\ldots o_m} = \neg p_j$. Assim pode concluir-se que $\lambda \models \bigcup_{o \in Atr\backslash\{o_1,\ldots,o_m\}}\{\mathbf{G}(\nabla a \Rightarrow (o \Leftrightarrow (\mathbf{X}\,o)))\}$ e $\lambda \models \bigcup_{1 \leq j \leq m}\{\mathbf{G}(\nabla a \Rightarrow (p_j \Leftrightarrow (\mathbf{X}\,o_j)))\}$.

(b) Prova-se agora que, sendo $q \in CE_\Sigma^{\mathbf{tf}}$, se $\lambda \models \bigcup_{o \in Atr\backslash\{o_1,\ldots,o_m\}}\{\mathbf{G}(\nabla a \Rightarrow (o \Leftrightarrow (\mathbf{X}\,o)))\}$ e $\lambda \models \bigcup_{1 \leq j \leq m}\{\mathbf{G}(\nabla a \Rightarrow (p_j \Leftrightarrow (\mathbf{X}\,o_j)))\}$ então $\lambda \models \mathbf{G}((\nabla a \wedge q_{p_1\ldots p_m}^{o_1\ldots o_m}) \Rightarrow (\mathbf{X}\,q))$. A prova decorre por indução na complexidade de $q \in CE_\Sigma^{\mathbf{tf}}$. Deste resultado decorre naturalmente que $\lambda \models \iota(\{s\}, CE_\Sigma^{\mathbf{tf}})$.

Base: O caso $q \in \{\mathbf{t}, \mathbf{f}\}$ é consequência da Definição 2.15 e do Lema 2.12. Se $q = o_j$ para algum $1 \leq j \leq m$, pelo Lema 2.12, $q_{p_1\ldots p_m}^{o_1\ldots o_m} = p_j$ e portanto, usando a hipótese, tem-se que $\lambda \models \mathbf{G}((\nabla a \wedge q_{p_1\ldots p_m}^{o_1\ldots o_m}) \Rightarrow (\mathbf{X}\,o_j))$. O caso $q = o \in Atr\backslash\{o_1, \ldots, o_m\}$ é semelhante.

Passo: Seja $q = q_1 \wedge q_2$, $k \in I\!N_0$ e suponha-se que $\lambda, k \models \nabla a \wedge q_{p_1\ldots p_m}^{o_1\ldots o_m}$. Pelo Lema 2.12, $q_{p_1\ldots p_m}^{o_1\ldots o_m} = {q_1}_{p_1\ldots p_m}^{o_1\ldots o_m} \wedge {q_2}_{p_1\ldots p_m}^{o_1\ldots o_m}$ e portanto $\lambda, k \models {q_1}_{p_1\ldots p_m}^{o_1\ldots o_m}$ e $\lambda, k \models {q_2}_{p_1\ldots p_m}^{o_1\ldots o_m}$. Por hipótese de indução, $\lambda, k \models \mathbf{X}\,q_1$ e $\lambda, k \models \mathbf{X}\,q_2$ pelo que $\lambda, k \models \mathbf{X}\,q$.

Seja $q = \neg q_1$, $k \in I\!N_0$ e suponha-se que $\lambda, k \models \nabla a \wedge q_{p_1\ldots p_m}^{o_1\ldots o_m}$.

(i) O caso $q_1 \in \{\mathbf{t}, \mathbf{f}\}$ decorre da Definição 2.15 e do Lema 2.12.

(ii) Se $q_1 = o_j$ para algum $1 \leq j \leq m$, pelo Lema 2.12, $q_{p_1\ldots p_m}^{o_1\ldots o_m} = \neg p_j$ e portanto, usando a hipótese, tem-se que $\lambda, k \models \mathbf{X}\,q$. O caso $q = o$ e $o \in Atr\backslash\{o_1, \ldots, o_m\}$ é semelhante.

(iii) Se $q_1 = \neg q_2$, pelo Lema 2.12, $q_{p_1\ldots p_m}^{o_1\ldots o_m} = \neg(\neg {q_2}_{p_1\ldots p_m}^{o_1\ldots o_m})$ e portanto $\lambda, k \models {q_2}_{p_1\ldots p_m}^{o_1\ldots o_m}$. Por hipótese de indução, $\lambda, k \models \mathbf{X}\,q_2$ e portanto $\lambda, k \models \mathbf{X}\,q$.

(iv) Se $q_1 = q_2 \wedge q_3$, pelo Lema 2.12, $q_{p_1\ldots p_m}^{o_1\ldots o_m} = \neg({q_2}_{p_1\ldots p_m}^{o_1\ldots o_m} \wedge {q_3}_{p_1\ldots p_m}^{o_1\ldots o_m})$ e portanto tem-se que $\lambda, k \models \neg {q_2}_{p_1\ldots p_m}^{o_1\ldots o_m}$ ou $\lambda, k \models \neg {q_3}_{p_1\ldots p_m}^{o_1\ldots o_m}$. No primeiro caso, novamente pelo Lema 2.12, $\neg {q_2}_{p_1\ldots p_m}^{o_1\ldots o_m} = (\neg q_2)_{p_1\ldots p_m}^{o_1\ldots o_m}$ e consequentemente $\lambda, k \models (\neg q_2)_{p_1\ldots p_m}^{o_1\ldots o_m}$. Por hipótese de indução, $\lambda, k \models \mathbf{X}(\neg q_2)$ e portanto $\lambda, k \models \mathbf{X}\,q$. O segundo caso é semelhante.

(2) A prova é semelhante à anterior. ∎

Proposição 2.27 Seja $f \in F_\Sigma$ e V_{eob} o conjunto

$$\{\mathbf{G}(\nabla a \Rightarrow \diamond a) \colon a \in Acc\} \cup \{\mathbf{G}(\neg(\nabla a \wedge \nabla a')) \colon a, a' \in Acc, a \neq a'\}$$
$$\cup \{\mathbf{G}(\nabla a_1 \vee \ldots \vee \nabla a_n)\} \cup AxF \cup F(AxS)$$

onde $a_1 \ldots a_n \in Enm(Acc)$ e $F(AxS) = \bigcup_{s \in AxS} F(s)$ sendo, para cada $s \in AxS$,

- $F(s) = \bigcup_{o \in Atr}\{\mathbf{G}(\nabla a \Rightarrow (o \Leftrightarrow (\mathbf{X}\,o)))\}$ se $s = \mathbf{G}((\nabla a \wedge \alpha) \Rightarrow (\mathbf{X}\,\alpha))$ e
- $F(s) = (\bigcup_{1 \leq j \leq m}\{\mathbf{G}(\nabla a \Rightarrow (p_j \Leftrightarrow (\mathbf{X}\,o_j)))\}) \cup (\bigcup_{o \in Atr\backslash\{o_1,\ldots,o_m\}}\{\mathbf{G}(\nabla a \Rightarrow (o \Leftrightarrow (\mathbf{X}\,o)))\}$ se $s = \mathbf{G}((\nabla a \wedge \alpha_{p_1\ldots p_m}^{o_1\ldots o_m}) \Rightarrow (\mathbf{X}\,\alpha))$ com $m \geq 1$.

Tem-se que $V_{eob} \cup \{\neg f\}$ é $LTPL(SP_\Sigma)$-impossível sse $eob \models f$.

Prova: (a) Seja $V_{eob} \cup \{\neg f\}$ $LTPL(SP_\Sigma)$-impossível e suponha-se, por absurdo, que existe uma estrutura de interpretação λ sobre Σ tal que λ é modelo de eob e $\lambda \models \neg f$. Pelas Definições 2.15, 2.14 e 2.22, $\lambda \models AxF$, $\lambda \models \{\mathbf{G}(\triangledown a \Rightarrow \diamond a) \colon a \in Acc\}$, $\lambda \models \mathbf{G}(\triangledown a_1 \vee \ldots \vee \triangledown a_n)$ e $\lambda \models \{\mathbf{G}(\neg(\triangledown a \wedge \triangledown a')) : a, a' \in Acc, a \neq a'\}$. Pela Definição 2.22, $\lambda \models \iota(AxS, CE_\Sigma^{\mathbf{tf}})$ e portanto, pelo Lema 2.26, $\lambda \models F(AxS)$. Assim, $\lambda \models V_{eob} \cup \{\neg f\}$ o que contradiz o facto de $V_{eob} \cup \{\neg f\}$ ser $LTPL(SP_\Sigma)$-impossível.

(b) Suponha-se que $eob \models f$ e suponha-se, por absurdo, que existe uma LTPL(SP_Σ)-estrutura de interpretação τ que satisfaz $V_{eob} \cup \{\neg f\}$. Como $\tau \models \{\mathbf{G}(\triangledown a \Rightarrow \diamond a) \colon a \in Acc\}$ então, quaisquer que sejam $a \in Acc$ e $k \in I\!N_0$, se $\triangledown a \in \tau(k)$ então $\diamond a \in \tau(k)$. Como $\tau \models \{\mathbf{G}(\neg(\triangledown a \wedge \triangledown a')) \colon a, a' \in Acc, a \neq a'\}$ e $\tau \models \mathbf{G}(\triangledown a_1 \vee \ldots \vee \triangledown a_n)$ então para todo $k \in I\!N_0$ existe um e um só $a \in Acc$ tal que $\triangledown a \in \tau(k)$. Assim, τ é uma estrutura de interpretação sobre Σ. Dado que $\tau \models F(AxS)$, pelo Lema 2.26, $\tau \models \iota(AxS, CE_\Sigma^{\mathbf{tf}})$. Como $\tau \models AxF$, conclui-se então que τ é modelo de eob. O facto de que $\tau \models \neg f$ contradiz a hipótese $eob \models f$. ■

2.5.2 Tableaux proposicionais

Nesta subsecção apresentam-se, na subsubsecção 2.5.2.1, a noção de tableau proposicional e outros conceitos e resultados habitualmente associados e, na subsubsecção 2.5.2.2, ilustra-se a utilização de tableaux proposicionais no âmbito da verificação de especificações de objectos. Apresenta-se ainda, na subsubsecção 2.5.2.3, um resultado sobre tableaux proposicionais que não surge habitualmente na literatura mas que é relevante no contexto da utilização destes tableaux nas técnicas abdutivas desenvolvidas nos capítulos seguintes.

2.5.2.1 Conceitos básicos

De entre vários livros que descrevem tableaux para lógica clássica podem citar-se [21, 5, 3, 4]. Estes tableaux são árvores etiquetadas cujas etiquetas são conjuntos de fórmulas. Nesta dissertação adopta-se uma definição de tableau na qual se considera que as etiquetas têm também informação relativa a certos nós da árvore. Mais concretamente, um tableau será uma árvore etiquetada em $\wp(CE_\Sigma^{\mathbf{tf}}) \times ((N \times CE_\Sigma^{\mathbf{tf}}) \cup \{(\star, \star)\})$, onde Σ é uma assinatura de objecto, N é o conjunto de nós da árvore e se assume que $\star \notin N$ e $\star \notin CE_\Sigma^{\mathbf{tf}}$. Esta alteração tem como objectivo permitir referir de um modo preciso qual é o nó e fórmula da sua etiqueta que é responsável pela existência de um dado nó do tableau e respectiva etiqueta. Essa informação encontra-se registada na segunda componente da etiqueta. A possibilidade de fazer tais referências de um modo preciso torna mais claras, em certas situações, as provas de alguns resultados relativos a tableaux, tendo sido particularmente importante para a prova apresentada para a Proposição 2.54 (e lemas associados). A inclusão do par $(\star, \star)$ tem apenas como objectivo providenciar a segunda componente da etiqueta para o nó raiz.

Note-se que, a partir da definição de tableau aqui adoptada, se pode recuperar a noção mais usual de tableau se se considerar como etiqueta de cada nó apenas a primeira componente da etiqueta aqui definida.

No seguimento assume-se fixada uma assinatura de objecto $\Sigma = (Acc, Atr)$.

Recorde-se que uma árvore pode ser vista como um conjunto parcialmente ordenado $(N, \leq)$ com mínimo e tal que $(\downarrow n, \leq_n)$, onde $\leq_n$ é a restrição de $\leq$ a $\downarrow n = \{n' \in N : n' \leq n\}$, é um conjunto totalmente ordenado para cada $n \in N$. Se N é finito a árvore diz-se *finita*.

Habitualmente associadas à noção de árvore estão diversas noções que se recordam seguidamente. Os elementos de N dizem-se nós e sendo n_1 e n_2 dois nós, n_2 é sucessor de n_1 (n_1 é predecessor de n_2) sse $n_1 \leq n_2$ e n_2 é sucessor directo de n_1 (n_1 é predecessor directo de n_2) sse $n_1 \leq n_2$, $n_1 \neq n_2$ e não existe $n' \in N \setminus \{n_1, n_2\}$ tal que $n_1 \leq n'$ e $n' \leq n_2$. Os nós que não têm sucessores directos dizem-se folhas e o nó mínimo é a raiz. Para cada nó n, $\downarrow n = \{n' \in N : n' \leq n\}$ é um caminho. O comprimento de um caminho é o seu cardinal e representa-se por $|\downarrow n|$; se $|\downarrow n| = k \in I\!N_0$, $|\downarrow n|$ pode ser representado pela sequência $n_1 \ldots n_k$ onde n_1 é a raiz da árvore e, para todo $1 \leq i < k$, n_i é o predecessor directo de n_{i+1}. Um caminho é um ramo sse inclui uma folha. Estas noções são naturalmente extensíveis a qualquer outra entidade que envolva árvores devendo ser nesse caso entendidas como relativos à(s) árvore(s) envolvida(s).

Recorde-se finalmente que, sendo E um conjunto, uma E-árvore ou árvore etiquetada em E é um par $((N, \leq), e)$ constituído por uma árvore $(N, \leq)$ e por uma função etiqueta $e : N \to E$. O conjunto E é conjunto das etiquetas e, para cada $n \in N$, $e(n)$ é a etiqueta do nó n.

Notação 2.28 Sejam N um conjunto, $N' \subseteq N$, $n \in N$ e $arv = (N, \leq)$ uma árvore

- o conjunto $\wp(CE^{\mathbf{tf}}_{\Sigma}) \times ((N \times CE^{\mathbf{tf}}_{\Sigma}) \cup \{(\star, \star)\})$ é no seguimento denotado por $Etq(\Sigma, N)$ e assume-se sempre que $\star \notin N \cup CE^{\mathbf{tf}}_{\Sigma}$;
- sendo (arv, e) uma $Etq(\Sigma, N)$-árvore e $e(n) = (A, (x, y))$ tem-se que: $e_{\mathbf{1}}(n) = A$, $e_{\mathbf{2}}(n) = (x, y)$ e $e_{\mathbf{1}}(N') = \bigcup_{n' \in N'} e_{\mathbf{1}}(n')$; $Rm((arv, e))$ é o conjunto de todos os ramos de arv. ■

No que se segue torna-se útil considerar a noção de α-fórmula e de β-fórmula.

Definição 2.29 Seja $q \in CE^{\mathbf{tf}}_{\Sigma}$:

- se $q = \neg(\neg q')$ ou $q = q' \wedge q''$ então q é *α-fórmula*; para cada α-fórmula q define-se o conjunto $\kappa_1(q)$ do seguinte modo:
  - $\kappa_1(\neg(\neg q')) = \{q'\}$,
  - $\kappa_1(q' \wedge q'') = \{q', q''\}$;
- se $q = \neg(q' \wedge q'')$ então q é *β-fórmula*; para cada β-fórmula q definem-se dois conjuntos $\kappa_1(q)$ e $\kappa_2(q)$ do seguinte modo: $\kappa_1(\neg(q' \wedge q'')) = \{\neg q'\}$ e $\kappa_2(\neg(q' \wedge q'')) = \{\neg q''\}$. ■

Definição 2.30 Seja $C \subset CE^{\mathbf{tf}}_{\Sigma}$. A $Etq(\Sigma, N)$-árvore t diz-se *tableau singular para C* sse N é um conjunto singular cujo elemento tem etiqueta $(C, (\star, \star))$. ■

Tableaux para C obtêm-se a partir de outros tableaux para C mais simples através de certas regras de construção.

Definição 2.31 Seja $q \in CE^{\mathbf{tf}}_{\Sigma}$. A *regra de construção associada* a q é a regra $\neg\neg$ se $q = \neg(\neg q')$, a regra $\wedge$ se $q = q' \wedge q''$ e a regra $\neg\wedge$ se $q = \neg(q' \wedge q'')$. ■

Definição 2.32 Seja $C \subseteq CE^{\mathbf{tf}}_{\Sigma}$ finito. O conjunto dos *tableaux proposicionais* para C, $T_{\Sigma}(C)$, é definido indutivamente do seguinte modo:

- se t é um tableau singular para C então $t \in T_{\Sigma}(C)$;

- se $t = ((N, \leq), e) \in T_{\Sigma}(C)$, $\rho \in Rm(t)$, q é α-fórmula e $q \in e_{\mathbf{1}}(n)$ para algum $n \in \rho$ tal que $e_{\mathbf{2}}(x) \neq (n, q)$ para todo $x \in \rho$ então a $Etq(\Sigma, N \cup \{n'\})$-árvore
$$t' = ((N \cup \{n'\}, \leq'), e') \in T_{\Sigma}(C)$$
onde $n' \notin N$, $\leq' = \leq \cup \{(n, n') : n \in \rho \cup \{n'\}\}$, $e'(n) = e(n)$ para todo $n \in N$ e $e'(n') = (\kappa_1(q), (n, q))$; nestas condições, t' diz-se *obtido a partir de t pela regra de construção associada a q aplicada a ρ relativamente a $q \in e_{\mathbf{1}}(n)$*;

- se $t = ((N, \leq), e) \in T_{\Sigma}(C)$, $\rho \in Rm(t)$, q é β-fórmula e $q \in e_{\mathbf{1}}(n)$ para algum $n \in \rho$ tal que $e_{\mathbf{2}}(x) \neq (n, q)$ para todo $x \in \rho$ então a $Etq(\Sigma, N \cup \{n', n''\})$-árvore
$$t' = ((N \cup \{n', n''\}, \leq'), e') \in T_{\Sigma}(C)$$
onde $n', n'' \notin N$, $n' \neq n''$, $\leq' = \leq \cup \{(n, n') : n \in \rho \cup \{n'\}\} \cup \{(n, n'') : n \in \rho \cup \{n''\}\}$, $e'(n) = e(n)$ para todo $n \in N$, $e'(n') = (\kappa_1(q), (n, q))$ e $e'(n'') = (\kappa_2(q), (n, q))$; nestas condições, t' diz-se *obtido a partir de t pela regra de construção associada a q aplicada a ρ relativamente a $q \in e_{\mathbf{1}}(n)$*.

Um *tableau proposicional no contexto de F_{Σ}* é um elemento de $T_{\Sigma}(C)$ onde $C \subseteq CE^{\mathbf{tf}}_{\Sigma}$ é finito e não vazio. ■

No seguimento, a referência a um tableau deve ser sempre entendida como sendo relativa a um tableau proposicional no contexto de F_{Σ} e assume-se fixado um conjunto finito e não vazio $C \subseteq CE^{\mathbf{tf}}_{\Sigma}$.

Um tableau t é assim uma árvore finita etiquetada em $((N, \leq), e)$ em que cada nó tem no máximo dois sucessores directos e em que a etiqueta de cada nó n distinto da raiz é um par $(\kappa_i(q), (n', q))$ onde $n' \neq n$ é um predecessor de n, $q \in e_{\mathbf{1}}(n')$ é α-fórmula ou β-fórmula e $1 \leq i \leq 2$. É a existência da α-fórmula ou β-fórmula q em $e_{\mathbf{1}}(n')$ que leva à existência de n e essa informação encontra-se explícita na etiqueta de n. A partir de t pode construir-se um novo tableau se existir outra α-fórmula (β-fórmula) $q' \in e_{\mathbf{1}}(m')$, $m' \in N$, que possa gerar um outro nó m'_1 (dois outros nós m'_1 e m'_2) como sucessor(es) directo(s) da folha de algum ramo ρ que contenha m' e que ainda não contenha nenhum nó m'' gerado por (m', q'), isto é, nenhum nó m'' tal que $e_{\mathbf{2}}(m'') = (m', q')$. O novo tableau t' é em tudo igual a t e apenas terá, como referido, o(s) nó(s) suplementar(es) cuja(s) etiqueta(s) segue(m) o padrão descrito. Consequentemente, $Rm(t') = (Rm(t)\backslash\{\rho\}) \cup \{\rho \cup \{m'_1\}\}$ se q' é α-fórmula e $Rm(t') = (Rm(t)\backslash\{\rho\}) \cup \{\rho \cup \{m'_1\}, \rho \cup \{m'_2\}\}$ se q' é β-fórmula.

Na literatura é comum encontrar as regras de construção representadas graficamente como na Figura 2.1.

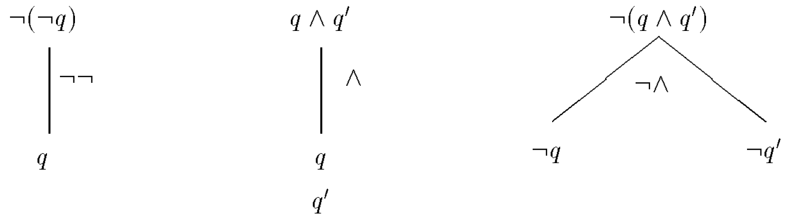

Figura 2.1: Regras de construção de tableaux

Da definição das regras de construção relativas aos conectivos primitivos resultam regras de construção $\vee$, $\neg\vee$, $\Rightarrow$,$\neg\Rightarrow$, $\Leftrightarrow$ e $\neg\Leftrightarrow$ relativas aos conectivos definidos como abreviatura. Estas regras encontram-se representadas na Figura 2.2.

Seguem-se as noções habituais neste contexto relativas a fórmulas, ramos e tableaux.

Definição 2.33 Sejam $t = ((N, \leq), e) \in T_\Sigma(C)$, $\rho \in Rm(t)$, $n \in \rho$ e $q \in e_\mathbf{1}(n)$:

- q diz-se *esgotada* em ρ sse $q \in LE_\Sigma^{\mathbf{tf}}$ ou existe $n' \in \rho$ tal que $e_\mathbf{2}(n') = (n, q)$;
- ρ diz-se *esgotado* sse qualquer que seja $n \in \rho$ se $q \in e_\mathbf{1}(n)$ então q está esgotada em ρ; $REsg(t)$ é o conjunto de todos os ramos esgotados de t;
- ρ diz-se *fechado* sse alguma das seguintes condições se verifica: (i) existe $q \in CE_\Sigma^{\mathbf{tf}}$ tal que $\{q, \neg q\} \subseteq e_\mathbf{1}(\rho)$, (ii) $\{\neg\mathbf{t}\} \subseteq e_\mathbf{1}(\rho)$, (iii) $\{\mathbf{f}\} \subseteq e_\mathbf{1}(\rho)$; $RFch(t)$ é o conjunto de todos os ramos fechados de t;
- ρ diz-se *aberto* sse $\rho \notin RFch(t)$; $RAbt(t)$ é o conjunto dos ramos abertos de t. ∎

Definição 2.34 Sejam $t = ((N, \leq), e) \in T_\Sigma(C)$ e a sequência $t_1 \ldots t_m$ de elementos de $T_\Sigma(C)$ onde $t_i = ((N_i, \leq_i), e_i)$ para cada $1 \leq i \leq m$:

- t diz-se *fechado* sse $Rm(t) = RFch(t)$;
- t diz-se *esgotado* sse $Rm(t) = REsg(t)$;
- t diz-se *aberto* sse $RAbt(t) \neq \emptyset$;
- t diz-se *tableau de decisão* sse qualquer que seja $\rho \in Rm(t)$, se $\rho \notin RFch(t)$ então $\rho \in REsg(t)$;

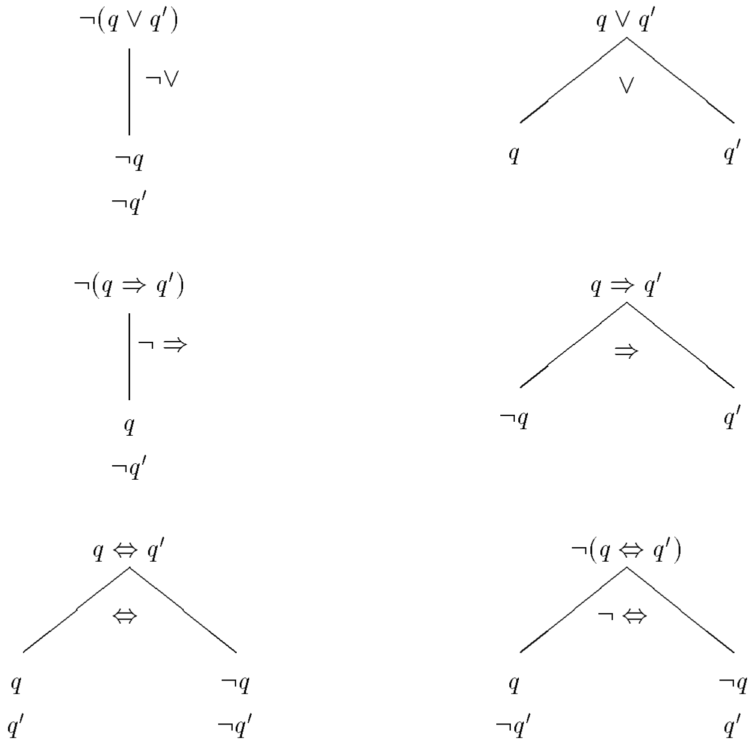

Figura 2.2: Regras de construção para abreviaturas

- $t_1 \ldots t_m$ diz-se *sequência de construção para* t sse $t_m = t$, t_1 é tableau singular para C e, para todo $1 \leq i < m$, t_{i+1} é obtido a partir de t_i pela regra de construção associada a uma fórmula $q \in e_{i\mathbf{1}}(n)$ aplicada a $\rho_i \in Rm(t_i)$ relativamente a q com $n \in \rho_i$. ∎

No que se segue, ao representar graficamente um tableau, apenas se representa em cada nó a primeira componente da respectiva etiqueta e adoptar-se-ão convenções usuais neste contexto: o símbolo $\times$ é usado para indicar os ramos fechados e omitem-se as chavetas nas etiquetas dos nós.

Exemplo 2.35 Seja Σ a assinatura da especificação de objecto *eob* apresentada no Exemplo 2.21. Na figura 2.3 representa-se graficamente um tableau para o subconjunto de $CE_\Sigma^{\mathbf{tf}}$

$$C = \{\neg y, x \vee y, \neg((\neg z) \vee x)\}$$

o qual é tableau fechado e tableau de decisão. Não é tableau esgotado porque a fórmula $\neg(\neg(z))$ não se encontra esgotada em nenhum dos ramos. ∎

Seguem-se os resultados habituais relativos à relação entre satisfação de conjuntos de fórmulas e tableaux.

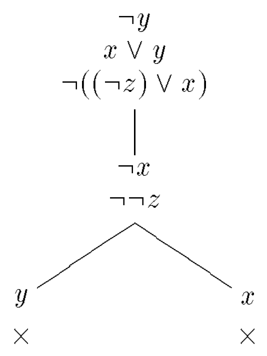

Figura 2.3: Tableau para C

Lema 2.36 Sejam λ uma estrutura de interpretação sobre Σ e $q \in CE_\Sigma^{\mathbf{tf}}$.

1. Se q é α-fórmula então $\lambda \models q$ sse $\lambda \models \kappa_1(q)$.

2. Se q é β-fórmula então $\lambda \models q$ sse $\lambda \models \kappa_i(q)$ para algum $1 \leq i \leq m$.

Prova: Imediata pelas Definições 2.15 e 2.29. ∎

Proposição 2.37 Seja $t = ((N, \leq), e) \in T_\Sigma(C)$ e $\rho \in Rm(t)$.

1. Se $\rho \in RFch(t)$ então $e_{\mathbf{1}}(\rho)$ é impossível.

2. Se $\rho \in REsg(t) \backslash RFch(t)$ então $e_{\mathbf{1}}(\rho)$ é possível e qualquer modelo de $e_{\mathbf{1}}(\rho) \cap LE_\Sigma$ é modelo de $e_{\mathbf{1}}(\rho)$.

Prova: 1. Trivial tendo em conta as Definições 2.15 e 2.33.

2.(a) Seja λ um modelo de $e_{\mathbf{1}}(\rho) \cap LE_\Sigma$. Prova-se por indução na complexidade de q que $\lambda \models q$ qualquer que seja $q \in e_{\mathbf{1}}(\rho)$.

Base: Como $\rho \notin RFch(t)$, $q \neq \mathbf{f}$. O caso $q = \mathbf{t}$, é trivial. Se $q \in Atr$ então $q \in e_{\mathbf{1}}(\rho) \cap LE_\Sigma$ e portanto $\lambda \models q$.

Passo: Seja $q \in e_{\mathbf{1}}(n)$ com $n \in \rho$.

Se q é α-fórmula ou é β-fórmula, dado que $\rho \in REsg(t)$, existe $n' \in \rho$ tal que $e_{\mathbf{2}}(n') = (n, q)$ e consequentemente $e_{\mathbf{1}}(n') = \kappa_i(q)$ para algum $1 \leq i \leq 2$. Por hipótese de indução, $\lambda \models \kappa_i(q)$ e portanto, pelo Lema 2.36, $\lambda \models q$.

Se q não α-fórmula nem β-fórmula então $q = \neg q'$ com $q' \in Atr \cup \{\mathbf{t}, \mathbf{f}\}$. Dado que $\rho \notin RFch(t)$, $q' \neq \mathbf{t}$. O caso $q' = \mathbf{f}$ é trivial. Se $q' \in Atr$ então $q \in e_{\mathbf{1}}(\rho) \cap LE_\Sigma$ e portanto $\lambda \models q$.

(b) Sendo $a \in Acc$ e $\lambda : I\!N_0 \to \wp(Atr \cup \nabla Acc \cup \diamond Acc)$ tal que $\lambda(0) = (e_{\mathbf{1}}(\rho) \cap Atr) \cup \{\nabla a, \diamond a\}$ e $\lambda(k) = \{\nabla a, \diamond a\}$ para todo $k > 0$ tem-se que λ é estrutura de interpretação sobre Σ. Seja $q \in e_{\mathbf{1}}(\rho) \cap LE_\Sigma$. Se $q \in Atr$ então $\lambda \models q$. Se $q = \neg q'$ com $q' \in Atr$, então, porque $\rho \notin RFch(t)$, $q' \notin e_{\mathbf{1}}(\rho)$ e portanto $q' \notin \lambda(0)$ o que significa que $\lambda \models q$. Conclui-se assim que λ é modelo de $e_{\mathbf{1}}(\rho) \cap LE_\Sigma$. Por (a), λ é modelo de $e_{\mathbf{1}}(\rho)$ e portanto $e_{\mathbf{1}}(\rho)$ é possível. ∎

Definição 2.38 A regra de construção associada a $q \in CE_\Sigma^{\mathbf{tf}}$ diz-se *correcta* sse se o tableau $t' = ((N', \leq'), e')$ foi obtido a partir do tableau $t = ((N, \leq), e)$ por aplicação da regra a $\rho \in Rm(t)$ relativamente a $q \in e_\mathbf{1}(n)$ com $n \in \rho$ e $e_\mathbf{1}(\rho)$ é um conjunto possível então existe $\{\rho'\} \in Rm(t') \backslash Rm(t)$ tal que $e'_\mathbf{1}(\rho')$ é também um conjunto possível. ∎

Proposição 2.39 As regras de construção $\neg\neg$, $\wedge$ e $\neg\wedge$ são correctas.

Prova: Suponha-se que $t' = ((N', \leq'), e')$ foi obtido a partir de $t = ((N, \leq), e)$ por aplicação de alguma destas regras a $\rho \in Rm(t)$ relativamente a $q \in e_\mathbf{1}(n)$ com $n \in \rho$ e seja λ uma estrutura de interpretação sobre Σ tal que $\lambda \models e_\mathbf{1}(\rho)$.

(a) Se a regra é $\neg\neg$ ou $\wedge$ então q é α-fórmula. Então $\{\rho \cup \{n'\}\} = Rm(t') \backslash Rm(t)$ com $\{n'\} = N' \backslash N$ e $e'_\mathbf{1}(n') = \kappa_1(q)$. Como $\lambda \models q$ então tem-se que $\lambda \models \kappa_1(q)$ e consequentemente $\lambda \models e'_\mathbf{1}(\rho \cup \{n'\})$.

(b) Se a regra é $\neg\wedge$ então q é β-fórmula. Neste caso, $\{\rho \cup \{n'_1\}, \rho \cup \{n'_2\}\} = Rm(t') \backslash Rm(t)$ com $\{n'_1, n'_2\} = N' \backslash N$, $e'_\mathbf{1}(n'_1) = \kappa_i(q)$ e $e'_\mathbf{1}(n'_2) = \kappa_j(q)$ onde $1 \leq i, j \leq 2$ e $i \neq j$. Dado que $\lambda \models q$ então tem-se que $\lambda \models \kappa_1(q)$ ou $\lambda \models \kappa_2(q)$ e consequentemente $\lambda \models e'_\mathbf{1}(\rho \cup \{n'_1\})$ ou $\lambda \models e'_\mathbf{1}(\rho \cup \{n'_1\})$. ∎

Proposição 2.40 Se $t = ((N, \leq), e) \in T_\Sigma(C)$ e C é possível então existe $\rho \in Rm(t)$ tal que $e_\mathbf{1}(\rho)$ é possível.

Prova: A prova decorre por indução estrutural.

Base:Imediato dado que t é um tableau singular para C e portanto o seu único ramo ρ é tal que $e_\mathbf{1}(\rho) = C$.

Passo: Há que considerar as três regras de construção pelas quais t pode ser obtido a partir de $t' = ((N', \leq'), e')$ por aplicação de uma regra a $\rho' \in Rm(t')$ relativamente a $q' \in e'_\mathbf{1}(n')$ com $n' \in \rho'$. Por hipótese de indução existe $\rho'_p \in Rm(t')$ tal que $e'_\mathbf{1}(\rho'_p)$ é possível.

(a) Regras $\neg\neg$ e $\wedge$. Nestes casos $Rm(t) = (Rm(t') \backslash \{\rho'\}) \cup \{\rho' \cup \{m\}\}$ com $\{m\} = N \backslash N'$. Se $\rho'_p \neq \rho'$ então $\rho'_p \in Rm(t)$ e $e'_\mathbf{1}(\rho'_p) = e_\mathbf{1}(\rho'_p)$ e o resultado fica estabelecido. Caso contrário, pela Proposição 2.39, $e_\mathbf{1}(\rho' \cup \{m\})$ é possível.

(b) Regra $\neg\wedge$. Neste caso tem-se que $Rm(t) = (Rm(t') \backslash \{\rho'\}) \cup \{\rho' \cup \{m_1\}, \rho' \cup \{m_2\}\}$ com $\{m'_1, m'_2\} = N \backslash N'$. Se $\rho'_p \notin \{\rho' \cup \{m_1\}, \rho' \cup \{m_2\}\}$, raciocinando como em (a), o resultado fica estabelecido. Caso contrário, pela Proposição 2.39, $e_\mathbf{1}(\rho' \cup \{m_1\})$ é possível ou $e_\mathbf{1}\rho' \cup \{m_2\})$ é possível. ∎

Proposição 2.41 Seja $t \in T_\Sigma(C)$ um tableau de decisão. O conjunto C é impossível sse t é fechado.

Prova: Seja $t = ((N, \leq), e)$. Suponha-se que C é impossível. Se existe $\rho \in Rm(t)$ tal que $\rho \notin RFch(t)$ então $\rho \in REsg(t)$ e, pela Proposição 2.37, $e_\mathbf{1}(\rho)$ é possível o que é uma contradição dado que $C \subseteq e_\mathbf{1}(\rho)$. Reciprocamente, suponha-se que t é fechado. Se C é possível então, pela Proposição 2.40, existe $\rho \in Rm(t)$ tal que $e_\mathbf{1}(\rho)$ possível o que é uma contradição porque $Rm(t) = RFch(t)$ e, pela Proposição 2.37, ter-se-ia que $e_\mathbf{1}(\rho)$ é impossível. ∎

Todas as proposições anteriores são válidas quando se utilizam as regras de construção relativas aos conectivos introduzidos como abreviaturas.

Dado $C \subseteq CE_{\Sigma}^{\mathbf{tf}}$ finito, a Proposição 2.41 garante que a partir da análise de um qualquer tableau decisão para C se pode concluir se o conjunto é ou não impossível: C é impossível se t é fechado e C é possível caso contrário. O caso particular $C = \{\neg q\}$ permite concluir a validade ou não validade de q.

Para qualquer conjunto finito $C \subseteq CE_{\Sigma}^{\mathbf{tf}}$ é sempre possível encontrar uma sequência de construção para um tableau $t \in T_{\Sigma}(C)$ esgotado. A justificação desta afirmação recorre em [4], por exemplo, à definição da noção de complexidade de um ramo como o valor natural resultante da soma da complexidade das fórmulas não esgotadas desse ramo e ao facto de que, ao longo de uma sequência de contrução, a complexidade dos ramos dos tableaux vai decrescendo.

Os tableaux descritos proporcionam assim um procedimento de decisão para o problema de saber se C é ou não impossível.

2.5.2.2 Verificação

Ilustra-se seguidamente a verificação de especificação de objectos com tableaux proposicionais dando particular atenção à prova de um certo tipo de propriedades de segurança muito comum na literatura: propriedades que podem ser expressas através de fórmulas temporais do tipo $\mathbf{G}\, q$ onde q é uma fórmula que não envolve operadores temporais. Estas propriedades são usualmente designadas por invariantes e exprimem condições sobre os estados que devem ser satisfeitas em qualquer estado.

A prova de invariantes baseia-se usualmente no argumento indutivo de que se pode concluir que q se verifica em todos os instantes sempre que (i) q se verifica inicialmente e (ii) se q se verifica num qualquer instante genérico então também se verifica no instante seguinte.

Assuma-se fixada uma especificção de objecto $eob = (\Sigma, AxF, AxS)$ com $\Sigma = (Acc, Atr)$. No âmbito da verificação de especificações de objectos, para garantir um invariante basta provar que as condições iniciais presentes em AxF implicam q e que a ocorrência de cada acção preserva q, isto é, que a ocorrência de cada acção em estados que satisfaçam q levam a estados que continuam a satisfazer q.

Seguidamente apresentam-se os resultados que justificam a prova de invariantes através de tableaux proposicionais. Esses resultados são casos particulares de outros mais gerais que se apresentam no Capítulo 3, no âmbito do raciocínio abdutivo sobre especificações de objectos, e portanto as provas consistem na indicação das proposições desse capítulo que são relevantes para cada caso. Refira-se que o que se pretende aqui é apenas ilustrar a utilização de tableaux proposicionais no âmbito da verificação das especificações de objecto consideradas nesta dissertação e não fazer um desenvolvimento mais aprofundado deste tópico.

Proposição 2.42 Seja $q \in CE_\Sigma^{\mathbf{tf}}$. Se $eob \models q$ e $eob \models \mathbf{G}((\nabla a \wedge q) \Rightarrow (\mathbf{X}\, q))$ para cada $a \in Acc$ então $eob \models \mathbf{G}\, q$.

Prova: Pelas Proposição 3.67 e Corolário 3.69. ∎

Proposição 2.43 Sejam $q \in CE_\Sigma^{\mathbf{tf}}$ e C_{CI} definido indutivamente do seguinte modo

– $AxF \cap CE_\Sigma^{\mathbf{tf}} \subseteq C_{CI}$

– se $q_1, \ldots, q_m \in C_{CI}$, $m \geq 1$, e existem $a' \in Acc$ e $f'_1 \ldots f'_{m'} \in Enm(AxF \cap RActv2_\Sigma^{a'})$, $m' \geq 1$, tal que a fórmula $(q_1 \wedge \ldots \wedge q_m) \Rightarrow (cnd(f'_1) \vee \ldots \vee cnd(f'_{m'}))$ é válida então $cnd(AxF \cap RActv1_\Sigma^{a'}) \subseteq C_{CI}$.

Se existe um tableau fechado para $C_{CI} \cup \{\neg q\}$ então $eob \models q$.

Prova: Pelas Definições 3.43 e 3.49 e Proposição 3.53. ∎

Proposição 2.44 Sejam $q \in CE_\Sigma^{\mathbf{tf}}$, $a \in Acc$, $AxS \cap S_\Sigma^a = \{\mathbf{G}((\nabla a \wedge \alpha_{p_1 \ldots p_n}^{o_1 \ldots o_n}) \Rightarrow (\mathbf{X}\, \alpha))\}$ e C_{RActv} definido indutivamente do seguinte modo

– $cnd(AxF \cap RActv1_\Sigma^a) \subseteq C_{RActv}$

– se $q_1, \ldots, q_m \in C_{RActv}$, $m \geq 1$, e existem $a' \in Acc$ e $f'_1 \ldots f'_{m'} \in Enm(AxF \cap RActv2_\Sigma^{a'})$, $m' \geq 1$, tal que a fórmula $(q_1 \wedge \ldots \wedge q_m) \Rightarrow (cnd(f'_1) \vee \ldots \vee cnd(f'_{m'}))$ é válida então $cnd(AxF \cap RActv1_\Sigma^{a'}) \subseteq C_{RActv}$.

Se existe um tableau fechado para $C_{RActv} \cup \{q, \neg q_{p_1 \ldots p_n}^{o_1 \ldots o_n}\}$ então $eob \models \mathbf{G}((\nabla a \wedge q) \Rightarrow (\mathbf{X}\, q))$.

Prova: Pelas Definições 3.6 e 3.14 e Proposição 3.18. ∎

Exemplo 2.45 Considere-se a especificação eob apresentada no Exemplo 2.21.

1.Pela Proposição 2.43 tem-se que $eob \models x \vee y$ pois existe tableau fechado para o conjunto $C_{CI} \cup \{\neg(x \vee y)\} = \{y, \neg(x \vee y)\}$ (Figura 2.4).

$$\begin{array}{c} y \\ \neg(x \vee y) \\ | \\ \neg x \\ \neg y \\ \times \end{array}$$

Figura 2.4: Tableau para $C_{CI} \cup \{\neg(x \vee y)\}$

2.Pela Proposição 2.44 tem-se que $eob \models \mathbf{G}((\nabla a_1 \wedge (x \vee y)) \Rightarrow (\mathbf{X}(x \vee y)))$ pois existe tableau fechado para $C_{RActv} \cup \{x \vee y, \neg(x \vee y)\,{}_{\neg z}^{x}\,{}_{x}^{y}\,{}_{\neg z}^{z}\} = \{\neg y, x \vee y, \neg((\neg z) \vee x)\}$ (ver Exemplo 2.35).

$$
\begin{array}{c}
z \\
x \vee y \\
\neg(x \vee z) \\
| \\
\neg x \\
\neg z \\
\times
\end{array}
$$

Figura 2.5: Tableau relativo à acção a_2

3.Pela Proposição 2.44 tem-se que $eob \models \mathbf{G}((\nabla a_2 \wedge (x \vee y)) \Rightarrow (\mathbf{X}(x \vee y)))$ pois existe tableau fechado para $C_{RActv} \cup \{z, x \vee y, \neg(x \vee y)\,{}^{y}_{z}\,{}^{z}_{\neg x}\} = \{z, x \vee y, \neg(x \vee z)\}$ (Figura 2.5).

4.Pela Proposição 2.42, $eob \models \mathbf{G}(x \vee y)$. ∎

Para terminar refira-se que provas de outros tipos de propriedades de segurança podem também ser conduzidas recorrendo a tableaux proposicionais de um modo semelhante ao que foi ilustrado para o caso dos invariantes. Como se verá no Capítulo 3, nesses casos é usualmente necessário provar não apenas asserções do tipo $eob \models \mathbf{G}((\nabla a \wedge q) \Rightarrow (\mathbf{X}\, q))$ e $eob \models q$ mas também asserções do tipo $eob \models \mathbf{G}((\nabla a \wedge q') \Rightarrow (\mathbf{X}\, q))$ com $q' \neq q$. Os tableaux que permitem provar este último tipo de asserções são semelhantes aos considerados na Proposição 2.44.

No caso das outras propriedades atrás referidas como, por exemplo, propriedades de resposta, garantia ou persistência, uma parte das premissas das regras usuais (ver Capítulo 3) são do tipo indicado e por isso os tableaux proposicionais podem ser usados para resolver uma parte das tarefas associadas ao problema da prova da sua verificação.

Note-se que neste contexto não se assegura a completude do processo de verificação. Contrariamente ao que acontece no caso de usar os tableaux temporais, pode acontecer que uma especificação verifique um determinado invariante $\mathbf{G}\, q$ mas que não seja possível encontrar uma prova do tipo descrito nesta subsecção. Basta pensar no caso de numa especificação tal que (i) $\mathbf{G}\, p$ verifica-se, (ii) existe uma acção a que não preserva q e (iii) a só está activada se se verificar $\neg p$.

2.5.2.3 Independência

O objectivo desta última subsubsecção é provar a Proposição 2.54. Esta proposição estabelece um resultado importante no contexto das técnicas de raciocínio abdutivo apresentadas nos próximos capítulos. Este resultado é mencionado sem demonstração em [45] e não foi encontrada nenhuma prova na literatura. Ele não é referido na literatura relativa à utilização destes tableaux como algoritmo de decisão para a validade de fórmulas proposionais pois não é relevante nesse contexto. No entanto, este resultado é importante quando se utilizam estes tableaux no âmbito do raciocínio abdutivo pois, como se verá nos capítulos seguintes, os literais presentes nas etiquetas dos ramos abertos de certos tableaux de decisão são fundamentais para as técnicas abdutivas utilizadas. O referido resultado assegura que não se obtêm resultados diferentes se se analisarem diferentes tableaux de decisão para um mesmo conjunto.

Para provar a Proposição 2.54 há que provar vários resultados intermédios e introduzir algumas noções auxiliares sobre tableaux que capitalizam na informação contida na segunda componente da etiqueta dos nós dos tableaux.

Definição 2.46 Sejam $t = ((N, \leq), e) \in T_\Sigma(C)$, $n \in N$ e $q \in e_{\mathbf{1}}(n)$:

- se n é distinto do nó raiz, o par $e_{\mathbf{2}}(n)$ diz-se *gerador* de n;
- a sequência $(n_1, q_1)\ldots(n_k, q_k)$ de elementos de $N \times CE^{\mathbf{tf}}_\Sigma$ diz-se *sequência geradora de* (n, q) sse $(n_k, q_k) = (n, q)$, n_1 é o nó raiz e (n_{i-1}, q_{i-1}) é o gerador de n_i para cada $1 < i \leq k$. ∎

Lema 2.47 Sejam $t = ((N, \leq), e) \in T_\Sigma(C)$, $n \in N$ e $q \in e_{\mathbf{1}}(n)$. Existe sequência geradora para (n, q).

Prova: Para cada $n \in N$ seja c_n o comprimento do caminho $\{n' \in N : n' \leq n\}$. Seja ν o nó raiz de t. A prova decorre por indução em c_n.

Base: se $c_n = 1$ então $n = \nu$ e portanto, para cada $q \in e_{\mathbf{1}}(n)$, a sequência constituída pelo par (n, q) é sequência geradora de (n, q).

Passo: seja $c_n = k > 1$. Sendo $e_{\mathbf{2}}(n) = (m, q_m)$, tem-se que $q_m \in e_{\mathbf{1}}(m)$ e $m < n$. Assim, $c_m < c_n$ e portanto, por hipótese de indução, (m, q_m) tem uma sequência geradora $(\nu, q_\nu)\ldots(m, q_m)$ pelo que $(\nu, q_\nu)\ldots(m, q_m)(n, q)$ é sequência geradora de (n, q). ∎

Definição 2.48 Sejam $t = ((N, \leq), e) \in T_\Sigma(C)$ e $t' = ((N', \leq'), e') \in T_\Sigma(C)$. Sejam γ e γ' caminhos de t e t', respectivamente. A função

$$s : S_\gamma \to S_{\gamma'}$$

onde $S_\gamma = \{(n, q) : n \in \gamma \text{ e } q \in e_{\mathbf{1}}(n)\}$ e $S_{\gamma'} = \{(n, q) : n \in \gamma' \text{ e } q \in e'_{\mathbf{1}}(n)\}$ diz-se *função simulação de* γ por γ' sse, para cada $(n, q) \in S_\gamma$, se $s((n, q)) = (n', q')$ então

(i) $q' = q$;

(ii) n' é o nó raiz de t' se n é o nó raiz de t

(iii) $s(e_{\mathbf{2}}(n)) = e'_{\mathbf{2}}(n')$ se n não é o nó raiz de t.

Diz-se que o caminho γ' *simula* o caminho γ, ou que o caminho γ *é simulado pelo* caminho γ' sse é possível estabelecer uma função simulação de γ por γ'. ∎

Observação 2.49 No seguimento, sempre que haja referência uma função de simulação $s : S_\gamma \to S_{\gamma'}$ de γ por γ' estará implícito que S_γ e $S_{\gamma'}$ são conjuntos definidos como na Definição 2.48. ∎

Lema 2.50 Sejam $t, t' \in T_\Sigma(C)$ tal que t' é tableau esgotado, $\rho' \in Rm(t')$ e $\gamma_k = n_1 \dots n_k$, $k \geq 1$, caminho de t tal que $\gamma_k \notin Rm(t)$. Se γ_k é simulado por ρ' então existe um sucessor directo de n_k, n_{k+1}, tal que o caminho $\gamma_{k+1} = n_1 \dots n_k n_{k+1}$ é simulado por ρ'.

Prova: Sejam $t = ((N, \leq), e)$ e $t' = ((N', \leq'), e')$. Como $\gamma_k \notin Rm(t)$, então n_k tem sucessores directos. Da definição de $T_\Sigma(C)$ decorre que n_k tem um ou dois sucessores directos. Seja $s_k : S_{\gamma_k} \to S_{\rho'}$ a função simulação de γ_k por ρ'.

Suponha-se que n_k tem um único sucessor directo n_{k+1} e seja $e_\mathbf{2}(n_{k+1})) = (n^g_{k+1}, q^g_{k+1})$. Da definição de $T_\Sigma(C)$ decorre que $(n^g_{k+1}, q^g_{k+1}) \in S_{\gamma_k}$, q^g_{k+1} é α-fórmula e $e_\mathbf{1}(n_{k+1}) = \kappa_1(q^g_{k+1})$. Seja $s_k((n^g_{k+1}, q^g_{k+1})) = (m^g_{k+1}, q^g_{k+1}) \in S_{\rho'}$. Como $\rho' \in REsg(t')$, existe $m_{k+1} \in \rho'$ tal que $e'(m_{k+1}) = (\kappa_1(q^g_{k+1}), (m^g_{k+1}, q^g_{k+1}))$. Considere-se a função $s_{k+1} : S_{\gamma_{k+1}} \to S_{\rho'}$ da seguinte forma: $s_{k+1}((n, q)) = s_k((n, q))$ para todo o par $(n, q) \in S_{\gamma_k}$ e $s_{k+1}((n_{k+1}, q)) = (m_{k+1}, q)$ para todo $q \in e_\mathbf{1}(n_{k+1}) = e'_\mathbf{1}(m_{k+1})$. A função s_{k+1} assim definida é função de simulação de $\gamma_{k+1} = n_1 \dots n_k n_{k+1}$ por ρ'.

Suponha-se que n_k tem dois sucessores directos. Sejam eles $n1_{k+1}$ e $n2_{k+1}$. Da definição de $T_\Sigma(C)$ decorre que $e_\mathbf{2}(n1_{k+1}) = e_\mathbf{2}(n2_{k+1})$. Seja $e_\mathbf{2}(n1_{k+1}) = (n^g_{k+1}, q^g_{k+1})$. Neste caso q^g_{k+1} é β-fórmula, $e_\mathbf{1}(n1_{k+1})) = \kappa_{i_1}(q^g_{k+1})$ e $e_\mathbf{1}(n2_{k+1})) = \kappa_{i_2}(q^g_{k+1})$ com $1 \leq i_1, i_2 \leq 2$ e $i_1 \neq i_2$. Dado que $(n^g_{k+1}, q^g_{k+1}) \in S_{\gamma_k}$, seja $s_k((n^g_{k+1}, q^g_{k+1})) = (m^g_{k+1}, q^g_{k+1}) \in S_{\rho'}$. Como $\rho' \in REsg(t')$, existe $m_{k+1} \in \rho'$ tal que $e'(m_{k+1}) = (\kappa_i(q^g_{k+1}), (m^g_{k+1}, q^g_{k+1}))$ para algum $1 \leq i \leq 2$. O nó que se procura, n_{k+1}, será $n1_{k+1}$ se $\kappa_{i_1}(q^g_{k+1}) = \kappa_i(q^g_{k+1})$ e $n2_{k+1}$ caso contrário. Tal como no caso anterior, pode ser agora definida uma função simulação $s_{k+1} : S_{\gamma_{k+1}} \to S_{\rho'}$ de $\gamma_{k+1} = n_1 \dots n_k n_{k+1}$ por ρ'. ■

Proposição 2.51 Sejam $t, t' \in T_\Sigma(C)$ tal que t' é tableau esgotado. Para cada $\rho' \in Rm(t')$ existe $\rho \in Rm(t)$ tal que ρ é simulado por ρ'.

Prova: Seja $\rho' \in Rm(t')$ e $\nu_{t'}$ o nó raiz de t'. O ramo ρ pretendido pode ser obtido como se descreve. Seja $\gamma_1 = n_1$ o caminho constituído pelo nó raiz de t. A função $s_1 : S_{\gamma_1} \to S_{\rho'}$ tal que $s_1((n_1, q)) = (\nu_{t'}, q)$ para todo $q \in e_\mathbf{1}(n_1) = e'_\mathbf{1}(\nu_{t'}) = C$ é função simulação de γ_1 por ρ'. Se $\gamma_1 \in Rm(t)$ então γ_1 é o ramo ρ que se procura. Caso contrário, pelo Lema 2.50, existe um sucessor directo de n_1 tal que $\gamma_2 = n_1 n_2$ é simulado por ρ'. Continuando a proceder de modo semelhante, como t tem um número finito de nós, obtém-se necessariamente a dado momento um caminho $\gamma_k = n_1 n_2 \dots n_k$, $k \geq 1$, simulado por ρ' e tal que $\gamma_k \in Rm(t)$ o que significa que γ_k é o ramo ρ que se procura. ■

Proposição 2.52 Sejam $t = ((N, \leq), e) \in T_\Sigma(C)$ e $t' = ((N', \leq'), e') \in T_\Sigma(C)$ dois tableaux esgotados. Para cada $\rho' \in Rm(t')$ existe $\rho \in Rm(t)$ tal que $e_\mathbf{1}(\rho) = e'_\mathbf{1}(\rho')$.

Prova: Sendo $\rho' \in Rm(t')$, pela Proposição 2.51 existe $\rho \in Rm(t)$ que é simulado por ρ' através de uma função simulação $s : S_\rho \to S_{\rho'}$.

(a) Se $q \in e_\mathbf{1}(\rho)$ tem-se que $q \in e_\mathbf{1}(n)$ para algum $n \in \rho$. Como $s((n, q)) = (n', q)$ onde $n' \in \rho'$ e $q \in e'_\mathbf{1}(n')$ conclui-se que $q \in e'_\mathbf{1}(\rho')$.

(b) Seja $q' \in e'_\mathbf{1}(n')$ para certo $n' \in \rho'$. O objectivo agora é mostrar que $q' \in e_\mathbf{1}(\rho)$. Sejam ν_t e $\nu_{t'}$ os nós raiz de t e t', respectivamente.

(b.i) Se $n' = \nu_{t'}$, $e'_1(n') = C = e_1(\nu_t) \subseteq e_1(\rho)$ e portanto $q' \in e_1(\rho)$.

(b.ii) Se $n' \neq \nu_{t'}$ seja $(n'_1, q'_1) \ldots (n'_k, q'_k)$ sequência geradora de $(n', q') = (n'_k, q'_k)$ cuja existência é garantida pelo Lema 2.47. Então $k > 1$, $n'_1 = \nu_{t'}$ e $e'_2(n'_{j+1}) = (n'_j, q'_j)$ para todo $1 \leq j < k$. Prova-se por indução em j que, para todo $1 \leq j \leq k$, $(n'_j, q'_j) = s((m_j, q'_j))$ para certo $m_j \in \rho$ com $q'_j \in e_1(m_j)$.

Base: seja $j = 1$. Neste caso, $q'_1 \in e'_1(\nu_{t'})$ e raciocinando como em (b.i) conclui-se que $q'_1 \in e_1(\nu_t)$ e portanto $(n'_1, q'_1) = (\nu_{t'}, q'_1) = s((\nu_t, q'_1))$.

Passo: seja $1 \leq j < k$. Por hipótese de indução, $(n'_j, q'_j) = s((m_j, q'_j))$ para certo $m_j \in \rho$ com $q'_j \in e_1(m_j)$. Como ρ é ramo esgotado, q'_j é esgotada em ρ e, como q'_j é α-fórmula ou β-fórmula, existe $m \in \rho$ tal que $e_2(m) = (m_j, q'_j)$. Seja $q \in e_1(m)$ e $s((m, q)) = (m', q) \in S_{\rho'}$. Então tem-se que $s(e_2(m)) = e'_2(m')$. Por outro lado, $s(e_2(m)) = s((m_j, q'_j)) = (n'_j, q'_j)$ e $e'_2(n'_{j+1}) = (n'_j, q'_j)$. Assim, $s(e_2(m)) = e'_2(n'_{j+1}) = e'_2(m')$. Dado que $n'_{j+1}, m' \in \rho'$, da definição de $T_\Sigma(C)$ decorre que $n'_{j+1} = m'$ e portanto $s((m, q)) = (n'_{j+1}, q)$. Se $e'_1(n'_{j+1}) = \{q\}$ então $q'_{j+1} = q \in e_1(m) \subseteq e_1(\rho)$ e $s((m, q'_{j+1})) = (n'_{j+1}, q'_{j+1})$. Se $e'_1(n'_{j+1})$ não fôr um conjunto singular, dado que $q \in e'_1(n'_{j+1})$ e $e'_2(n'_{j+1}) = (n'_j, q'_j)$, então $q'_j = q \wedge q'_{j+1}$ ou $q'_j = q'_{j+1} \wedge q$ com $q'_{j+1} \neq q$ e, em ambos os casos, $e'_1(n'_{j+1}) = \{q, q'_{j+1}\}$. Como $e_2(m) = (m_j, q'_j)$, $e_1(m) = \{q, q'_{j+1}\}$. Assim, $q'_{j+1} \in e_1(m)$ com $m \in \rho$ e $s((m, q'_{j+1})) = (n'_{j+1}, q'_{j+1})$.

Tem-se então que $(n', q') = (n'_k, q'_k) = s((m_k, q'_k))$ para algum $m_k \in \rho$ com $q'_k \in e_1(m_k)$ e portanto $q'_k = q' \in e_1(\rho)$.

(c) De (a) e (b) resulta que $e_1(\rho) = e'_1(\rho')$. ■

Corolário 2.53 Se $t = ((N, \leq), e) \in T_\Sigma(C)$ e $t' = ((N', \leq'), e') \in T_\Sigma(C)$ são tableaux esgotados então $\{e_1(\rho) : \rho \in RAbt(t)\} = \{e'_1(\rho') : \rho' \in RAbt(t')\}$.

Prova: Sendo $B' \in \{e_1(\rho') : \rho' \in RAbt(t')\}$ então $B' = e'_1(\rho')$ para algum $\rho' \in RAbt(t')$. Pela Proposição 2.52, existe $\rho \in Rm(t)$ tal que $B' = e_1(\rho)$. Se $\rho \in RFch(t)$ então $\rho' \in RFch(t')$. Assim, $\rho \in RAbt(t)$ e portanto $B' \in \{e_1(\rho) : \rho \in RAbt(t)\}$ concluindo-se assim que o primeiro conjunto é subconjunto do segundo.

A prova de que o segundo conjunto é subconjunto do primeiro é análoga e portanto tem-se a igualdade pretendida. ■

Proposição 2.54 Se $t = ((N, \leq), e) \in T_\Sigma(C)$ e $t' = ((N', \leq'), e') \in T_\Sigma(C)$ são tableaux de decisão então $\{e_1(\rho) : \rho \in RAbt(t)\} = \{e'_1(\rho') : \rho' \in RAbt(t')\}$.

Prova: (a) Seja a sequência de construção $t_1 \ldots t$ para t. É possível prolongar esta sequência por forma a obter uma sequência de construção $t_1 \ldots t \ldots t_n$ para um tableau esgotado $t_n = ((N_n, \leq_n), e_n) \in T_\Sigma(C)$ esgotado.

(a.i) Seja $B \in \{e_1(\rho) : \rho \in RAbt(t)\}$. Então $B = e_1(\rho)$ com $\rho \in RAbt(t)$. Como t é tableau de decisão, $\rho \in REsg(t)$. Tendo em conta o modo como cada tableau da sequência é obtido a partir do tableau que anterior, $\rho \in REsg(t_n)$ e $e_1(\rho) = e_{n1}(\rho)$. Tem-se que $\rho \notin RFch(t_n)$ pois, caso contrário, $\rho \in RFch(t)$. Consequentemente, $\rho \in RAbt(t_n)$ e portanto $B \in \{e_{n1}(\rho) : \rho \in RAbt(t_n)\}$.

(a.ii) Seja $B \in \{e_{n1}(\rho) : \rho \in RAbt(t_n)\}$. Então $B = e_{n1}(\rho_n)$ com $\rho_n \in RAbt(t_n)$. Tendo novamente em conta o modo como os tableaux da sequência são construídos, existe

$\rho \in Rm(t)$ tal que $\rho \subseteq \rho_n$ e $e_{\mathbf{1}}(\rho) \subseteq e_{n\mathbf{1}}(\rho_n)$. Novamente, $\rho \notin RFch(t)$ pois, caso contrário, $\rho_n \in RFch(t_n)$. Assim, $\rho \in RAbt(t)$ e, como t é esgotado, $\rho \in REsg(t)$. Devido, uma vez mais, ao modo como se constrói a sequência, $\rho \in REsg(t_n)$ e $e_{\mathbf{1}}(\rho) = e_{n\mathbf{1}}(\rho)$. Mas se $\rho, \rho_n \in Rm(t_n)$ e $\rho \subseteq \rho_n$ então $\rho = \rho_n$. Assim, $B = e_{n\mathbf{1}}(\rho_n) = e_{n\mathbf{1}}(\rho) = e_{\mathbf{1}}(\rho)$ e portanto $B \in \{e_{\mathbf{1}}(\rho) : \rho \in RAbt(t)\}$.

(a.iii) De (a.i) e (a.ii) resulta que $\{e_{n\mathbf{1}}(\rho) : \rho \in RAbt(t_n)\} = \{e_{\mathbf{1}}(\rho) : \rho \in RAbt(t)\}$.

(b) Raciocínio idêntico se pode fazer relativamente a t', considerando-se a sequência de construção $t'_1 \dots t' \dots t'_m$ para $t'_m = (((N'_m, \leq'_m), e'_m) \in T_\Sigma(C)$ que prolonga a sequência de construção para t', concluindo-se que $\{e'_{m\mathbf{1}}(\rho) : \rho \in RAbt(t'_m)\} = \{e'_{\mathbf{1}}(\rho) : \rho \in RAbt(t')\}$.

(c) Pelo Corolário 2.53, $\{e_{n\mathbf{1}}(\rho) : \rho \in RAbt(t_n)\} = \{e'_{m\mathbf{1}}(\rho) : \rho \in RAbt(t'_m)\}$ e portanto o resultado fica estabelecido. ■

2.6 Conclusões

Neste capítulo introduziram-se as noções sintácticas e semânticas ligadas à especificação de objectos e fez-se referência ao problema da verificação neste âmbito.

Adoptou-se uma abordagem à especificação de objectos baseada na lógica temporal proposicional linear, na linha do trabalho desenvolvido em [60, 61].

Uma especificação de objecto foi definida como sendo constituída por uma assinatura, por um conjunto de fórmulas e por um conjunto de fórmulas-esquema. Como é usual, na assinatura introduzem-se os identificadores dos atributos e das acções do objecto a partir dos quais se definem as fórmulas da linguagem temporal associada ao objecto. As fórmulas e as fórmulas-esquema caracterizam o modo como o objecto poderá evoluir em termos dos requisitos que são impostos à ocorrência das acções e do efeito que a sua ocorrência tem sobre os atributos. As estruturas de interpretação são sucessões de conjuntos de literais positivos verificando certos requisitos por forma a assegurar que em cada instante ocorre apenas uma acção e que as acções só ocorrem se estiverem activadas.

No âmbito da verificação foi dada ênfase à utilização de tableaux. Em primeiro lugar descreveu-se sucintamente a utilização de tableaux temporais para testar se uma dada fórmula é satisfeita por todos os modelos de uma especificação, ou seja, para testar se uma dada propriedade expressável à custa de uma fórmula da linguagem associada ao objecto é ou não uma propriedade do comportamente especificado para o objecto. Como caso particular tem-se o teste à coerência da especificação. Seguidamente refere-se como, em certos casos, é possível tratar o problema da verificação recorrendo a tableaux proposicionais. São conhecidas na literatura várias regras que permitem assegurar a verificação de certas classes de fórmulas, expressando propriedades reconhecidamente importantes no âmbito dos sistemas reactivos, a partir da verificação de um conjunto de fórmulas mais simples. No caso particular dos invariantes ilustrou-se o modo como essas premissas podem ser provadas exclusivamente com recurso aos tableaux proposicionais. Mas o mesmo se pode dizer em relação a outras propriedades de segurança. No caso de propriedades de resposta uma parte das premissas podem também ser provadas através de tableaux proposicionais.

Os tableaux proposicionais foram descritos com um certo detalhe dado que vão ser largamente utilizados no âmbito das técnicas de raciocínio abdutivo sobre especificações de objectos/comunidades de objectos que se irão apresentar nos capítulos seguintes. Em particular, na subsubsecção 2.5.2.3, provou-se um resultado que não é habitualmente referido na literatura relativa a tableaux proposicionais, mas que é importante para a utilização destes nas técnicas de raciocínio abdutivo, pois permite assegurar que, dado um conjunto C de fórmulas, é indiferente qual é o tableaux de decisão para C que se utiliza no decurso da aplicação das referidas técnicas. A prova apresentada pressupõe uma ligeira modificação na forma como os tableaux proposicionais são usualmente definidos. O referido resultado é mencionado sem demonstração em [45] e não foi encontrada nenhuma prova na literatura.

Capítulo 3

Raciocínio abdutivo sobre objectos

3.1 Introdução

Muito trabalho sobre verificação tem vindo a ser desenvolvido na área da especificação temporal de objectos. Nesse âmbito, o objectivo é conseguir provar que os comportamentos dos objectos prescritos pelas especificações construídas verificam um certo número de propriedades. O objectivo deste capítulo é analisar o problema da verificação no âmbito de uma especificação de objecto de um ponto de vista abdutivo. Sob este ponto de vista, mais do que saber se o comportamento determinado pela especificação $eob = (\Sigma, AxF, AxS)$ verifica uma dada propriedade, aquilo que interessa é encontrar formas de completar a especificação sempre essa propriedade não é verificada. O objectivo é encontrar um conjunto E de novos axiomas com os quais se possa enriquecer a especificação dada de tal modo que o comportamento do objecto determinado pela nova especificação $eob' = (\Sigma, AxF \cup E, AxS)$ já verifique a propriedade desejada.

O problema da verificação no âmbito de especificações de objecto é enquadrado na abordagem lógica ao raciocínio abdutivo. Neste enquadramento, e usando as designações usuais na literatura, tem-se que: (i) a especificação de objecto representa o conhecimento de que se dispõe sobre o domínio em estudo (o comportamento prescrito pela especificação); (ii) as propriedades cuja verificação se pretende assegurar são as observações; (iii) as fórmulas abdutíveis são as fórmulas com as quais que se pode enriquecer a especificação; (iv) uma situação em que uma dada propriedade não é verificada constitui um problema de abdução para o qual vai ser necessário construir uma explicação.

Tal como é usual no contexto do raciocínio abdutivo, a linguagem das observações vai ser distinta da linguagem das fórmulas abdutíveis.

Neste trabalho, são consideradas como observações várias propriedades importantes no âmbito da especificação do comportamento de sistemas reactivos. Seguindo as designações utilizadas, em particular, em [41, 42], são consideradas propriedades de segurança, propriedades de resposta, propriedades de garantia e propriedades de persistência. A respectiva caracterização sintáctica é baseada na caracterização apresentada nos trabalhos mencionados.

As fórmulas abdutíveis são novos axiomas da especificação. Assim, tendo em conta o tipo de especificações de objecto com que se trabalha no âmbito desta dissertação, as fórmulas abdutíveis são condições iniciais, restrições de activação e requisitos de justiça.

As técnicas desenvolvidas ao longo deste capítulo para a geração de explicações para problemas de abdução em especificações de objectos baseiam-se, por um lado, em técnicas propostas na literatura para a verificação de propriedades de segurança [43] e de propriedades de resposta [41] e animação [39] de sistemas reactivos concorrentes e, por outro, em técnicas de raciocínio abdutivo baseadas em tableaux proposicionais [45].

As referidas técnicas para verificação de propriedades são adaptadas ao caso particular da especificação de objectos. Tipicamente essas técnicas são constituídas por regras que permitem concluir que uma dada fórmula é verificada se forem verificadas um certo número de fórmulas mais simples (as premissas da regra).

No caso das regras relativas a propriedades de segurança existem, geralmente, dois tipos de premissas. Por um lado há que garantir que são verificadas certas condições iniciais. Por outro lado há que garantir que alguns constrangimentos de estado se verificam após a ocorrência das acções sempre que certos constrangimentos de estado sejam verificados quando tal ocorrência tem lugar. As explicações que se constroem são constituídas por novos axiomas a incluir na especificação de tal forma que as premissas que não são verificadas pela especificação dada o sejam pela nova especificação. Assim, cada explicação inclui novas condições iniciais sempre que as premissas relativas à verificação das condições iniciais pretendidas não sejam verificadas. Inclui também novas restrições de activação (de tipo 1) sobre as acções que não verifiquem o outro tipo de premissas referido.

No caso dos regras relativas às outras propriedades existem mais dois tipos de premissas. Há que garantir a activação de certas acções em determinadas circunstâncias e também a verificação de certos requisitos de justiça. Neste caso as explicações vão incluir também restrições de activação (de tipo 2) e requisitos de justiça.

As técnicas de geração de explicações conduzem, geralmente, a diversas explicações possíveis. Ao longo do capítulo são apresentados diversos critérios para selecionar as explicações. Em certos casos são também indicados métodos que impedem que venham a ser geradas explicações menos desejáveis.

Este capítulo está organizado da forma que seguidamente se descreve. Na secção 3.2 introduzem-se as noções de observação sobre assinatura de objecto, de problema de abdução numa especificação de objecto e de explicação para problemas de abdução. Na secção 3.3 mostra-se como se podem construir restrições de activação que permitem assegurar que, após a ocorrência da uma dada acção, se verifica um dado constrangimento de estado q, sempre que um outro constrangimento de estado q' seja verificado quando tal ocorrência tem lugar. Na secção 3.4 mostra-se como se podem construir constrangimentos de estado que assegurem a verificação de uma dada condição inicial. Na secção 3.5 são descritas técnicas de construção de explicações para problemas de segurança (subsecção 3.5.1), para problemas de resposta (subsecção 3.5.2), para problemas de garantia (subsecção 3.5.3) e para problemas de persistência (subsecção 3.5.4). Na secção 3.6 são apresentadas as conclusões.

Ao longo das várias secções são apresentados diversos exemplos. São apresentadas inicialmente algumas especificações de objecto com as quais ao longo do capítulo vão sendo ilustradas as técnicas de abdução relativas às diferentes propriedades analisadas. Para que os detalhes relacionados com a resolução dos problemas de abdução não ficassem obscurecidos face à eventual complexidade da especificação, optou-se por considerar especificações simples que não pretendem descrever nenhum sistema em particular.

3.2 Conceitos básicos

Nesta secção introduzem-se os conceitos de observação sobre uma assinatura de objecto, de problema de abdução numa especificação de objecto e de explicação para um problema de abdução.

As observações são fórmulas que caracterizam propriedades relativas ao comportamento dos objectos e são divididas em várias classes: segurança, resposta, garantia e persistência. As várias classes de observações consideradas e sua caracterização sintáctica tem como base a hierarquia de propriedades apresentada em [41, 42] já mencionada no Capítulo 1. A caracterização sintáctica adoptada neste trabalho não é feita usando directamente as fórmulas canónicas referidas. Isto deve-se ao facto de tais fórmulas canónicas pressuporem que se trabalha no âmbito da lógica temporal incluindo também operadores de passado. Todas as fórmulas que aqui se consideram como observações de segurança, por exemplo, são equivalentes a fórmulas canónicas de segurança $\mathbf{G}\, f$ onde f envolve operadores temporais de passado. O mesmo se passa com as outras observações. Cada classe de observações para a qual são desenvolvidas no presente trabalho técnicas abdutivas constitui uma subclasse da classe correspondente na referida hierarquia.

Definição 3.1 Seja Σ uma assinatura de objecto e sejam $r, q, q_1, q_2 \in CE_\Sigma^{\mathbf{tf}}$

- as fórmulas
  - $\mathbf{G}(r \Rightarrow (\mathbf{X}\, q))$
  - $r \Rightarrow (q_1\, \mathbf{W}\, q_2)$
  - $\mathbf{G}(r \Rightarrow (q_1\, \mathbf{W}\, q_2))$

  dizem-se *observações de segurança sobre* Σ;
- a fórmula $\mathbf{G}(r \Rightarrow (q_1\, \mathbf{U}\, q_2))$ diz-se *observação de resposta sobre* Σ;
- a fórmula $r \Rightarrow (q_1\, \mathbf{U}\, q_2)$ diz-se *observação de garantia sobre* Σ;
- a fórmula $\mathbf{G}(r \Rightarrow (\mathbf{F}(\mathbf{G}\, q)))$ diz-se *observação de persistência sobre* Σ.

Qualquer fórmula equivalente a uma observação de segurança, de resposta, de garantia ou de persistência é também considerada observação de segurança, de resposta, de garantia ou de persistência, respectivamente. O conjunto O_Σ constituído por todas as observações de segurança, resposta, garantia e persistência sobre Σ designa-se por *conjunto das observações sobre* Σ. ■

Em particular, e sendo $r, q \in CE_\Sigma^{\mathbf{tf}}$, tem-se que: (i) a fórmula $\mathbf{G}\, q$ é uma observação de segurança pois é equivalente a $\mathbf{t} \Rightarrow (q\,\mathbf{W}\,\mathbf{f})$; (ii) a fórmula $\mathbf{G}(r \Rightarrow (\mathbf{F}\, q))$ é uma observação de resposta dado que é equivalente a $\mathbf{G}(r \Rightarrow (\mathbf{t}\,\mathbf{U}\, q))$; (iii) a fórmula $\mathbf{F}\, q$ é uma observação de garantia dado que é equivalente a $\mathbf{t} \Rightarrow (\mathbf{t}\,\mathbf{U}\, q))$.

As observações consideradas exprimem requisitos sobre o comportamento do objecto no que respeita à evolução do valor dos atibutos.

As observações do tipo $\mathbf{G}(r \Rightarrow (\mathbf{X}\, q))$ podem ser enquadradas no tipo de requisitos de segurança designados por vezes como requisitos dinâmicos [17, 19]. Estas observações exprimem condições que envolvem dois instantes consecutivos impondo restrições à ocorrência de acções em instantes que satisfaçam determinados constrangimentos de estado.

As bem conhecidas propriedades de invariância, ou invariantes, estão representados pelas observações do tipo $\mathbf{G}\, q$. Exprimem requisitos de segurança estáticos [17, 19] afirmando que existe um certo constrangimento de estado que é invariante, isto é, que é satisfeito em todos os instantes. Como referido, estas observações são casos particulares de $r \Rightarrow (q_1\,\mathbf{W}\, q_2)$. Um outro caso particular são as observações do tipo $r \Rightarrow (q_1\,\mathbf{W}\,\mathbf{f})$ que exprimem requisitos de invariância condicional: se r se verifica no instante inicial então q_1 é invariante. No caso geral, as observações $r \Rightarrow (q_1\,\mathbf{W}\, q_2)$ exprimem a invariância de q_1 condicionada à verificação de r no instante inicial e à invariância de $\neg q_2$.

As observações $\mathbf{G}(r \Rightarrow (q_1\,\mathbf{W}\, q_2))$, exprimem propriedades de precedência [42, 43]. Quando r é $\mathbf{t}$, exprimem que a satisfação de $\neg q_1$ tem de ser precedida pela satisfação de q_2. Podem ainda ser vistas como impondo uma certa invariância condicional parcial de q_1: a fórmula $\mathbf{G}(r \Rightarrow (q_1\,\mathbf{W}\,\mathbf{f}))$ exprime a invariância de q_1 a partir de qualquer estado que satisfaça r e fórmula $\mathbf{G}(r \Rightarrow (q_1\,\mathbf{W}\, q_2))$ exprime a invariância de q_1 a partir de qualquer estado que satisfaça r desde que $\neg q_2$ se mantenha também invariante a partir desse estado.

As observações do tipo $\mathbf{G}(r \Rightarrow (\mathbf{F}\, q))$ exprimem o facto de, em determinadas condições, mais concretamente, sempre que r se verifique, se tenha de ter necessariamente a satisfação de q ou no presente ou nalgum instante futuro. Tal pode ser visto como uma resposta q a um certo estímulo r. O caso mais geral de propriedades de resposta, $\mathbf{G}(r \Rightarrow (q_1\,\mathbf{U}\, q_2))$, exprime um requisito semelhante só que agora se pretende que haja uma certa condição que seja continuamente satisfeita até se chegar ao instante que verifica q_2.

Relativamente às observações de garantia, podem ser feitos comentários semelhantes aos apresentados no parágrafo anterior, mas, neste caso, os requisitos são mais fracos no sentido em que a resposta apenas precisa de se concretizar se o respectivo estímulo se verificar no estado inicial. O caso particular de $\mathbf{F}\, q$ exprime uma condição que apenas precisa de se verificar uma vez.

As observações de persistência $\mathbf{G}(r \Rightarrow (\mathbf{F}(\mathbf{G}\, q)))$, por seu lado, podem ser vistas como impondo também uma invariância parcial condicional de q, de certo modo à semelhança de certas propriedades de segurança que se mencionou acima. No entanto, neste caso, a invariância de q, desencadeada pela verificação de r, não está sujeita à invariância de nenhuma outra condição (q têm mesmo de se verificar persistentemente a partir de certa altura) e o início da sua verificação não tem de ser simultâneo com a verificação de r.

Uma observação sobre Σ que não seja verificada por uma especificação eob sobre Σ é um problema de abdução em eob para o qual é desejável encontrar explicações.

Definição 3.2 Seja $eob = (\Sigma, AxF, AxS)$ uma especificação de objecto. Um *problema de abdução* em eob é uma fórmula $f \in O_\Sigma$ tal que $eob \not\models f$. ∎

No que se segue, sempre que a observação envolvida num certo problema de abdução em eob seja uma observação de segurança, de resposta, de garantia, etc., dir-se-á que é um problema de segurança em eob, um problema de resposta em eob, um problema de garantia em eob, etc.

Exemplo 3.3 Considere-se $eob_1 = (\Sigma_1, AxF_1, AxS_1)$ com

$$\Sigma_1 = (\{a_1, a_2\}, \{x, y, z\})$$

$$AxF_1 = \{\neg y, \quad \mathbf{G}(\diamond a_2 \Rightarrow z)\}$$

$$AxS_1 = \{\mathbf{G}((\nabla a_1 \wedge \alpha\,{}^{x}_{\neg z}\,{}^{y}_{x}\,{}^{z}_{\neg z}) \Rightarrow (\mathbf{X}\,\alpha)), \quad \mathbf{G}((\nabla a_2 \wedge \alpha\,{}^{x}_{\neg y}\,{}^{y}_{z}\,{}^{z}_{\neg x}) \Rightarrow (\mathbf{X}\,\alpha))\}$$

A fórmula $\mathbf{G}(x \vee y)$ é um problema de abdução em eob_1. Para que $\mathbf{G}(x \vee y)$ seja eob_1-válida é necessário que $x \vee y$ seja satisfeita em todos os instantes. Mas essa satisfação não está assegurada, por exemplo, no instante inicial. A ocorrência de a_2 preserva a satisfação de $x \vee y$ uma vez que esta acção só pode ocorrer quando z é satisfeito e após a sua ocorrência y é satisfeito se e só se z o fôr quando tal ocorrência tem lugar. No entanto, a ocorrência de a_1 não preserva necessariamente a satisfação de $x \vee y$ nomeadamente quando $\neg z$ e x não são satisfeitos. ∎

Pretende-se que uma explicação E para um problema de abdução numa especificação de objecto eob seja um conjunto de novos axiomas construídos de modo a que, sendo eob' o enriquecimento da especificação eob dada com E, a observação em questão seja eob'-válida e eob' seja coerente. As explicações são conjuntos de fórmulas abdutíveis e portanto, tendo em conta o tipo de especificações que se tem vindo a considerar, as fórmulas abdutíveis são constrangimentos de estado, restrições de activação e requisitos de justiça.

Definição 3.4 Seja $eob = (\Sigma, AxF, AxS)$ uma especificação de objecto e $f \in O_\Sigma$ um problema de abdução em eob. Uma *explicação* para f é um conjunto

$$E \subseteq CE_\Sigma \cup RActv_\Sigma \cup RJst_\Sigma$$

tal que, sendo eob' o enriquecimento de eob com E,

- $eob' \models f$
- eob' é coerente. ■

Um dos requisitos habituais sobre as explicações está relacionado com a questão da coerência. Neste caso, exige-se que a nova especificação eob' seja coerente, ou seja, E tem de ser eob-possível. Tal como já foi comentado no Capítulo 1, a questão da coerência é uma questão que usualmente é resolvida *a posteriori*. Não é possível, na maior parte dos casos, encontrar técnicas de construção de explicações que construam apenas conjuntos de fórmulas que sejam coerentes com a teoria dada, ou seja, neste caso, conjuntos de fórmulas eob-possíveis. As técnicas de construção de explicações que se descrevem ao longo deste capítulo não asseguram que sejam apenas encontrados conjuntos de fórmulas eob-possíveis e portanto haverá sempre que fazer essa verificação. Para tal pode usar-se, por exemplo, tableaux temporais tal como foi referido no Capítulo 2.

Exemplo 3.5 Os conjuntos

$$E_1 = \{x, \mathbf{G}(\diamond a_1 \Rightarrow x)\}$$
$$E_2 = \{x, \mathbf{G}(\diamond a_1 \Rightarrow (\neg y))\}$$
$$E_3 = \{x, \mathbf{G}(\diamond a_1 \Rightarrow (\neg z))\}$$
$$E_4 = \{x, \mathbf{G}(\diamond a_1 \Rightarrow (x \vee (\neg y) \vee (\neg z)))\}$$

são quatro explicações possíveis para o problema de segurança referido no Exemplo 3.3.

Dado que $x \vee y$ tem de ser satisfeita no estado inicial e $eob_1 \models \neg y$, há que assegurar que x é necessariamente satisfeito no instante inicial e daí a inclusão deste constrangimento de estado em todas as explicações.

Considere-se a explicação E_1. A restrição de activação para a_1 contribui para a preservação de $x \vee y$ por a_1 porque exige que esta acção apenas possa ocorrer quando x se verifica. Como a_1 atribui a y o valor que tem x no instante em que a_1 ocorre, após a sua ocorrência $x \vee y$ é satisfeita. Comentário semelhante pode ser feito relativamente à restrição de activação em E_3.

Considere-se a explicação E_2. A restrição de activação para a_1 exige que esta acção apenas possa ocorrer quando se tem $\neg y$. Se também se tem $\neg x$ então a preservação de $x \vee y$ é trivialmente assegurada. Caso contrário, como a_1 atribui a y o valor que tem x no instante em que a_1 ocorre, a preservação de $x \vee y$ é também assegurada.

A restrição de activação para a_1 em E_4 exige que esta acção apenas possa ocorrer quando se tem x ou se tem $\neg y$ ou se tem $\neg z$ e portanto, tendo em conta os comentários anteriores, a preservação de $x \vee y$ é assegurada po a_1. ■

3.3 Geração de explicações para a garantia de constrangimento de estado a partir de outro constrangimento de estado através de uma acção

Nesta secção descreve-se o modo como se obtêm as restrições que é necessário impôr à ocorrência de uma dada acção a para que haja a garantia de que se o estado do objecto verifica $q' \in CE_\Sigma^{\mathbf{tf}}$, então as eventuais modificações sobre esse estado provocadas pela ocorrência de a conduzem à verificação de $q \in CE_\Sigma^{\mathbf{tf}}$.

Na subsecção 3.3.1 introduz-se a definição de garantia de q a partir de q' por uma acção a no âmbito de uma dada especificação de objecto e a definição de explicação para a referida garantia no âmbito dessa especificação. Para a construção das explicações contribui a análise de um certo tableau proposicional para um determinado conjunto de constrangimentos de estado escolhidos de forma apropriada a partir de q, q' e da especificação dada. Na subsecção 3.3.2 descreve-se e justifica-se a escolha do conjunto de fórmulas que se considera para construir o referido tableau. Na subsecção 3.3.3 introduz-se a noção de fecho de tableau e mostra-se como tais fechos contribuem para a construção das explicações pretendidas. Por último, na subsecção 3.3.4, discutem-se alguns critérios de preferência entre explicações.

Nas subsecções que se seguem assume-se fixada a especificação de objecto $eob = (\Sigma, AxF, AxS)$ onde $\Sigma = (Acc, Atr)$. Assumem-se também fixadas $a \in Acc$ e as fórmulas $q, q' \in CE_\Sigma^{\mathbf{tf}}$.

3.3.1 Explicações

Definição 3.6 Diz-se que *a garante q a partir de q′ em eob* sse

$$eob \models \mathbf{G}((\triangledown a \wedge q') \Rightarrow (\mathbf{X}\, q)).$$

Em particular, se $q' = \mathbf{t}$ diz-se que *a garante q em eob* e se $q' = q$ diz-se que *a preserva q em eob*. ∎

Definição 3.7 Uma *explicação para a garantia de q a partir de q′ por a em eob* é uma restrição de activação

$$\mathbf{G}(\diamond a \Rightarrow p)$$

onde

- $p = \mathbf{f}$ ou $p = (l_{11} \wedge \ldots \wedge l_{1m_1}) \vee \ldots \vee (l_{n1} \wedge \ldots \wedge l_{nm_n})$ com $n \geq 1$ e, para cada $1 \leq i \leq n$, $m_i \geq 1$, $l_{ij} \in LE_\Sigma$ para todo $1 \leq j \leq m_i$ e $l_{ij} \neq \overline{l_{ij'}}$ para quaisquer $1 \leq j, j' \leq m_i$

e tal que, sendo eob' o enriquecimento de eob com $\{\mathbf{G}(\diamond a \Rightarrow p)\}$,

- a garante q a partir de q' em eob';
- eob' é coerente.

Em particular, se $q' = \mathbf{t}$ a referida restrição de activação diz-se *explicação para a garantia de q por a em eob* e se $q' = q$ diz-se *explicação para a preservação de q por a em eob*. ∎

Exemplo 3.8 Considere-se a especificação de objecto eob_1 do Exemplo 3.3. As restrições de activação

$$f_1 = \mathbf{G}(\diamond a_1 \Rightarrow x) \qquad f_2 = \mathbf{G}(\diamond a_1 \Rightarrow (\neg y)) \qquad f_3 = \mathbf{G}(\diamond a_1 \Rightarrow (\neg z))$$
$$f_4 = \mathbf{G}(\diamond a_1 \Rightarrow (x \vee (\neg y) \vee (\neg z)))$$

são exemplos de explicações para a garantia da preservação de $x \vee y$ por a_1 em eob_1 acerca das quais foram já feitos vários comentários no Exemplo 3.5. ■

Exemplo 3.9 Considere-se a especificação de objecto $eob_2 = (\Sigma_2, AxF_2, AxS_2)$ com

$$\Sigma_2 = (\{a_1, a_2\}, \{x, y, z, u\})$$

$$AxF_2 = \{\mathbf{G}(\diamond a_1 \Rightarrow u), \mathbf{G}(\diamond a_2 \Rightarrow z), \mathbf{G}(u \Rightarrow \diamond a_2)\}$$

$$AxS_2 = \{\mathbf{G}((\nabla a_1 \wedge \alpha\,{}^{x}_{z}\,{}^{y}_{x}\,{}^{z}_{\neg z}) \Rightarrow (\mathbf{X}\,\alpha)), \mathbf{G}((\nabla a_2 \wedge \alpha\,{}^{x}_{y}\,{}^{u}_{\neg u}) \Rightarrow (\mathbf{X}\,\alpha))\}$$

As restrições de activação

$$f_1 = \mathbf{G}(\diamond a_1 \Rightarrow x) \qquad f_2 = \mathbf{G}(\diamond a_1 \Rightarrow (\neg y)) \qquad f_3 = \mathbf{G}(\diamond a_1 \Rightarrow (\neg u))$$
$$f_4 = \mathbf{G}(\diamond a_1 \Rightarrow (\neg z)) \qquad f_5 = \mathbf{G}(\diamond a_1 \Rightarrow (x \vee (\neg y)))$$

são exemplos de explicações para a garantia de $x \wedge y$ a partir de y através de a_1 em eob_2.

A explicação f_1 exige que a_1 apenas possa ocorrer quando se tem x. Das restrições de activação em AxF_2 decorre também que a_1 apenas pode ocorrer quando se tem z. Como a_1 atribui a x e y os anteriores valores de z e x, respectivamente, após a ocorrência de a_1 a fórmula $x \wedge y$ é satisfeita.

A explicação f_2 assegura trivialmente que a_1 garante qualquer fórmula a partir de y porque exige que a_1 apenas possa ocorrer quando se tem $\neg y$.

A explicação f_3 exige que a_1 apenas possa ocorrer quando se tem $\neg u$. Dado que a fórmula $\mathbf{G}(\diamond a_1 \Rightarrow u)$ é axioma de eob_2, isto significa que a_1 nunca ocorre e portanto a garantia de qualquer constrangimento de estado a partir de um outro qualquer constrangimento de estado por a_1 é trivialmente assegurada. Comentário semelhante se pode fazer relativamente a f_4 uma vez que de AxF_2 decorre que $eob_2 \models \mathbf{G}(\diamond a_1 \Rightarrow z)$.

A explicação f_5 exige que a_1 apenas possa ocorrer quando se tem x ou se tem $\neg y$ e portanto, tendo em conta os comentários anteriores, a garantia de $x \wedge y$ a partir de y é assegurada por a_1. ■

Uma forma trivial de assegurar a garantia do constrangimento de estado q a partir do constrangimento de estado q' através da acção a é impedir a ocorrência de a considerando, por exemplo, a restrição de activação $\mathbf{G}(\diamond a \Rightarrow \mathbf{f})$.

Proposição 3.10 Se $\mathbf{G}(\diamond a \Rightarrow \mathbf{f})$ é eob-possível então $\mathbf{G}(\diamond a \Rightarrow \mathbf{f})$ é uma explicação para a garantia de q a partir de q' por a em eob.

Prova: Seja eob' o enriquecimento de eob com $\{\mathbf{G}(\diamond a \Rightarrow \mathbf{f})\}$.

Seja λ um modelo de eob' e $k \in I\!N_0$. Dado que $\lambda, k \models \diamond a \Rightarrow \mathbf{f}$ tem-se necessariamente que $\lambda, k \models \neg \triangledown a$ e portanto $\lambda, k \models (\triangledown a \wedge q') \Rightarrow (\mathbf{X}\, q)$. Assim, $\lambda \models \mathbf{G}((\triangledown a \wedge q') \Rightarrow (\mathbf{X}\, q))$. Consequentemente tem-se que $eob' \models \mathbf{G}((\triangledown a \wedge q') \Rightarrow (\mathbf{X}\, q))$, isto é, a garante q a partir de q' em eob'.

Como $\mathbf{G}(\diamond a \Rightarrow \mathbf{f})$ é eob-possível então existe um modelo λ de eob que satisfaz $\mathbf{G}(\diamond a \Rightarrow \mathbf{f})$ e portanto eob' é coerente. ∎

Certas explicações restringem mais a ocorrência da acção a do que outras no sentido em que permitem que esta ocorra num maior número de situações. Introduz-se assim a noção de explicação mais liberal.

Definição 3.11 Sejam f_1 e f_2 duas explicações para a garantia de q a partir de q' por a em eob.

- f_1 é *mais liberal* que f_2 sse $cnd(f_2) \Rightarrow cnd(f_1)$ é válida;
- f_1 é *estritamente mais liberal* que f_2 sse f_1 é mais liberal que f_2 e f_2 não é mais liberal que f_1. ∎

Exemplo 3.12 Considerem-se as explicações para a garantia da preservação de $x \vee y$ por a_1 em eob_1 referidas no Exemplo 3.8. A explicação f_4 é estritamente mais liberal que as explicações f_1, f_2 e f_3.

Também no caso das explicações para a garantia de $x \wedge y$ a partir de y através de a_1 em eob_2 descritas no Exemplo 3.9 se tem que a explicação f_5 é estritamente mais liberal que as explicações f_1 e f_2. ∎

Naturalmente que qualquer explicação será mais liberal que a explicação $\mathbf{G}(\diamond a \Rightarrow \mathbf{f})$ pois com esta restrição de activação a acção a nunca poderá ocorrer.

Proposição 3.13 Qualquer explicação f para a garantia de q a partir de q' por a em eob é mais liberal que a explicação $\mathbf{G}(\diamond a \Rightarrow \mathbf{f})$.

Prova: A fórmula $\mathbf{f} \Rightarrow cnd(f)$ é válida e portanto f é mais liberal que $\mathbf{G}(\diamond a \Rightarrow \mathbf{f})$. ∎

3.3.2 Fórmulas e tableaux geradores de explicações

O objectivo desta subsecção é estabelecer quais as fórmulas resultantes da especificação e do problema de garantia em causa que se usam para construir explicações. A ideia é escolher um conjunto de constrangimentos de estado cuja incoerência seja condição suficiente para assegurar a garantia de q a partir de q' pela acção a em eob. Dado que é possível usar tableaux proposicionais para determinar a coerência ou incoerência de conjuntos de constrangimentos de estado, estes podem ser utilizados para testar a garantia de q a partir de q' por a e, quando tal garantia não é assegurada, fornecer informação relevante para a construção de explicações.

No que se segue far-se-á referência a esquemas de valoração $\mathbf{G}((\triangledown a \wedge \alpha^{o_1 \ldots o_n}_{p_1 \ldots p_n}) \Rightarrow (\mathbf{X}\, \alpha))$ em S^a_Σ e a fórmulas $q^{o_1 \ldots o_n}_{p_1 \ldots p_n}$ onde se assume genericamente que $n \in I\!N_0$. O caso $n = 0$ deverá ser entendido como o esquema $\mathbf{G}((\triangledown a \wedge \alpha) \Rightarrow (\mathbf{X}\, \alpha))$ e a fórmula q, respectivamente.

Definição 3.14 O *conjunto de constrangimentos de estado geradores de explicações para a garantia de q a partir de q' por a em eob*, $G_{eob}^{q' \xrightarrow{a} q}$, define-se do seguinte modo:

$$G_{eob}^{q' \xrightarrow{a} q} = G_{RActv} \cup G_{Obs}$$

onde G_{RActv} é a *componente de* $G_{eob}^{q' \xrightarrow{a} q}$ *induzida pelas restrições de activação em eob* e G_{Obs} é a *componente de* $G_{eob}^{q' \xrightarrow{a} q}$ *induzida pela observação* as quais se definem como se segue sendo $AxS \cap S_{\Sigma}^{a} = \{\mathbf{G}((\nabla a \wedge \alpha_{p_1 \ldots p_n}^{o_1 \ldots o_n}) \Rightarrow (\mathbf{X}\, \alpha))\}$

- G_{RActv} define-se indutivamente do seguinte modo
  - $cnd(AxF \cap RActv1_{\Sigma}^{a}) \subseteq G_{RActv}$,
  - se $q_1, \ldots, q_m \in G_{RActv}$, $m \geq 1$, e existem $a' \in Acc$ e $f_1' \ldots f_{m'}' \in Enm(AxF \cap RActv2_{\Sigma}^{a'})$, $m' \geq 1$, tal que a fórmula $(q_1 \wedge \ldots \wedge q_m) \Rightarrow (cnd(f_1') \vee \ldots \vee cnd(f_{m'}'))$ é válida então $cnd(AxF \cap RActv1_{\Sigma}^{a'}) \subseteq G_{RActv}$;
- $G_{Obs} = \{q', \neg q_{p_1 \ldots p_n}^{o_1 \ldots o_n}\}$. ■

Exemplo 3.15 Considere-se a especificação de objecto eob_1 do Exemplo 3.3. O conjunto de constrangimentos de estado geradores de explicações para a preservação de $x \vee y$ por a_1 em eob_1 é

$$G_{eob_1}^{x \vee y \xrightarrow{a_1} x \vee y} = \{x \vee y, \neg(x \vee y)\,{}_{\neg z}^{x}\,{}_{x}^{y}\,{}_{\neg z}^{z}\} = \{x \vee y, \neg((\neg z) \vee x)\}.$$

A componente de $G_{eob_1}^{x \vee y \xrightarrow{a_1} x \vee y}$ induzida pelas restrições de activação é $G_{RActv} = \emptyset$ e a componente induzida pela observação é $G_{Obs} = G_{eob_1}^{x \vee y \xrightarrow{a_1} x \vee y}$. ■

Exemplo 3.16 Considere-se a especificação de objecto eob_2 do Exemplo 3.9. O conjunto de constrangimentos de estado geradores de explicações para a garantia de $x \wedge y$ a partir de y por a_1 em eob_2 é

$$G_{eob_2}^{y \xrightarrow{a_1} x \wedge y} = \{u, y, z, \neg(x \wedge y)\,{}_{z}^{x}\,{}_{x}^{y}\,{}_{\neg z}^{z}\} = \{u, z, y, \neg(z \wedge x)\}.$$

A componente de $G_{eob_2}^{y \xrightarrow{a_1} x \wedge y}$ induzida pelas restrições de activação é $G_{RActv} = \{u, z\}$ e a componente induzida pela observação é $G_{Obs} = \{y, \neg(z \wedge x)\}$. ■

Note-se que pela Observação 2.25, $AxS \cap S_{\Sigma}^{a}$ é sempre um conjunto singular. A componente G_{RActv} de $G_{eob}^{q' \xrightarrow{a} q}$ é um subconjunto de $cnd(AxF \cap RActv1_{\Sigma})$ e portanto é um conjunto finito.

Tal como pretendido, a incoerência do conjunto $G_{eob}^{q' \xrightarrow{a} q}$ assegura a garantia de q a partir de q' pela acção a em eob.

Proposição 3.17 Se $G_{eob}^{q' \xrightarrow{a} q}$ é impossível então a garante q a partir de q' em eob.

Prova: Sejam λ modelo de eob e $k \in I\!N_0$ tal que $\lambda, k \models \nabla a \wedge q'$. Seja $G_{eob}^{q' \xrightarrow{a} q} = G_{RActv} \cup G_{Obs}$ e seja $AxS \cap S_{\Sigma}^{a} = \{\mathbf{G}((\nabla a \wedge \alpha_{p_1 \ldots p_n}^{o_1 \ldots o_n}) \Rightarrow (\mathbf{X}\, \alpha))\}$.

(a) Pelas Definições 2.14 e 2.15, $\lambda, k \models \diamond a$. Pelas Definições 2.19 e 2.22, $\lambda \models AxF \cap RActv_\Sigma$ e $\lambda \models \mathbf{G}((\triangledown a \wedge p^{o_1 \ldots o_n}_{p_1 \ldots p_n}) \Rightarrow (\mathbf{X}\, p))$ para todo $p \in CE^{\mathbf{tf}}_\Sigma$.

(b) Prova-se por indução estrutural que $\lambda, k \models p$ qualquer que seja $p \in G_{RActv}$.

Base: seja $p \in cnd(AxF \cap RActv1^a_\Sigma)$. Dado que $\lambda, k \models \diamond a$ e $\lambda \models AxF \cap RActv_\Sigma$ tem-se que $\lambda, k \models p$.

Passo: seja $p \in cnd(AxF \cap RActv1^{a'}_\Sigma)$ com $a' \in Acc$ e sejam $q_1, \ldots, q_m \in G_{RActv}$ e $f'_1 \ldots f'_{m'} \in Enm(AxF \cap RActv2^{a'}_\Sigma)$, $m' \geq 1$, tal que a fórmula $(q_1 \wedge \ldots \wedge q_m) \Rightarrow (cnd(f'_1) \vee \ldots \vee cnd(f'_{m'}))$ é válida. Por hipótese de indução $\lambda, k \models q_i$ para cada $1 \leq i \leq m$ e portanto $\lambda, k \models cnd(f'_j)$ para algum $1 \leq j \leq m'$. Por (a) $\lambda, k \models cnd(f'_j) \Rightarrow \diamond a'$ e portanto $\lambda, k \models \diamond a'$. Novamente por (a) $\lambda, k \models \diamond a' \Rightarrow p$ e portanto $\lambda, k \models p$.

(c) Dado que $G^{q' \xrightarrow{a} q}_{eob}$ é impossível e que $\lambda, k \models G_{RActv} \cup \{q'\}$ tem-se que $\lambda, k \models q^{o_1 \ldots o_n}_{p_1 \ldots p_n}$ pois, caso contrário, pelo Lema 2.18, a estrutura de interpretação λ' tal que $\lambda'(k') = \lambda(k + k')$ para cada $k' \in \mathbb{N}_0$ seria um modelo de $G^{q' \xrightarrow{a} q}_{eob}$. Assim, $\lambda, k \models \triangledown a \wedge q^{o_1 \ldots o_n}_{p_1 \ldots p_n}$ e, por (a), $\lambda, k \models \mathbf{X}\, q$. Pela Definição 2.22, $eob \models \mathbf{G}((\triangledown a \wedge q') \Rightarrow (\mathbf{X}\, q))$. ∎

Das propriedades dos tableaux proposicionais referidas na subsecção 2.5.2 resulta que a existência de um tableaux proposicional fechado para $G^{q' \xrightarrow{a} q}_{eob}$ assegura que a garante q a partir de q' em eob.

Proposição 3.18 Se existe $t \in T_\Sigma(G^{q' \xrightarrow{a} q}_{eob})$ fechado então a garante q a partir de q' em eob.

Prova: Pelas Proposições 2.41 e 3.17. ∎

3.3.3 Geração de explicações

Nesta subsecção descreve-se o modo como se podem gerar restrições de activação que constituem potenciais explicações para a garantia de q a partir de q' por a em eob. A construção de tais explicações baseia-se na análise dos ramos abertos de um qualquer tableau de decisão em $T_\Sigma(G^{q' \xrightarrow{a} q}_{eob})$.

3.3.3.1 Fecho de tableau

Seja $C \subseteq CE^{\mathbf{tf}}_\Sigma$. Resulta da Proposição 2.41 que se existe $t \in T_\Sigma(C)$ tableau de decisão aberto então C é coerente. Com a noção de fecho de t pretende-se caracterizar um conjunto de fórmulas Fc de modo que $C \cup Fc$ seja incoerente. Naturalmente que uma forma trivial de o fazer é considerar um conjunto Fc que inclua $\mathbf{f}$ ou $\neg\mathbf{t}$ ou inclua um par de fórmulas tal que uma seja a negação da outra. Mas, de acordo com o fim em vista, ou seja, para construir potenciais explicações, não são estes fechos triviais que mais interessa considerar. O que se pretende obter são conjuntos de literais de estado (que não contenham pares de literais conjugados) que caracterizem as situações em que a ocorrência da acção não comprometa a garantia desejada. Dado que, novamente pela Proposição 2.41, se um tableau para C é fechado então C é incoerente, tais conjuntos podem ser obtidos a partir dos conjugados dos literais de estado presentes na etiqueta de cada ramo aberto de t. Estes conjuntos dizem-se fechos de t na medida em que são constituídos por fórmulas que permitem tornar fechado cada um dos ramos abertos de t e, consequentemente, transformar t num tableau fechado.

No que se segue assume-se fixado $C \subseteq CE_\Sigma^{\mathbf{tf}}$ finito.

Definição 3.19 Seja $t \in T_\Sigma(C)$ tableau de decisão aberto com função etiqueta e:

- sendo $\rho \in RAbt(t)$, designa-se por *fecho de* ρ o conjunto $Fc^\rho = \overline{e_\mathbf{1}(\rho) \cap LE_\Sigma}$;
- designa-se por *fecho de* t qualquer conjunto $Fc \subseteq \bigcup_{\rho \in RAbt(t)} Fc^\rho$ tal que
  - $Fc \cap \overline{Fc} = \emptyset$,
  - para cada $\rho \in RAbt(t)$ existe $l \in Fc^\rho$ tal que $l \in Fc$. ∎

Exemplo 3.20 Seja $Atr = \{x, y, z, u\}$ o conjunto dos atributos da assinatura de objecto Σ. Considere-se o conjunto de constrangimentos de estado $C = \{y \Rightarrow (z \vee u), \neg(\mathbf{t} \Rightarrow (\mathbf{f} \vee z))\}$ e o tableau de decisão $t \in T_\Sigma(C)$ representado na Figura 3.1.

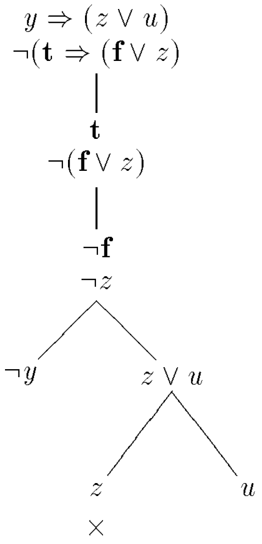

Figura 3.1: Tableau de decisão para o conjunto C

Sendo ρ_1 e ρ_2 os dois ramos abertos de t tem-se que o fecho de ρ_1 é $Fc^{\rho_1} = \{y, z\}$ e o fecho de ρ_2 é $Fc^{\rho_2} = \{z, \neg u\}$. Os conjuntos $Fc_1 = \{z\}$, $Fc_2 = \{y, \neg u\}$, $Fc_3 = \{z, y\}$, $Fc_4 = \{z, \neg u\}$ e $Fc_5 = \{y, z, \neg u\}$ são fechos de t. ∎

Proposição 3.21 Se $t \in T_\Sigma(C)$ é tableau de decisão aberto e Fc é fecho de t então $C \cup Fc$ é impossível.

Prova: Seja $t = ((N, \leq), e)$. Considere-se $t' = ((N, \leq), e') \in T_\Sigma(C \cup Fc)$ onde, sendo ν_t o nó raiz de t, $e'(n) = e(n)$ para todo $n \in N \backslash \{\nu_t\}$, $e'_\mathbf{1}(\nu_t) = e_\mathbf{1}(\nu_t) \cup Fc = C \cup Fc$ e $e'_\mathbf{2}(\nu_t) = e_\mathbf{2}(\nu_t)$. Tem-se que $Rm(t) = Rm(t')$ e que se $\rho \in RFch(t)$ então $\rho \in RFch(t')$. Seja $\rho \in RAbt(t)$ qualquer, Fc^ρ o seu fecho e $l \in Fc^\rho \cap Fc$. Então $\overline{l} \in e_\mathbf{1}(\rho)$ e, dado que $e_\mathbf{1}(\rho) \subseteq e'_\mathbf{1}(\rho)$ e

$l \in e'_{\mathbf{1}}(\nu_t) \subseteq e'_{\mathbf{1}}(\rho)$, tem-se que $\rho \in RFch(t')$. Assim, t é tableau fechado e portanto, pela Proposição 2.41, $C \cup Fc$ é impossível. ∎

Existem situações em que, segundo a Definição 3.19, não existem fechos para um dado tableau de decisão aberto para C. Estas situações correspondem a dois casos. Uma primeira hipótese é que os únicos literais de algum ramo aberto do tableau sejam **t** ou $\neg$**f**. A outra hipótese é a seguinte: todo o conjunto $Fc \subseteq \bigcup_{\rho \in RAbt(t)} Fc^{\rho}$ cuja intersecção com o fecho de cada um dos ramos abertos é não vazia contém dois literais conjugados. Em ambos os casos tal significa que qualquer estrutura de interpretação sobre Σ é modelo de C.

Proposição 3.22 Seja $t \in T_{\Sigma}(C)$ tableau de decisão aberto. Se não existem fechos de t então qualquer estrutura de interpretação sobre Σ é modelo de C.

Prova: Sejam $t = ((N, \leq), e)$ e λ estrutura de interpretação sobre Σ. Se não existem fechos de t verifica-se algumas das condições seguintes: (a) existe $\rho \in RAbt(t)$ tal que $e_{\mathbf{1}}(\rho) \cap LE_{\Sigma} = \emptyset$; (b) $e_{\mathbf{1}}(\rho) \cap LE_{\Sigma} \neq \emptyset$ para cada $\rho \in RAbt(t)$ e $Fc \cap \overline{Fc} \neq \emptyset$ qualquer que seja $Fc \subseteq \bigcup_{\rho \in RAbt(t)} Fc^{\rho}$ tal que para cada $\rho \in RAbt(t)$ existe $l \in Fc^{\rho}$ tal que $l \in Fc$.

(a) Pela Definição 2.15, qualquer estrutura de interpretação sobre Σ é modelo de $\emptyset$. Como $\rho \in RAbt(t)$ então $\rho \in REsg(t) \backslash RFch(t)$. Assim, pela Proposição 2.37 (2), tem-se que $\lambda \models e_{\mathbf{1}}(\rho)$ e portanto $\lambda \models C$ pois $C \subseteq e_{\mathbf{1}}(\rho)$.

(b) Suponha-se, por absurdo, que $\lambda \not\models C$.

(b.i) Se $\rho \in RAbt(t)$, novamente porque $\rho \in REsg(t) \backslash RFch(t)$ e pela Proposição 2.37 (2), tem-se que $\lambda \not\models e_{\mathbf{1}}(\rho) \cap LE_{\Sigma}$.

(b.ii) Seja $\rho_1 \dots \rho_n \in Enm(RAbt(t))$. Para cada $1 \leq i \leq n$ seja $l_i \in e_{\mathbf{1}}(\rho_i) \cap LE_{\Sigma}$ tal que $\lambda \not\models l_i$ (a existência de tal literal é garantida por (b.i)). Sendo $Fc_{\lambda} = \{\overline{l_1}, \dots, \overline{l_n}\}$, tem-se que $Fc_{\lambda} \subseteq \bigcup_{\rho \in RAbt(t)} Fc^{\rho}$ e para cada $\rho \in RAbt(t)$ existe $l \in Fc^{\rho}$ tal que $l \in Fc_{\lambda}$. Da hipótese resulta que $Fc_{\lambda} \cap \overline{Fc_{\lambda}} \neq \emptyset$. Sejam $1 \leq i, j \leq n$ tal que $\overline{l_i} \in Fc_{\lambda}$, $\overline{\overline{l_j}} = l_j \in \overline{Fc_{\lambda}}$ e $\overline{l_i} = l_j$. Uma vez que, pela definição de Fc_{λ}, $\lambda \not\models l_j$, então $\lambda \not\models \overline{l_i}$ e consequentemente $\lambda \models l_i$. Chega-se a uma contradição porque, pela definição de Fc_{λ}, $\lambda \not\models l_i$. Conclui-se assim que $\lambda \models C$. ∎

Dado que é a partir dos fechos de tableaux de decisão que se pretende construir as explicações, uma questão que se coloca é a de saber se tais fechos dependem ou não do tableau de decisão que se analisa. A resposta a esta questão, como se mostra seguidamente, é que é indiferente qual é o tableau de decisão que se considera. A Proposição 3.23 garante que se encontra o mesmo conjunto de fechos qualquer que seja o tableau de decisão para C que se construa.

Proposição 3.23 Sejam $t, t' \in T_{\Sigma}(C)$ tableaux de decisão abertos. O conjunto de todos os fechos de t é igual ao conjunto de todos os fechos de t'.

Prova: Sejam e e e' as funções etiqueta de t e t', respectivamente. Pela Proposição 2.54, $\{Fc^{\rho} : \rho \in RAbt(t)\} = \{Fc^{\rho'} : \rho' \in RAbt(t')\}$. Seja Fc fecho de t. Então, em particular,

$Fc \subseteq \bigcup_{\rho \in RAbt(t)} Fc^{\rho} = \bigcup_{\rho' \in RAbt(t')} Fc^{\rho'}$ e $Fc \cap \overline{Fc} = \emptyset$. Seja $\rho' \in RAbt(t')$. Existe então $\rho \in RAbt(t)$ tal que $Fc^{\rho} = Fc^{\rho'}$ e portanto existe $l \in Fc^{\rho} = Fc^{\rho'}$ tal que $l \in Fc$. Conclui-se assim que Fc é fecho de t'. A prova de que se Fc é fecho de t' então Fc é fecho de t é igual. ■

Definição 3.24 O *conjunto dos fechos sobre* $T_{\Sigma}(C)$, $Fc(C)$, é o conjunto de todos os fechos de um qualquer tableau de decisão aberto em $T_{\Sigma}(C)$. ■

Note-se que a Definição 3.24 é uma boa definição devido à Proposição 3.23.

Exemplo 3.25 Recorde-se Exemplo 3.20. O conjunto dos fechos sobre $T_{\Sigma}(C)$ é o conjunto $Fc(C) = \{Fc_1, Fc_2, Fc_3, Fc_4, Fc_5\}$. ■

Para a geração de explicações a partir de fechos de tableau será ainda útil a noção de fecho minimal num conjunto de fechos. Esta noção vai estar relacionada com noção de explicação mais liberal.

Definição 3.26 Seja $F \subseteq Fc(C)$. O conjunto Fc diz-se *fecho minimal em* F sse

- $Fc \in F$;
- não existe $Fc' \in F$ tal que $Fc' \subset Fc$.

O *conjunto dos fechos minimais em* F denota-se por $min(F)$. ■

Exemplo 3.27 Recorde-se o Exemplo 3.25. O conjunto dos fechos minimais em $Fc(C)$ é o conjunto $min(Fc(C)) = \{Fc_1, Fc_2\}$. ■

Dado que existe apenas um número finito de fechos o conjunto $min(F)$ é sempre não vazio qualquer que seja $F \subseteq Fc(C)$.

3.3.3.2 Geração de explicações a partir de fechos de tableau

Descreve-se agora a forma como a partir dos fechos sobre $T_{\Sigma}(G_{eob}^{q' \xrightarrow{a} q})$ se podem encontrar restrições de activação que constituem potenciais explicações para a garantia de q a partir de q' por a em eob.

Definição 3.28 Seja $L \subseteq \wp(LE_{\Sigma}) \backslash \{\emptyset\}$ não vazio. A restrição de activação $\mathbf{G}(\diamond a \Rightarrow p)$ diz-se *induzida por* L sse existem $L_1 \ldots L_n \in Enm(L)$ e $l_{i1} \ldots l_{im_i} \in Enm(L_i)$ para cada $1 \leq i \leq n$ tal que $p = p_1 \vee \ldots \vee p_n$ com $p_i = l_{i1} \wedge \ldots \wedge l_{im_i}$ para cada $1 \leq i \leq n$. ■

Notação 3.29 No seguimento

- o conjunto dos fechos sobre $T_{\Sigma}(G_{eob}^{q' \xrightarrow{a} q})$, $Fc(G_{eob}^{q' \xrightarrow{a} q})$, é denotado por $Fc_{eob}^{q' \xrightarrow{a} q}$;
- dir-se-á simplesmente que uma restrição de activação é induzida por L_1 sempre que ela seja induzida por um conjunto singular $L = \{L_1\} \subseteq \wp(LE_{\Sigma}) \backslash \{\emptyset\}$. ■

As restrições de activação induzidas por subconjuntos de $Fc_{eob}^{q' \xrightarrow{a} q}$ são candidatas a explicações para a garantia de q a partir de q' através de a em eob.

Proposição 3.30 Seja $F \subseteq Fc_{eob}^{q' \xrightarrow{a} q}$ não vazio. Se f é uma restrição de activação induzida por F e f é eob-possível então f é uma explicação para a garantia de q a partir de q' por a em eob.

Prova: Seja eob' o enriquecimento de eob com $\{f\}$.

(a) O primeiro requisito da Definição 3.7 é satisfeito pelas Definições 3.19 e 3.28.

(b) Pela Definição 3.14, se $\lambda \models G_{eob'}^{q' \xrightarrow{a} q}$ então $\lambda \models G_{eob}^{q' \xrightarrow{a} q} \cup \{cnd(f)\}$ qualquer que seja a estrutura de interpretação λ sobre Σ. Pela Proposição 3.21, $G_{eob}^{q' \xrightarrow{a} q} \cup Fc$ é impossível qualquer que seja $Fc \in F$. Pelas Definições 2.15, 2.16 e 3.28, $G_{eob}^{q' \xrightarrow{a} q} \cup \{cnd(f)\}$ é impossível e consequentemente $G_{eob'}^{q' \xrightarrow{a} q}$ é impossível. Pela Proposição 3.17, a garante q a partir de q' em eob'.

(c) Dado que por hipótese f é eob-possível, pelas Definições 2.22 e 2.23, tem-se que eob' é coerente. ∎

Exemplo 3.31 O tableau t representado na Figura 3.2 é um tableau de decisão em $T_{\Sigma_1}(G_{eob_1}^{x \vee y \xrightarrow{a_1} x \vee y})$ sendo $G_{eob_1}^{x \vee y \xrightarrow{a_1} x \vee y}$ o conjunto construído no Exemplo 3.15.

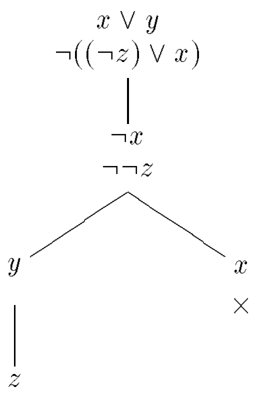

Figura 3.2: Tableau de decisão para $\{x \vee y, \neg((\neg z) \vee x)\}$

O fecho do único ramo aberto do tableau é $\{x, \neg y, \neg z\}$ e consequentemente os conjuntos $Fc_1 = \{x\}$, $Fc_2 = \{\neg y\}$ e $Fc_3 = \{\neg z\}$ são exemplos de elementos de $Fc_{eob_1}^{x \vee y \xrightarrow{a_1} x \vee y}$. As restrições de activação f_1, f_2, f_3 e f_4 apresentadas no Exemplo 3.8 são induzidas por Fc_1, Fc_2, Fc_3 e $\{Fc_1, Fc_2, Fc_3\}$, respectivamente. ∎

Exemplo 3.32 O tableau t representado na Figura 3.3 é um tableau de decisão em $T_{\Sigma_2}(G_{eob_2}^{y \xrightarrow{a_1} x \wedge y})$ sendo $G_{eob_2}^{y \xrightarrow{a_1} x \wedge y}$ é o conjunto construído no Exemplo 3.16.

O fecho do único ramo aberto do tableau é $\{x, \neg y, \neg z, \neg u\}$ e consequentemente os conjuntos $Fc_1 = \{x\}$, $Fc_2 = \{\neg y\}$, $Fc_3 = \{\neg u\}$ e $Fc_4 = \{\neg z\}$ são exemplos de elementos de

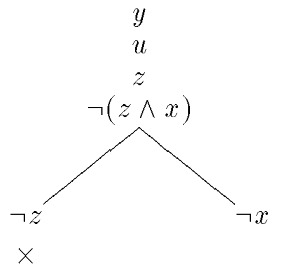

Figura 3.3: Tableau de decisão para $\{y, u, z\neg(z \wedge x)\}$

$Fc^{y \xrightarrow{a_1} x\wedge y}_{eob_2}$. As restrições de activação f_1, f_2, f_3, f_4 e f_5 apresentadas no Exemplo 3.9 são induzidas por Fc_1, Fc_2, Fc_3, Fc_4 e $\{Fc_1, Fc_2\}$, respectivamente. ∎

Em certos casos podem não existir fechos para os tableaux de decisão abertos em $T_\Sigma(G^{q' \xrightarrow{a} q}_{eob})$. Quando isso acontece então a garante $\neg q$ em eob o que significa que a única forma de obter a garantia pretendida é proibir a ocorrência de a. Uma potencial explicação é a restrição de activação $\mathbf{G}(\diamond a \Rightarrow \mathbf{f})$.

Proposição 3.33 Se existem tableaux de decisão abertos em $T_\Sigma(G^{q' \xrightarrow{a} q}_{eob})$ e $Fc^{q' \xrightarrow{a} q}_{eob} = \emptyset$ então a garante $\neg q$ em eob.

Prova: Sejam λ um modelo de eob e $k \in \mathbb{N}_0$ tal que $\lambda, k \models \triangledown a$. Pela Observação 2.25, existe $\mathbf{G}((\triangledown a \wedge \alpha^{o_1 \ldots o_n}_{p_1 \ldots p_n}) \Rightarrow (\mathbf{X}\, \alpha)) \in AxS$ com $n \geq 0$. A função $\lambda' : \mathbb{N}_0 \to \wp(\triangledown Acc \cup \diamond Acc \cup Atr)$ tal que $\lambda'(k') = \lambda(k + k')$ para cada $k' \in \mathbb{N}_0$ é uma estrutura de interpretação sobre Σ. Pela Definição 3.24 e Proposição 3.22, λ' é modelo de $G^{q' \xrightarrow{a} q}_{eob}$. Pela Definição 3.14, $\lambda', 0 \models \neg q^{o_1 \ldots o_n}_{p_1 \ldots p_n}$. Pelo Lema 2.12, $\lambda', 0 \models (\neg q)^{o_1 \ldots o_n}_{p_1 \ldots p_n}$. Pelo Lema 2.18, $\lambda, k \models (\neg q)^{o_1 \ldots o_n}_{p_1 \ldots p_n}$. Pela Definição 2.22, $\lambda, k \models (\triangledown a \wedge (\neg q)^{o_1 \ldots o_n}_{p_1 \ldots p_n}) \Rightarrow (\mathbf{X}(\neg q))$. Assim, $\lambda, k \models \mathbf{X}(\neg q)$ e portanto, pela Definição 3.6, a garante $\neg q$ em eob. ∎

Nem todas as restrições de activação induzidas da forma que tem vindo a ser descrita constituirão explicações para a garantia de q a partir de q' por a em eob. Para que tal aconteça é necessário assegurar que o enriquecimento de eob com a restrição de activação é uma especificação coerente.

Sendo F um subconjunto não vazio de $Fc^{q' \xrightarrow{a} q}_{eob}$, o conjunto de explicações induzidas por F é constituído por todas as restrições de activação que sejam induzidas por subconjuntos não vazios de F e que sejam eob-possíveis. Testar se uma dada restrição de activação f é eob-possível significa testar a coerência da especificação eob' que se obtém enriquecendo eob com $\{f\}$. Como foi referido no Capítulo 2, o teste à coerência de eob' pode ser feito usando tableaux temporais.

Definição 3.34 Seja $F \subseteq Fc^{q' \xrightarrow{a} q}_{eob}$. O *conjunto das explicações para a garantia de q a partir de q' por a em eob induzido por F* denota-se por

$$E_{RActv}(F)$$

e é tal que $f \in E_{RActv}(F)$ sse f é *eob*-possível e f é uma restrição de activação induzida por $F' \subseteq F$ não vazio. ∎

Proposição 3.35 Seja $F \subseteq Fc_{eob}^{q' \xrightarrow{a} q}$. Se $f \in E_{RActv}(F)$ então f é uma explicação para a garantia de q a partir de q' por a em *eob*.

Prova: Pela Proposição 3.30. ∎

Exemplo 3.36 Todas as restrições de activação referidas nos Exemplos 3.31 e 3.32 são explicações em $E_{RActv}(Fc_{eob_1}^{x \vee y \xrightarrow{a_1} x \vee y})$ e em $E_{RActv}(Fc_{eob_2}^{y \xrightarrow{a_1} x \wedge y})$, respectivamente. ∎

As explicações que menos restringem a ocorrência de a, as explicações mais liberais, são obtidas a partir de fechos minimais.

Proposição 3.37 Sejam $F \subseteq Fc_{eob}^{q' \xrightarrow{a} q}$ e $f \in E_{RActv}(F)$.

1. Se f é induzida por $Fc \in min(F)$ então não existe $f' \in E_{RActv}(F)$ que seja induzida por um fecho $Fc' \in F$ e seja estritamente mais liberal que f e se $min(F)$ é um conjunto singular então f é mais liberal que qualquer $f' \in E_{RActv}(F)$ que seja induzida por um fecho $Fc' \in F$.

2. Se f é induzida por $min(F)$ então não existe $f' \in E_{RActv}(F)$ estritamente mais liberal que f.

Prova: (1) Seja f' uma restrição de activação induzida por $Fc' \in F$. Tendo em conta as Definições 3.19 e 3.28, $cnd(f) = l_1 \wedge \ldots \wedge l_n$ e $cnd(f') = l'_1 \wedge \ldots \wedge l'_{n'}$ com $n, n' \geq 1$, $Fc = \{l_1, \ldots, l_n\} \subseteq LE_\Sigma$, $Fc' = \{l'_1, \ldots, l'_{n'}\} \subseteq LE_\Sigma$ e, em particular, $Fc \cap \overline{Fc} = \emptyset$.

(1.a) Suponha-se que $Fc' \not\subseteq Fc$. Existe $1 \leq j \leq n'$ tal que $l'_j \notin Fc$. Se $l'_j \in LE_\Sigma^+$, dado que $Fc \cap \overline{Fc} = \emptyset$, a estrutura de interpretação λ sobre Σ tal que $\lambda(k) = \{\nabla a, \diamond a\} \cup (Fc \cap LE_\Sigma^+)$ para todo $k \in I\!N_0$ é tal que $\lambda, 0 \models cnd(f)$ mas $\lambda, 0 \not\models cnd(f')$. Se $l'_j \in LE_\Sigma^-$, por um argumento idêntico, a estrutura de interpretação λ sobre Σ tal que $\lambda(k) = \{\nabla a, \diamond a, \overline{l'_j}\} \cup (Fc \cap LE_\Sigma^+)$ para todo $k \in I\!N_0$ é tal que $\lambda, 0 \models cnd(f)$ mas $\lambda, 0 \not\models cnd(f')$. Conclui-se então que $cnd(f) \Rightarrow cnd(f')$ não é válida e portanto f' não é estritamente mais liberal que f.

Suponha-se que $Fc' \subseteq Fc$. Se $Fc' \subset Fc$ então $Fc \notin min(F)$ o que contradiz a hipótese. Logo $Fc' = Fc$ e portanto $cnd(f') \Rightarrow cnd(f)$ é válida o que significa que f' não é estritamente mais liberal que f.

Dos dois parágrafos anteriores resulta que f' não é estritamente mais liberal que f.

(1.b) Se $min(F) = \{Fc\}$ então $Fc \subseteq Fc'$ qualquer que seja $Fc' \in F$. Consequentemente, sendo f' induzida por $Fc' \in F$, tem-se que $cnd(f') \Rightarrow cnd(f)$ é válida e portanto f é mais liberal que f'.

(2) Se $f' \in E_{RActv}(F)$, f' é induzida por $F' \subseteq F$ não vazio. Sendo $cnd(f) = p_1 \vee \ldots \vee p_n$ com $p_i = l_{i1} \wedge \ldots \wedge l_{im_i}$ para cada $1 \leq i \leq n$, tem-se que $min(F) = \{Fc_1, \ldots, Fc_n\}$ e $Fc_i = \{l_{i1}, \ldots, l_{im_i}\}$ para cada $1 \leq i \leq n$ e, sendo $cnd(f') = p'_1 \vee \ldots \vee p'_{n'}$ com $p'_j = l'_{j1} \wedge \ldots \wedge l'_{jm'_j}$

para cada $1 \leq j \leq n'$, tem-se que $F' = \{Fc'_1 \ldots Fc'_{n'}\}$ e $Fc'_j = \{l_{j1}, \ldots, l_{jm'_j}\}$ para cada $1 \leq j \leq n'$.

Para cada $1 \leq j \leq n'$ existe $1 \leq i_j \leq n$ tal que $Fc_{i_j} \subseteq Fc'_j$ uma vez que $min(\{A \in F : A \subseteq Fc'_j\} \subseteq min(F)$. Sendo λ uma estrutura de interpretação sobre Σ tal que $\lambda, 0 \models cnd(f')$ tem-se que $\lambda, 0 \models Fc'_j$ para algum $1 \leq j \leq n'$. Então $\lambda, 0 \models Fc_{i_j}$ e portanto $\lambda, 0 \models cnd(f)$. Conclui-se asim que a fórmula $cnd(f') \Rightarrow cnd(f)$ é válida o que significa que f' não é estritamente mais liberal que f. ∎

Nem todas as possíveis explicações para a garantia de q a partir de q' por a em eob são encontradas através do método proposto. No entanto é possível garantir que, para cada possível explicação f e sob certas condições, o método descrito encontra uma explicação f' mais liberal que f.

Proposição 3.38 Seja eob uma especificação de objecto tal que a não garante q a partir de q' em eob. Seja f uma explicação para a garantia de q a partir de q' por a em eob tal que $cnd(f) \neq \mathbf{f}$. Se $G_{eob}^{q' \xrightarrow{a} q} \cup \{cnd(f)\}$ é impossível então existe $f' \in E_{RActv}(min(Fc_{eob}^{q' \xrightarrow{a} q}))$ tal que f' é mais liberal que f.

Prova: Pela Definição 3.7, tem-se que $cnd(f) = q_1 \vee \ldots \vee q_n$ com $n \geq 1$ e, para cada $1 \leq i \leq n$, $q_i = l_{i1} \wedge \ldots \wedge l_{in_i}$, onde $n_i \geq 1$, $l_{ij} \in LE_\Sigma$ para todo $1 \leq j \leq n_i$ e $l_{ij} \neq \overline{l_{ij'}}$ para quaisquer $1 \leq j, j' \leq n_i$. Tem-se também que o enriquecimento de eob com $\{f\}$, eob', é coerente.

Seja $t = ((N, \leq), e) \in T_\Sigma(G_{eob}^{q' \xrightarrow{a} q})$ tableau de decisão. Pela Proposição 3.18 como a não garante q a partir de q' em eob tem-se que t é tableau aberto.

Sejam $\rho_1 \ldots \rho_r \in Enm(RAbt(t))$ e, para cada $1 \leq k \leq r$, seja n_{ρ_k} a folha de ρ_k. Pela Definição 2.34, $\rho_1, \ldots, \rho_r \in REsg(t)$.

A exposição da prova torna-se mais fácil nos casos em que $n \geq 2$ e $n_i \geq 2$ para todo $1 \leq i \leq n$. Para assegurar esta condição, e sem perda de generalidade, em vez de $cnd(f)$ usa-se a disjunção $p = p_1 \vee \ldots \vee p_m$ onde $m = n + 1$, $p_m = (l_{m1} \wedge l_{m2})$, $l_{m1} = l_{m2} = \mathbf{f}$ e, para cada $1 \leq i < m$, $p_i = q_i \wedge \mathbf{t} = l_{i1} \wedge \ldots \wedge l_{im_i}$ com $m_i = n_i + 1$ e $l_{im_i} = \mathbf{t}$.

Considere-se o tableau de decisão $t' = ((N', \leq'), e')$ para $G_{eob}^{q' \xrightarrow{a} q} \cup \{p_1 \vee \ldots \vee p_m\}$ tal que, sendo ν_t o nó raiz de t:

(i) $N' = N \cup (\bigcup_{1 \leq k \leq r} N_{\rho_k})$ onde $N_{\rho_k} = (\bigcup_{2 \leq i \leq m} \{n_k^i, n_k^{\sigma_i - 1}\}) \cup (\bigcup_{1 \leq i \leq m} (\bigcup_{2 \leq j \leq m_i} \{n_k^{i,j}\}))$ para cada $1 \leq k \leq r$ e σ_i é a sequência $1 \ldots i$ para cada $i \in I\!N$ (assume-se, sem perda de generalidade, que $N_{\rho_k} \cap N = \emptyset$ para todo $1 \leq k \leq r$ e identifica-se n_k^1 com $n_k^{\sigma_1}$ para todo $1 \leq k \leq r$);

(ii) $\leq'$ é o fecho reflexivo e transitivo de $\leq \cup (\bigcup_{1 \leq k \leq r} \leq_{\rho_k})$ onde, para cada $1 \leq k \leq r$, $\leq_{\rho_k} = \{(n_{\rho_k}, n_k^m), (n_{\rho_k}, n_k^{\sigma_{m-1}})\} \cup (\bigcup_{2 \leq i < m} \{(n_k^{\sigma_i}, n_k^i), (n_k^{\sigma_i}, n_k^{\sigma_{i-1}})\}) \cup (\bigcup_{1 \leq i \leq m} \leq_{\rho_k}^i)$ e, para cada $1 \leq i \leq m$, $\leq_{\rho_k}^i = \{(n_k^i, n_k^{i,m_i})\} \cup (\bigcup_{3 \leq j \leq m_i} \{(n_k^{i,j}, n_k^{i,j-1})\})$;

(iii) $e'(n) = e(n)$ para todo $n \in N \backslash \{\nu_t\}$, $e'_{\mathbf{1}}(\nu_t) = G_{eob}^{q' \xrightarrow{a} q} \cup \{p_1 \vee \ldots \vee p_m\}$, e, para cada $1 \leq k \leq r$, $e'_{\mathbf{1}}(n_k^{\sigma_i}) = \{p_1 \vee \ldots \vee p_i\}$ para cada $1 < i < m$, $e'_{\mathbf{1}}(n_k^i) = \{p_i\}$ para cada $1 \leq i \leq m$ e $e'_{\mathbf{1}}(n_k^{i,j}) = \{l_{ij}, l_{i1} \wedge \ldots \wedge l_{ij-1}\}$ para cada $1 \leq i \leq m$ e $2 \leq j \leq m_i$;

(iv) $e'_{\mathbf{2}}(n)=e_{\mathbf{2}}(n)$ para todo $n \in N$ e, para cada $1 \leq k \leq r$, $e'_{\mathbf{2}}(n_k^m)=e'_{\mathbf{2}}(n_k^{\sigma_{m-1}})=(\nu_t, p_1 \vee \ldots \vee p_m)$, $e'_{\mathbf{2}}(n_k^i)=e'_{\mathbf{2}}(n_k^{\sigma_{i-1}})=(n_k^{\sigma_i}, p_1 \vee \ldots \vee p_i)$ para cada $2 \leq i < m$, $e'_{\mathbf{2}}(n_k^{i,m_i})=(n_k^i, p_i)$ para cada $1 \leq i \leq m$ e $e'_{\mathbf{2}}(n_k^{i,j})=(n_k^{i,j+1}, l_{i1} \wedge \ldots \wedge l_{ij})$ para cada $1 \leq i < m$ e $2 \leq j < m_i$.

Dado que $G_{eob}^{q' \xrightarrow{a} q} \cup \{cnd(f)\}$ é impossível tem-se que $G_{eob}^{q' \xrightarrow{a} q} \cup \{p_1 \vee \ldots \vee p_m\}$ é também impossível e portanto, pela Proposição 2.41, t' é fechado.

Pela definição de t' tem-se que para cada $1 \leq k \leq r$ existem m ramos de t', $\rho_k^1, \ldots, \rho_k^m$, tal que $\rho_k^i = \rho_k \cup \{n_k^i\} \cup \{n_k^{\sigma_{i'}} : i \leq i' < m\} \cup \{n_k^{i,j} : 2 \leq j \leq m_i\}$ para cada $1 \leq i \leq m$. Seja $1 \leq k \leq r$ e $1 \leq i \leq m-1$. Uma vez que $\rho_k \in RAbt(t)$ e $\rho_k^i \in RFch(t')$, decorre da definição de t' e do facto de $l_{ij} \neq \overline{l_{ij'}}$ para todo $1 \leq j, j' \leq m_i$ que existe $q_k^i \in CE_\Sigma^{\mathbf{tf}}$ tal que alguma das seguintes condições é satisfeita: (1) $q_k^i \in e'_{\mathbf{1}}(\rho_k)\backslash\{p\}$ e $\neg q_k^i \in e'_{\mathbf{1}}(\rho_k^i \backslash \rho_k)$, (2) $\neg q_k^i \in e'_{\mathbf{1}}(\rho_k)\backslash\{p\}$ e $q_k^i \in e'_{\mathbf{1}}(\rho_k^i \backslash \rho_k)$ e (3) $\neg q_k^i \in e'_{\mathbf{1}}(\rho_k)\backslash\{p\}$ e $q_k^i = p = p_1 \vee \ldots \vee p_m \in e'_{\mathbf{1}}(\nu_t)$.

Suponha-se que se tem (1). Atendendo à definição de t', $\neg q_k^i = l_{ij_k^i} \in LE_\Sigma$ para algum $1 \leq j_k^i < m_i$ e portanto $\overline{l_{ij_k^i}} = q_k^i \in e'_{\mathbf{1}}(\rho_k)\backslash\{p\} = e_{\mathbf{1}}(\rho_k)$.

Suponha-se que se tem (2). Tendo em conta a definição de t' alguma das três condições seguintes é satisfeita: (2.i) $q_k^i = l_{ij_k^i} \in LE_\Sigma$ para algum $1 \leq j_k^i < m_i$ ou (2.ii) $q_k^i = l_{i1} \wedge \ldots \wedge l_{ij'}$ para algum $2 \leq j' \leq m_i$ ou (2.iii) $q_k^i = p_1 \vee \ldots \vee p_{i'}$ para algum $i \leq i' < m$ e $i' \geq 2$.

No caso (2.i) se $l_{ij_k^i} \in LE_\Sigma^+$ então $\overline{l_{ij_k^i}} = \neg q_k^i \in e'_{\mathbf{1}}(\rho_k)\backslash\{p\} = e_{\mathbf{1}}(\rho_k)$; se $l_{ij_k^i} = \neg l' \in LE_\Sigma^-$ então $\neg q_k^i = \neg(\neg l')$ e porque $\rho_k \in REsg(t)$, tem-se que $l' = \overline{l_{ij_k^i}} \in e_{\mathbf{1}}(\rho_k)$.

No caso (2.ii) novamente porque $\rho_k \in REsg(t)$ tem-se que $\neg l_{ij'} \in e_{\mathbf{1}}(\rho_k)$ ou $\neg(l_{i1} \wedge \ldots \wedge l_{ij'-1}) \in e_{\mathbf{1}}(\rho_k)$. No primeiro caso, se $j' = m_i$ então, dado que $\rho_k \in RAbt(t)$, não é possível ter $\neg l_{im_i} = \neg \mathbf{t} \in e_{\mathbf{1}}(\rho_k)$ e portanto necessariamente $\neg(l_{i1} \wedge \ldots \wedge l_{m_i-1}) \in e_{\mathbf{1}}(\rho_k)$. Prova-se por indução no conjunto $J' = \{j' \in I\!N_0 : 2 \leq j' < m_i\}$ que se $j' \in J'$ e $\neg(l_{i1} \wedge \ldots \wedge l_{ij'}) \in e_{\mathbf{1}}(\rho_k)$ então existe $1 \leq j'' \leq j'$ tal que $\neg l_{ij''} \in e_{\mathbf{1}}(\rho_k)$.

Base: Se $j' = 2$, porque $\rho_k \in REsg(t)$ tem-se que $\neg l_{i1} \in e_{\mathbf{1}}(\rho_k)$ ou $\neg l_{i2} \in e_{\mathbf{1}}(\rho_k)$.

Passo: Seja $2 \leq j' < m_i - 1$ e $\neg(l_{i1} \wedge \ldots \wedge l_{ij'+1}) \in e_{\mathbf{1}}(\rho_k)$. Novamente porque $\rho_k \in REsg(t)$ tem-se que $\neg l_{ij'+1} \in e_{\mathbf{1}}(\rho_k)$ ou $\neg(l_{i1} \wedge \ldots \wedge l_{ij'}) \in e_{\mathbf{1}}(\rho_k)$. No primeiro caso o resultado é imediato e no segundo caso o resultado é estabelecido pela hipótese de indução.

Conclui-se assim que existe $1 \leq j_k^i < m_i$ tal que $\neg l_{ij_k^i} \in e_{\mathbf{1}}(\rho_k)$. Raciocinando como em (2.i) conclui-se que existe $\overline{l_{ij_k^i}} \in e_{\mathbf{1}}(\rho_k)$ para algum $1 \leq j_k^i < m_i$.

No caso (2.iii) tem-se que $\neg(p_1 \vee \ldots \vee p_{i'}) \in e_{\mathbf{1}}(\rho_k)$. Prova-se por indução no conjunto $I' = \{i' \in I\!N_0 : i \leq i' < m \text{ e } i' \geq 2\}$ que se $i' \in I'$ e $\neg(p_1 \vee \ldots \vee p_{i'}) \in e_{\mathbf{1}}(\rho_k)$ então $\neg p_{i''} \in e_{\mathbf{1}}(\rho_k)$ para todo $1 \leq i'' \leq i'$.

Base: Se $i' = 2$, porque $\rho_k \in REsg(t)$ tem-se que $\neg p_1 \in e_{\mathbf{1}}(\rho_k)$ e $\neg p_2 \in e_{\mathbf{1}}(\rho_k)$.

Passo: Seja $2 \leq i' < m-1$ e $\neg(p_1 \vee \ldots \vee p_{i'+1}) \in e_{\mathbf{1}}(\rho_k)$. Novamente porque $\rho_k \in REsg(t)$ tem-se que $\neg p_{i'+1} \in e_{\mathbf{1}}(\rho_k)$ e $\neg(p_1 \vee \ldots \vee p_{i'}) \in e_{\mathbf{1}}(\rho_k)$. Pela pela hipótese de indução o resultado fica estabelecido.

Assim, em particular, $\neg p_i \in e_{\mathbf{1}}(\rho_k)$ e portanto, raciocinando como em (ii), conclui-se que existe $\overline{l_{ij_k^i}} = q_k^i \in e_{\mathbf{1}}(\rho_k)$ para algum $1 \leq j_k^i \leq m_i - 1$.

Suponha-se que se tem (3). Chega-se uma vez mais à conclusão que existe $\overline{l_{ij_k^i}} = q_k^i \in e_{\mathbf{1}}(\rho_k)$ para algum $1 \leq j_k^i \leq m_i - 1$ raciocinando como no caso (2.iii) .

Recordando que $n = m - 1$, e $m_i - 1 = n_i$ para todo $1 \leq i \leq n$, resulta dos parágrafos anteriores que para cada $1 \leq k \leq r$ e $1 \leq i \leq n$ existe $1 \leq j_k^i \leq n_i$ tal que $\overline{l_{ij_k^i}} \in \mathbf{e_1}(\rho_k) \cap LE_\Sigma$. Assim, pelas Definições 3.19 e 3.24, $\{l_{1j_k^1}, \ldots, l_{nj_k^n}\} \subseteq Fc^{\rho_k}$ para cada $1 \leq k \leq r$ e $Fc_i = \{l_{ij_1^i}, \ldots, l_{ij_r^i}\} \in Fc_{eob}^{q' \xrightarrow{a} q}$ para cada $1 \leq i \leq n$.

Para cada $1 \leq i \leq n$, seja $Fc'_i \in min(Fc_{eob}^{q' \xrightarrow{a} q})$ tal que $Fc'_i \subseteq Fc_i$ e seja f' uma restrição de activação induzida por $\{Fc'_1, \ldots, Fc'_n\} \subseteq min(Fc_{eob}^{q' \xrightarrow{a} q})$. Pelas Definições 2.15, 2.16 e 3.28, $cnd(f) \Rightarrow cnd(f')$ é válida. Por hipótese f é eob-possível e portanto f' é eob-possível. Pela Definição 3.34, $f' \in E_{RActv}(min(Fc_{eob}^{q' \xrightarrow{a} q}))$. Pela Definição 3.11, f' é mais liberal que f. ■

3.3.4 Alguns critérios de preferência

De todas as explicações que se geram para a garantia de q a partir de q' por a em eob existem algumas que, sob certos aspectos, se poderão considerar melhores que outras. O objectivo desta subsecção é analisar alguns critérios de preferência entre explicações .

Explicações não independentes de q e q'

Recorde-se que o conjunto de constrangimentos de estado gerador de explicações para a garantia de q a partir de q' por a em eob, $G_{eob}^{q' \xrightarrow{a} q}$, é a união de dois conjuntos: G_{RActv} (a componente induzida pelas restrições de activação) e G_{Obs} (a componente induzida pela observação). O primeiro conjunto é obtido exclusivamente a partir dos axiomas de eob e o segundo é construído tendo também em conta as fórmulas q' e q relativas ao problema de garantia que pretende tratar.

Suponha-se que uma dada explicação $f \in E_{RActv}(F)$ é induzida por $Fc \in Fc(G_{RActv})$. Pela Proposição 3.21, $G_{RActv} \cup Fc$ é incoerente e consequentemente $G_{RActv} \cup \{cnd(f)\}$ é incoerente. Sendo eob' o enriquecimento de eob com $\{f\}$, da Definição 3.14 resulta que $G_{RActv} \cup \{cnd(f)\} \subseteq G_{eob'}^{p' \xrightarrow{a} p}$ quaisquer que sejam os constrangimentos de estado $p, p' \in CE_\Sigma^{\mathbf{tf}}$. Assim, $G_{eob'}^{p' \xrightarrow{a} p}$ é incoerente e, portanto, das Proposições 2.41 e 3.18 resulta que a acção a garante p a partir de p' em eob' *quaisquer que sejam* $p, p' \in CE_\Sigma^{\mathbf{tf}}$. Este tipo de restrição de activação é independente da particular garantia que se pretende estabelecer.

Comentários análogos se podem fazer também em relação à restrição de activação $\mathbf{G}(\diamond a \Rightarrow \mathbf{f})$.

Exemplo 3.39 Considere-se a especificação de objecto eob_2 do Exemplo 3.9. Dos Exemplos 3.16 e 3.32 resulta que $\{\neg u\} \in Fc_{eob_2}^{y \xrightarrow{a_1} x \wedge y}$ e $\{\neg u\} \in Fc(G_{RActv})$. Tal como já havia sido referido no Exemplo 3.9, a restrição de activação

$$\mathbf{G}(\diamond a_1 \Rightarrow (\neg u)) \in E_{RActv}(Fc_{eob_2}^{y \xrightarrow{a_1} x \wedge y})$$

contribui para a garantia de $x \wedge y$ a partir de y por a_1 porque impede à partida a ocorrência de a_1: esta restrição de activação assegura que a_1 só pode ocorrer quando $\neg u$ se verifica e da especificação eob_2 decorre que a_1 só pode ocorrer quando u se verifica. Esta restrição de activação é bastante restritiva no que se refere à ocorrência de a_1 e é independente dos constrangimentos de estado envolvidos na garantia que se deseja estabelecer. ■

Os comentários anteriores relativos a fechos em $Fc(G_{RActv})$ permitem também concluir que também não serão muito interessantes as restrições de activação induzidas por subconjuntos de $Fc_{eob}^{q' \xrightarrow{a} q}$ que incluam elementos de $Fc(G_{RActv})$.

Exemplo 3.40 Considere-se uma vez mais a especificação de objecto eob_2 do Exemplo 3.9. O Exemplo 3.32 permite concluir que, em particular,

$$\mathbf{G}(\diamond a_1 \Rightarrow (x \vee (\neg y) \vee (\neg u))) \in E_{RActv}(Fc_{eob_2}^{y \xrightarrow{a_1} x \wedge y}).$$

Esta restrição de activação é estritamente mais liberal que a explicação, $\mathbf{G}(\diamond a_1 \Rightarrow (x \vee (\neg y)))$ já anteriormente referida. No entanto, tendo em conta os comentários feitos no Exemplo 3.39, ela não aumenta o número de situações em que a_1 pode ocorrer. O constrangimento de estado $\neg u$ não é aqui particularmente relevante. ■

Do que ficou exposto resulta que não são muito interessantes as explicações que são independentes dos constrangimentos de estado q e q' envolvidos na garantia que se pretende assegurar. Deste modo, um critério de preferência entre explicações será o de preferir aquelas que não são independentes de q e q'.

O conjunto $Fc(G_{RActv})$ pode ser calculado independentemente do problema de garantia para o qual se pretendem encontrar explicações pois só depende da especificação eob. Pode ser calculado previamente e ser depois utilizado no processo de construção de explicações, no âmbito de eob, para eliminar de $Fc_{eob}^{q' \xrightarrow{a} q}$ este tipo de fechos que conduzem a restrições de activação como as que se descreveram.

Note-se que, tal como já foi anteriormente referido, também as restrições de activação $\mathbf{G}(\diamond a \Rightarrow \mathbf{f})$ são independentes de q e q'.

Explicações mais liberais

Dadas duas quaisquer explicações para a garantia de q a partir de q' em eob, a explicação que fôr *mais liberal* é aquela que menos restringe a ocorrência de a. Assim, se se pretende encontrar explicações que assegurem a garantia desejada restringindo o menos possível a ocorrência de a, de entre várias restrições de activação que se considerem igualmente interessantes, devem ser preferidas restrições de activação mais liberais.

Como ficou provado na Proposição 3.37, sendo $F \subseteq Fc_{eob}^{q' \xrightarrow{a} q}$ e f induzida por $min(F)$ então não existe em $E_{RActv}(F)$ explicação estritamente mais liberal que f.

Exemplo 3.41 Considere-se a especificação de objecto eob_1 do Exemplo 3.3. Do Exemplo 3.31 resulta que $min(Fc_{eob_1}^{x \vee y \xrightarrow{a_1} x \vee y}) = \{\{x\}, \{\neg y\}, \{\neg z\}\}$. A restrição de activação

$$\mathbf{G}(\diamond a_1 \Rightarrow (x \vee (\neg y) \vee (\neg z)))$$

é mais liberal qualquer outra restrição de activação em $E_{RActv}(Fc_{eob_1}^{x \vee y \xrightarrow{a_1} x \vee y})$. ■

Exemplo 3.42 Considere-se a especificação de objecto eob_2 do Exemplo 3.9. Do Exemplo 3.32 resulta que $F = \{\{x\}, \{\neg y\}\} \subseteq Fc_{eob_2}^{y \xrightarrow{a_1} x \wedge y}$. A restrição de activação

$$\mathbf{G}(\diamond a_1 \Rightarrow (x \vee (\neg y)))$$

é mais liberal qualquer outra restrição de activação em $E_{RActv}(F)$. ■

3.4 Geração de explicações para a garantia inicial de um constrangimento de estado

Nesta secção descreve-se o modo de construir novos constrangimentos de estado que assegurem que um dado constrangimento de estado seja verificado no instante inicial, isto é, em $k = 0$.

Esta secção está estruturada à semelhança da secção 3.3. Assim, em primeiro lugar, introduz-se a definição de garantia inicial de um constrangimento de estado no âmbito de uma especificação de objecto e a definição de explicação para a referida garantia. Seguidamente, descreve-se o conjunto de fórmulas a partir do qual se constrói o tableau que se usa para obter explicações e descreve-se o modo como estas se constroem a partir dos ramos abertos daquele. Por fim, discutem-se alguns critérios de preferência entre explicações.

No resto da secção assume-se fixada a especificação de objecto $eob = (\Sigma, AxF, AxS)$ com $\Sigma = (Acc, Atr)$ e assume-se fixada a fórmula $q \in CE^{\mathbf{tf}}_{\Sigma}$.

3.4.1 Explicações

Definição 3.43 Diz-se que existe *garantia inicial de q em eob* sse $eob \models q$. ∎

Definição 3.44 Uma *explicação em eob para a garantia inicial de q* é uma fórmula

$$p = p_1 \vee \ldots \vee p_n \in CE_{\Sigma}$$

onde

- $n \geq 1$ e, para cada $1 \leq i \leq n$, $p_i = l_{i1} \wedge \ldots \wedge l_{im_i}$, $m_i \geq 1$ e $l_{ij} \in LE_{\Sigma}$ para todo $1 \leq j \leq m_i$.

e tal que, sendo eob' o enriquecimento de eob com $\{p\}$,

- existe garantia inicial de q em eob',
- eob' é coerente. ∎

Exemplo 3.45 Considere-se a especificação eob_1 do Exemplo 3.3. O constrangimento de estado x é explicação para a garantia inicial de $x \vee y$ em eob_1. ∎

Exemplo 3.46 Considere-se a especificação de objecto $eob_3 = (\Sigma_3, AxF_3, AxS_3)$ com

$$\Sigma_3 = (\{a_1, a_2, a_3\}, \{x, y, z, u\})$$

$$AxF_3 = \{y\}$$

$$\begin{aligned} AxS_3 = \{&\mathbf{G}((\nabla a_1 \wedge \alpha\,{}^{y\ z\ u}_{\mathbf{f}\ x\ \mathbf{f}}) \Rightarrow (\mathbf{X}\,\alpha)),\\ &\mathbf{G}((\nabla a_2 \wedge \alpha\,{}^{y\ z\ u}_{\mathbf{t}\ \mathbf{f}\ z}) \Rightarrow (\mathbf{X}\,\alpha)),\\ &\mathbf{G}((\nabla a_3 \wedge \alpha\,{}^{x}_{\neg x}) \Rightarrow (\mathbf{X}\,\alpha))\}. \end{aligned}$$

Os constrangimentos de estado

$$p_1 = z \qquad\qquad p_2 = u \qquad\qquad p_3 = z \vee u$$

são explicações para a garantia inicial de $y \Rightarrow (z \vee u)$ em eob_3. ■

Também no âmbito de explicações para a garantia inicial de constrangimentos de estado surge a noção de explicação mais liberal.

Definição 3.47 Sejam p_1 e p_2 explicações para a garantia inicial de q em eob.

- p_1 é *mais liberal* que p_2 sse $p_2 \Rightarrow p_1$ é válida.
- p_1 é *estritamente mais liberal* que p_2 sse p_1 é mais liberal que p_2 mas p_2 não é mais liberal que p_1. ■

Exemplo 3.48 Recorde-se o Exemplo 3.46. A explicação $p_3 = z \vee u$ para a garantia inicial de $y \Rightarrow x \wedge z$ em eob_3 é estritamente mais liberal que as explicações p_1 e p_2. ■

3.4.2 Fórmulas e tableaux geradores de explicações

O objectivo desta subsecção é estabelecer quais as fórmulas resultantes da especificação e do problema de garantia inicial que se usam para construir as explicações. Tal como no caso da garantia de um contrangimento de estado a partir de outro constrangimento de estado através de uma acção, vai ser escolhido um conjunto de constrangimentos de estado cuja incoerência seja condição suficiente para assegurar a garantia inicial de q em eob.

Definição 3.49 O *conjunto de constrangimentos de estado geradores de explicações para a garantia inicial de q em eob*, $G_{eob}^{\overset{ci}{\rightarrow} q}$, define-se do seguinte modo:

$$G_{eob}^{\overset{ci}{\rightarrow} q} = G_{CI} \cup G_{Obs}$$

onde G_{CI} é a *componente de $G_{eob}^{\overset{ci}{\rightarrow} q}$ induzida pelas condições iniciais em eob* e G_{Obs} é a *componente de $G_{eob}^{\overset{ci}{\rightarrow} q}$ induzida pela observação* as quais se definem como se segue

- G_{CI} define-se indutivamente do seguinte modo
  - $AxF \cap CE_\Sigma^{\mathbf{tf}} \subseteq G_{CI}$,
  - se $q_1, \ldots, q_m \in G_{CI}$, $m \geq 1$, e existem $a' \in Acc$ e $f'_1 \ldots f'_{m'} \in Enm(AxF \cap RActv2_\Sigma^{a'})$, $m' \geq 1$, tal que a fórmula $(q_1 \wedge \ldots \wedge q_m) \Rightarrow (cnd(f'_1) \vee \ldots \vee cnd(f'_{m'}))$ é válida então $cnd(AxF \cap RActv1_\Sigma^{a'}) \subseteq G_{CI}$;
- $G_{Obs} = \{\neg q\}$. ■

Exemplo 3.50 Considere-se a especificação eob_1 do Exemplo 3.3. O conjunto de constrangimentos de estado geradores de explicações para a garantia inicial de $x \vee y$ em eob_1 é

$$G_{eob_1}^{\overset{ci}{\rightarrow} x \vee y} = \{\neg y, \neg(x \vee y)\}.$$

A componente de $G^{\overset{ci}{-}x\vee y}_{eob_1}$ induzida pelas condições iniciais é $G_{CI} = \{\neg y\}$ e a componente induzida pela observação é $G_{Obs} = \{\neg(x \vee y)\}$. ∎

Exemplo 3.51 Considere-se a especificação eob_3 do Exemplo 3.46. O conjunto de constrangimentos de estado geradores de explicações para a garantia inicial de $y \Rightarrow (z \vee u)$ em eob_3 é

$$G^{\overset{ci}{-}y\Rightarrow(z\vee u)}_{eob_3} = \{y, \neg(y \Rightarrow (z \vee u))\}.$$

A componente de $G^{\overset{ci}{-}y\Rightarrow(z\vee u)}_{eob_3}$ induzida pelas condições iniciais é $G_{CI} = \{y\}$ e a componente induzida pela observação é $G_{Obs} = \{\neg(y \Rightarrow (z \vee u))\}$. ∎

Tal como pretendido, a incoerência do conjunto $G^{\overset{ci}{-}q}_{eob}$ assegura a garantia inicial de q em eob e, consequentemente, a existência de um tableau fechado para $G^{\overset{ci}{-}q}_{eob}$ assegura a referida garantia.

Proposição 3.52 Se $G^{\overset{ci}{-}q}_{eob}$ é impossível então existe garantia inicial de q em eob.

Prova: Seja λ um modelo de eob e seja $G^{\overset{ci}{-}q}_{eob} = G_{CI} \cup G_{Obs}$ como na Definição 3.49.

(a) Prova-se por indução estrutural que $\lambda \models p$ qualquer que seja $p \in G_{CI}$.

Base: seja $p \in AxF \cap CE^{\mathbf{tf}}_{\Sigma}$. Pela Definição 2.22, $\lambda \models p$.

Passo: seja $p \in cnd(AxF \cap RActv1^{a'}_{\Sigma})$ com $a' \in Acc$ e sejam $q_1, \ldots, q_m \in G_{CI}$ e $f'_1 \ldots f'_{m'} \in Enm(AxF \cap RActv2^{a'}_{\Sigma})$, $m' \geq 1$, tal que a fórmula $(q_1 \wedge \ldots \wedge q_m) \Rightarrow (cnd(f'_1) \vee \ldots \vee cnd(f'_{m'}))$ é válida. Por hipótese de indução $\lambda \models q_i$ para cada $1 \leq i \leq m$ e portanto $\lambda \models cnd(f'_j)$ para algum $1 \leq j \leq m'$. Pelas Definições 2.15, 2.16 e 2.22, $\lambda \models cnd(f'_j) \Rightarrow \diamond a'$ e $\lambda \models \diamond a' \Rightarrow p$ o que permite concluir que $\lambda \models p$.

(b) Dado que $G^{\overset{ci}{-}q}_{eob}$ é impossível então $\lambda \not\models G_{Obs}$, ou seja, $\lambda \models q$. ∎

Proposição 3.53 Se existe $t \in T(G^{\overset{ci}{-}q}_{eob})$ fechado então há garantia inicial de q em eob.

Prova: Pelas Proposições 2.41 e 3.52. ∎

3.4.3 Geração de explicações

O modo como se geram os constrangimentos de estado candidatos a explicações para a garantia inicial de q em eob é análogo ao usado na secção anterior para gerar as restrições de activação candidatas a explicações para garantia de um constrangimento de estado a partir de outro constrangimento de estado através de uma acção a em eob. Os referidos constrangimentos de estado são obtidos, neste caso, a partir de fechos de um tableau de decisão em $T_{\Sigma}(G^{\overset{ci}{-}q}_{eob})$.

Definição 3.54 Seja $L \subseteq \wp(LE_{\Sigma}) \backslash \{\emptyset\}$ não vazio. A condição inicial p diz-se *induzida por* L sse existem $L_1 \ldots L_n \in Enm(L)$ e $l_{i1} \ldots l_{im_i} \in Enm(L_i)$ para cada $1 \leq i \leq n$ tal que $p = p_1 \vee \ldots \vee p_n$ com $p_i = l_{i1} \wedge \ldots \wedge l_{im_i}$ para cada $1 \leq i \leq n$. ∎

Notação 3.55 No seguimento

- o conjunto dos fechos sobre $T_\Sigma(G_{eob}^{\overset{ci}{\rightarrow}q})$, $Fc(G_{eob}^{\overset{ci}{\rightarrow}q})$, é denotado por $Fc_{eob}^{\overset{ci}{\rightarrow}q}$;
- dir-se-á simplesmente que uma condição inicial é induzida por L_1 sempre que ela seja induzida por um conjunto singular $L = \{L_1\} \subseteq \wp(LE_\Sigma) \backslash \{\emptyset\}$. ■

Proposição 3.56 Seja $F \subseteq Fc_{eob}^{\overset{ci}{\rightarrow}q}$ não vazio. Se p é uma condição inicial induzida por F e p é *eob*-possível então p é uma explicação para a garantia de inicial de q em *eob*.

Prova: Seja eob' o enriquecimento de eob com $\{p\}$.

(a) O primeiro requisito da Definição 3.44 é satisfeito pelas Definições 3.19 e 3.54.

(b) Pela Definição 3.49, se $\lambda \models G_{eob'}^{\overset{ci}{\rightarrow}q}$ então $\lambda \models G_{eob}^{\overset{ci}{\rightarrow}q} \cup \{p\}$ qualquer que seja a estrutura de interpretação λ sobre Σ. Pela Proposição 3.21, $G_{eob}^{\overset{ci}{\rightarrow}q} \cup Fc$ é impossível qualquer que seja $Fc \in F$. Tendo em conta as Definições 2.15, 2.16 e 3.54, $G_{eob}^{\overset{ci}{\rightarrow}q} \cup \{p\}$ é impossível e consequentemente $G_{eob'}^{\overset{ci}{\rightarrow}q}$ é impossível. Pela Proposição 3.52, existe garantia inicial de q em *eob*.

(c) Dado que por hipótese p é *eob*-possível, pelas Definições 2.22 e 2.23, tem-se que eob' é coerente. ■

Exemplo 3.57 O tableau t representado na Figura 3.4 é um tableau de decisão em $T_{\Sigma_1}(G_{eob_1}^{\overset{ci}{\rightarrow}x\vee y})$ onde $G_{eob_1}^{\overset{ci}{\rightarrow}x\vee y}$ é o conjunto construído no Exemplo 3.50.

$$\begin{array}{c} \neg y \\ \neg(x \vee y) \\ | \\ \neg x \\ \neg y \end{array}$$

Figura 3.4: Tableau de decisão para $\{\neg y, \neg(x \vee y)\}$

O fecho do único ramo do tableau é $\{x, y\}$ e consequentemente $Fc_1 = \{x\}$ e $Fc_2 = \{y\}$ são exemplos de elementos em $Fc_{eob_1}^{\overset{ci}{\rightarrow}x\vee y}$. O constrangimento de estado x referido no Exemplo 3.45 é induzido por Fc_1. ■

Exemplo 3.58 O tableau t representado no Figura 3.5 é um tableau de decisão em $T_{\Sigma_3}(G_{eob_3}^{\overset{ci}{\rightarrow}y\Rightarrow(z\vee u)})$ sendo $G_{eob_3}^{\overset{ci}{\rightarrow}y\Rightarrow(z\vee u)}$ o conjunto construído no Exemplo 3.51.

O fecho do único ramo aberto é $\{\neg y, z, u\}$ e consequentemente $Fc_1 = \{\neg y\}$, $Fc_2 = \{z\}$ e $Fc_3 = \{u\}$ são exemplos de elementos de $Fc_{eob_3}^{\overset{ci}{\rightarrow}y\Rightarrow(z\vee u)}$. Os constrangimentos de estado $\neg y$, z, u e $z \vee u$ são induzidos por Fc_1, Fc_2, Fc_3 e $\{Fc_2, Fc_3\}$, respectivamente. ■

As situações em que não existem fechos para os tableaux de decisão abertos em $T_\Sigma(G_{eob}^{\overset{ci}{\rightarrow}q})$ correspondem aos casos em que existe garantia inicial de $\neg q$ em *eob*. Contrariamente ao que acontece no caso da garantia de um constrangimento de estado a partir de

$$\neg(y \Rightarrow (z \vee u))$$
$$y$$
$$|$$
$$y$$
$$\neg(z \vee u)$$
$$|$$
$$\neg z$$
$$\neg u$$

Figura 3.5: Tableau de decisão para $\{y, \neg(y \Rightarrow (z \vee u))\}$

outro constrangimento de estado através de uma acção a, não existem neste caso, como é óbvio, explicações para a garantia inicial de q em eob.

Proposição 3.59 Se existem tableaux de decisão abertos em $T_\Sigma(G^{\stackrel{ci}{\to}q}_{eob})$ e $Fc^{\stackrel{ci}{\to}q}_{eob} = \emptyset$ então existe garantia inicial de $\neg q$ em eob.

Prova: Seja λ um modelo de eob. Pela Definição 3.24 e Proposição 3.22, $\lambda \models G^{\stackrel{ci}{\to}q}_{eob}$ e portanto, pelas Definições 3.49 e 3.43 existe garantia inicial de $\neg q$ em eob. ■

De novo se tem que nem todos os constrangimentos de estado induzidos por subconjuntos não vazios de $Fc^{\stackrel{ci}{\to}q}_{eob}$ são explicações para a garantia inicial de q em eob. Para que sejam efectivamente explicações é necessário que o enriquecimento de eob com o constrangimento de estado seja uma especificação coerente.

Definição 3.60 Seja $F \subseteq Fc^{\stackrel{ci}{\to}q}_{eob}$. O *conjunto das explicações para a garantia inicial de q em eob induzido por F* denota-se por

$$E_{CI}(F)$$

e é tal que $p \in E_{CI}(F)$ sse p é uma condição inicial induzida por $F' \subseteq F$ não vazio e p é eob-possível. ■

Proposição 3.61 Seja $F \subseteq Fc^{\stackrel{ci}{\to}q}_{eob}$. Se $p \in E_{CI}(F)$ então p é uma explicação para a garantia inicial de q por a em eob.

Prova: Pela Proposição 3.56. ■

Exemplo 3.62 O constrangimento de estado x referido no Exemplo 3.57 é uma explicação em $E_{CI}(Fc^{\stackrel{ci}{\to}x \vee y}_{eob_1})$.

Os constrangimentos de estado z, u e $z \vee u$ referidos no Exemplo 3.58 são explicações em $E_{CI}(Fc^{\stackrel{ci}{\to}y \Rightarrow (z \vee u)}_{eob_3})$. O constangimento de estado $\neg y$ não pertence a $E_{CI}(Fc^{\stackrel{ci}{\to}y \Rightarrow (z \vee u)}_{eob_3})$ dado que não é eob_3-possível. ■

Contrariamente ao que acontece no caso da garantia de um constrangimento de estado a partir de outro constrangimento de estado através de uma acção a, no caso da garantia inicial de q é possível identificar facilmente vários subconjuntos de $Fc_{eob}^{\overset{ci}{\to}q}$ que não vão induzir elementos de $E_{CI}(Fc_{eob}^{\overset{ci}{\to}q})$, isto é, que não vão induzir condições iniciais eob-possíveis.

Proposição 3.63 Seja $F \subseteq Fc_{eob}^{\overset{ci}{\to}q}$ tal que para todo $Fc \in F$ existe $Fc' \subseteq Fc$ tal que $Fc' \in Fc(G_{CI})$ onde G_{CI} é a componente de $G_{eob}^{\overset{ci}{\to}q}$ induzida pelas condições iniciais. Se p é uma condição inicial induzida por F então $p \notin E(Fc_{eob}^{\overset{ci}{\to}q})$.

Prova: Seja $Fc \in F$ e $Fc' \in Fc(G_{CI})$ tal que $Fc' \subseteq Fc$. Pela Proposição 3.21 e Definição 3.24, $G_{CI} \cup Fc'$ é impossível e portanto $G_{CI} \cup Fc$ é impossível.

Suponha-se, por absurdo, que existe um modelo λ de eob tal que $\lambda \models p$. Tem-se então que $\lambda \models Fc$ para algum $Fc \in F$. Como $\lambda \models G_{CI}$ tem-se que $\lambda \models G_{CI} \cup Fc$ o que contradiz o parágrafo anterior. Assim, nenhum modelo de eob é modelo de p.

Como p não é eob-possível, pela Definição 3.60, $p \notin E(Fc_{eob}^{\overset{ci}{\to}q})$. ∎

Exemplo 3.64 O fecho $Fc_1 = \{\neg y\}$ em $Fc_{eob_3}^{\overset{ci}{\to}y \Rightarrow (z \vee u)}$ referido no Exemplo 3.58 é um fecho em $Fc(G_{CI})$ onde $G_{CI} = \{y\}$ é a componente de $G_{eob_3}^{\overset{ci}{\to}y \Rightarrow (z \vee u)}$ induzida pelas condições iniciais. Tal como já havia sido referido no Exemplo 3.62, o constrangimentode estado $\neg y$ induzido por Fc_1 não é explicação para a garantia inicial de $y \Rightarrow (z \vee u)$ pois não é eob_3-possível. ∎

Também aqui as explicações iniciais mais liberais são obtidas a partir de fechos minimais.

Proposição 3.65 Sejam $F \subseteq Fc_{eob}^{\overset{ci}{\to}q}$ e $p \in E_{CI}(F)$.

1. Se p é induzida por $Fc \in min(F)$ então não existe $p' \in E_{CI}(F)$ que seja induzida por um fecho $Fc' \in F$ e seja estritamente mais liberal que p e se $min(F)$ é um conjunto singular então p é mais liberal que qualquer $p' \in E_{CI}(F)$ que seja induzida por um fecho $Fc' \in F$.

2. Se f é induzida por $min(F)$ então não existe $p' \in E_{CI}(F)$ estritamente mais liberal que p.

Prova: As provas são análogas às apresentadas na prova da Proposição 3.37. ∎

Proposição 3.66 Seja eob tal que não existe garantia inicial de q em eob. Seja p uma explicação para a garantia inicial de q em eob. Se $G_{eob}^{\overset{ci}{\to}q} \cup \{p\}$ é um conjunto impossível então existe $p' \in E_{CI}(min(Fc_{eob}^{\overset{ci}{\to}q}))$ tal que p' é mais liberal que p.

Prova: A prova é análoga à apresentada para a Proposição 3.38. ∎

Para terminar esta secção refira-se que também no caso da garantia inicial q se pode introduzir como critério de preferência entre explicações a noção de explicação (estritamente) mais liberal.

3.5 Geração de explicações para problemas de abdução

Nesta secção descreve-se o modo como se encontram explicações para problemas de abdução em especificações de objectos. Os problemas de abdução considerados são os problemas descritos na secção 3.2, ou seja, problemas de segurança, de garantia, de resposta e de persistência. Em cada uma das subsecções seguintes é tratado um destes tipos de problemas. Como já foi referido anteriormente, os resultados que fundamentam a estratégia utilizada para a construção das explicações são adaptações de técnicas conhecidas na literatura para a verificação de propriedades de segurança e animação/resposta.

Assume-se fixada a especificação de objecto $eob = (\Sigma, AxF, AxS)$ com $\Sigma = (Acc, Atr)$. Assumem-se também fixadas as fórmulas $r, q, q_1, q_2 \in CE^{\mathbf{tf}}_{\Sigma}$.

3.5.1 Problemas de segurança

Nesta subsecção descreve-se o modo como explicações para problemas de segurança em eob podem ser obtidas.

Proposição 3.67 Se $eob \models \mathbf{G}((\nabla a \wedge r) \Rightarrow (\mathbf{X}\, q))$ qualquer que seja $a \in Acc$ então tem-se que $eob \models \mathbf{G}(r \Rightarrow (\mathbf{X}\, q))$.

Prova: Sejam λ um modelo de eob, $k \in I\!N_0$ e suponha-se que $\lambda, k \models r$. Pela Definição 2.14 existe $a \in Acc$ tal que $\lambda, k \models \nabla a$ e portanto $\lambda, k \models \mathbf{X}\, q$. ∎

Proposição 3.68 Se

(i) $eob \models r \Rightarrow (q_1 \vee q_2)$,

(ii) $eob \models \mathbf{G}((q_1 \wedge (\neg q_2)) \Rightarrow (\mathbf{X}(q_1 \vee q_2)))$,

então $eob \models r \Rightarrow (q_1\, \mathbf{W}\, q_2)$.

Prova: Seja λ modelo de eob e suponha-se que $\lambda \models r$. Por (i) $\lambda \models q_1$ ou $\lambda \models q_2$.

Se $\lambda \models q_2$ então $\lambda \models q_1\, \mathbf{W}\, q_2$ e portanto $\lambda \models r \Rightarrow (q_1\, \mathbf{W}\, q_2)$.

Suponha-se $\lambda \models q_1$ e $\lambda \not\models q_2$. Se $\lambda, k \models q_1 \wedge (\neg q_2)$ para todo $k \geq 0$ então, em particular, $\lambda, k \models q_1$ para todo $k \geq 0$ e portanto $\lambda, 0 \models q_1\, \mathbf{W}\, q_2$ e consequentemente $\lambda \models r \Rightarrow (q_1 \mathbf{W} q_2)$. Caso contrário, existe $k' > 0$ tal que $\lambda, k' \not\models q_1 \wedge (\neg q_2)$ e $\lambda, k \models q_1 \wedge (\neg q_2)$ para todo $0 \leq k < k'$. Se $\lambda, k' \not\models \neg q_2$, ou seja, $\lambda, k' \models q_2$ então $\lambda \models q_1\, \mathbf{W}\, q_2$ e portanto $\lambda \models r \Rightarrow (q_1\, \mathbf{W}\, q_2)$. Caso contrário, $\lambda, k' \not\models q_1$ Uma vez que $\lambda, k'-1 \models q_1 \wedge (\neg q_2)$, pela hipótese (ii), $\lambda, k' \models q_2$ e novamente se conclui que $\lambda \models r \Rightarrow (q_1\, \mathbf{W}\, q_2)$.

Dos parágrafos anteriores resulta que $eob \models r \Rightarrow (q_1\, \mathbf{W}\, q_2)$. ∎

Corolário 3.69 Se

(i) $eob \models q$,

(ii) $eob \models \mathbf{G}(q \Rightarrow (\mathbf{X}\, q))$, então $eob \models \mathbf{G}\, q$.

Prova: Pela Proposição 3.68 fazendo $r = \mathbf{t}$, $q_1 = q$ e $q_2 = \mathbf{f}$. ∎

Proposição 3.70 Se

(i) $eob \models \mathbf{G}(r \Rightarrow (q_1 \vee q_2))$,

(ii) $eob \models \mathbf{G}((q_1 \wedge (\neg q_2)) \Rightarrow (\mathbf{X}(q_1 \vee q_2)))$,

então $eob \models \mathbf{G}(r \Rightarrow (q_1\, \mathbf{W}\, q_2))$.

Prova: Sejam λ um modelo de eob e $k \in I\!N_0$. Suponha-se que $\lambda, k \models r$. Pela hipótese (i), $\lambda, k \models r \Rightarrow (q_1 \vee q_2)$ e portanto $\lambda, k \models q_j$ para algum $1 \leq j \leq 2$. O resto da prova é semelhante à prova apresentada para a Proposição 3.68. ∎

As proposições anteriores mostram como se pode concluir que observações de segurança são eob-válidas a partir do conhecimento de que em eob: (i) existe garantia inicial de um certo contrangimento de estado e (ii) existe garantia por cada $a \in Acc$ de determinados constrangimentos de estado a partir de outros constrangimentos de estado. Nas secções 3.3 e 3.4 descreveram-se precisamente métodos para construir explicações para tais garantias os quais podem agora ser utilizados para construir explicações para problemas de segurança.

Definição 3.71 Seja $f = \mathbf{G}(r \Rightarrow (\mathbf{X}\, q)) \in O_\Sigma$. Para cada $a \in Acc$, a fórmula

$$\mathbf{G}((\nabla a \wedge r) \Rightarrow (\mathbf{X}\, q))$$

designa-se por *garantia induzida por f relativamente à acção a* e denota-se por $gr_a(f)$. ∎

Proposição 3.72 Seja $f = \mathbf{G}(r \Rightarrow (\mathbf{X}\, q))$ um problema de segurança em eob. Seja

$$A = \{a \in Acc\colon eob \not\models gr_a(f)\}$$

e, para cada $a \in A$, seja f'_a uma explicação para a garantia de q a partir de r por a em eob. Se

$$E = \bigcup_{a \in A} \{f'_a\}$$

é eob-possível então E é uma explicação para o problema $\mathbf{G}(r \Rightarrow (\mathbf{X}\, q))$ em eob.

Prova: Seja eob' o enriquecimento de eob com E.

(a) Sejam $a \in Acc$ e λ modelo de eob'.

Suponha-se que $a \notin A$. Dado que λ é também modelo de eob, $\lambda \models gr_a(f)$.

Suponha-se que $a \in A$. Sendo eob'' o enriquecimento de eob com $\{f'_a\}$, pela Definição 3.7, $eob'' \models gr_a(f)$ e, dado que λ é também modelo de eob'', tem-se que $\lambda \models gr_a(f)$.

Dos dois parágrafos anteriores resulta que $eob' \models gr_a(f)$ para cada $a \in Acc$.

(b) Por (a) e Proposição 3.67, $eob' \models \mathbf{G}(r \Rightarrow (\mathbf{X}\, q))$.

(c) Pelas Definições 2.22 e 2.23, dado que E é eob-possível, tem-se que eob' é coerente.

(d) Por (b), (c) e Definição 3.4, E é uma explicação para $\mathbf{G}(r \Rightarrow (\mathbf{X}\, q))$. ∎

Exemplo 3.73 Recorde-se a especificação de objecto eob_1 apresentada no Exemplo 3.3. A fórmula $\mathbf{G}((x \vee y) \Rightarrow (\mathbf{X}(x \vee y)))$ é um problema de segurança em eob_1.

Tal como referido no Exemplo 3.36, as restrições de activação

$$f_1 = \mathbf{G}(\diamond a_1 \Rightarrow x) \qquad f_2 = \mathbf{G}(\diamond a_1 \Rightarrow (\neg y)) \qquad f_3 = \mathbf{G}(\diamond a_1 \Rightarrow (\neg z))$$
$$f_4 = \mathbf{G}(\diamond a_1 \Rightarrow (x \vee (\neg y) \vee (\neg z)))$$

são explicações para o problema da preservação de $x \vee y$ por a_1 em eob_1.

Dado que a acção a_2 preserva $x \vee y$ em eob_1, os conjuntos $E_i = \{f_i\}$, $1 \leq i \leq 4$, são explicações para o problema de segurança $\mathbf{G}((x \vee y) \Rightarrow (\mathbf{X}(x \vee y)))$ em eob_1. O conjunto E_4 corresponde à explicação mais liberal. ∎

Para encontrar explicações para problemas de segurança do tipo $r \Rightarrow (q_1 \mathbf{W} q_2)$ há que procurar explicações não só para problemas do tipo $\mathbf{G}(p \Rightarrow (\mathbf{X}\, q))$ mas também para a garantia inicial de certos constrangimentos de estado.

Definição 3.74 Seja $f = r \Rightarrow (q_1 \mathbf{W} q_2) \in O_\Sigma$. Os *subproblemas para a explicação de f* são as fórmulas

- $sp_{CI}(f) = r \Rightarrow (q_1 \vee q_2)$;
- $sp_{seg}(f) = \mathbf{G}((q_1 \wedge (\neg q_2)) \Rightarrow (\mathbf{X}(q_1 \vee q_2)))$.

O conjunto dos subproblemas para a explicação de f é o conjunto constituído pelas fórmulas anteriores e denota-se por $Sp(f)$.

Para cada $a \in Acc$, a fórmula

$$\mathbf{G}((\nabla a \wedge q_1 \wedge (\neg q_2)) \Rightarrow (\mathbf{X}(q_1 \vee q_2)))$$

designa-se por *garantia induzida por f relativamente à acção a* e denota-se por $gr_a(f)$.

No que se segue, dada a especificação de objecto eob, entende-se por *explicação para $sp_{CI}(f)$ em eob* um conjunto $\{f_{CI}\}$ onde f_{CI} seja uma explicação para a garantia inicial de $sp_{CI}(f)$ em eob. ∎

Proposição 3.75 Seja $r \Rightarrow (q_1 \mathbf{W} q_2)$ um problema de segurança em *eob*. Seja

$$X = \{sp \in Sp(r \Rightarrow (q_1 \mathbf{W} q_2)) \colon eob \not\models sp\}$$

e para cada $sp \in X$ seja E_{sp} uma explicação para sp em *eob*. Se

$$E = \bigcup_{sp \in X} E_{sp}$$

é *eob*-possível então E é uma explicação para o problema $r \Rightarrow (q_1 \mathbf{W} q_2)$ em *eob*.

Prova: Sejam eob' o enriquecimento de eob com E e $f = r \Rightarrow (q_1 \mathbf{W} q_2)$.

(a) Tem-se que $eob' \models sp$ para todo $sp \in Sp(f)$ tal que $sp \notin X$.

Seja $sp \in X$. Se $sp = sp_{CI}(f)$ e sendo eob'' o enriquecimento de eob com E_{sp}, pela Definição 3.44, $eob'' \models sp$ e portanto $eob' \models sp$. Se $sp = sp_{seg}(f)$, e sendo eob'' o enriquecimento de eob com E_{sp}, pela Definição 3.4, $eob'' \models sp$ e novamente $eob' \models sp$.

Pela Proposição 3.68, conclui-se que $eob' \models r \Rightarrow (q_1 \,\mathbf{W}\, q_2)$.

(b) Pelas Definições 2.22 e 2.23, dado que E é eob-possível, tem-se que eob' é coerente.

(c) Por (a), (b) E é uma explicação para o problema de segurança $r \Rightarrow (q_1 \,\mathbf{W}\, q_2)$. ∎

Exemplo 3.76 Considere-se a especificação de objecto eob_3 descrita no Exemplo 3.46. A fórmula

$$f = y \Rightarrow (z \,\mathbf{W}\, u)$$

é um problema de segurança em eob_3.

1. Tem-se que $sp_{CI}(f) = y \Rightarrow (z \vee u)$ e $eob_3 \not\models sp_{CI}(f)$. Do Exemplo 3.62 decorre que, em particular, o conjunto

$$\{z \vee u\}$$

é explicação para $sp_{CI}(f)$ em eob_3.

2. Tem-se que $sp_{seg}(f) = \mathbf{G}((z \wedge (\neg u)) \Rightarrow (\mathbf{X}(z \vee u)))$ e $eob_3 \not\models sp_{seg}(f)$.

2.1. A acção a_1 não garante $z \vee u$ a partir de $z \wedge (\neg u)$ em eob_3. O tableau representado na Figura 3.6 é um tableau de decisão em $T_{\Sigma_3}(G_{eob_3}^{z \wedge (\neg u) \xrightarrow{a_1} z \vee u})$.

$$\begin{array}{c} \neg(x \vee \mathbf{f}) \\ z \wedge (\neg u) \\ | \\ \neg x \\ \neg \mathbf{f} \\ | \\ z \\ \neg u \end{array}$$

Figura 3.6: Tableau de decisão para $\{\neg(x \vee \mathbf{f}), z \wedge (\neg u)\}$

A restrição de activação $\mathbf{G}(\diamond a_1 \Rightarrow (x \vee (\neg z) \vee u)) \in E_{RActv}(Fc_{eob_3}^{z \wedge (\neg u) \xrightarrow{a_1} z \vee u})$ e é induzida por $min(Fc_{eob_3}^{z \wedge (\neg u) \xrightarrow{a_1} z \vee u})$. É, portanto, uma explicação para a garantia de $z \vee u$ a partir de $z \wedge (\neg u)$ por a_1 em eob_3.

2.2. As acções a_2 e a_3 garantem $z \vee u$ a partir de $z \wedge (\neg u)$ em eob_3.

2.3. O conjunto

$$\{\mathbf{G}(\diamond a_1 \Rightarrow (x \vee (\neg z) \vee u))\}$$

é explicação para $sp_{seg}(f)$ em eob_3.

3. O conjunto

$$\{z \vee u,\ \mathbf{G}(\diamond a_1 \Rightarrow (x \vee (\neg z) \vee u))\}$$

é explicação para o problema de segurança $y \Rightarrow (z\ \mathbf{W}\ u)$.

4. Na Figura 3.7 está representado um fragmento de um possível modelo da especificação eob_3' que se obtém enriquecendo eob_3 com a explicação referida em **3**. Para cada $0 \leq k \leq 4$ referem-se os atributos que são ou não satisfeitos.

$$\underset{(0)}{\boxed{\neg x, \boldsymbol{y}, \boldsymbol{z}, \neg u}} \xrightarrow{\nabla a_3} \underset{(1)}{\boxed{x, y, \boldsymbol{z}, \neg u}} \xrightarrow{\nabla a_1} \underset{(2)}{\boxed{x, \neg y, \boldsymbol{z}, \neg u}} \xrightarrow{\nabla a_2} \underset{(3)}{\boxed{x, y, \neg z, \boldsymbol{u}}} \xrightarrow{\nabla a_2} \underset{(4)}{\boxed{x, y, \neg z, \neg u}} \ \ldots$$

Figura 3.7: Modelo de eob_3'

Neste modelo, y é satisfeito no instante inicial, u é satisfeito em (3) e tem-se z satisfeito desde o instante inicial até ao primeiro instante que satisfaz u. A nova especificação só verifica $y \Rightarrow (z\ \mathbf{W}\ u)$ no instante inicial pois em (4) y é satisfeito mas aí já não se verifica $z\ \mathbf{W}\ u$.

Note-se que existem modelos de eob_3' nos quais u pode nunca chegar a ser satisfeito. ■

Apresentam-se, seguidamente, dois exemplos de explicações problemas de segurança correspondentes a fórmulas do tipo $\mathbf{G}\ q$, ou seja, explicações para invariantes.

Exemplo 3.77 Considere-se a especificação de objecto eob_1 e o problema de segurança em eob_1

$$f = \mathbf{G}(x \vee y)$$

referidos no Exemplo 3.3.

1. Tem-se que $sp_{CI}(f) = x \vee y$ e $eob_1 \not\models sp_{CI}(f)$. Do Exemplo 3.62 decorre que o conjunto

$$\{x\}$$

é explicação para $sp_{CI}(f)$ em eob_1.

2. Tem-se que $sp_{seg}(f) = \mathbf{G}((x \vee y) \Rightarrow (\mathbf{X}(x \vee y)))$ e $eob_1 \not\models sp_{seg}(f)$.

2.1. A acção a_1 não preserva $x \vee y$ em eob_1. No Exemplo 3.36 são mencionadas restrições de activação que constituem explicações para a referida preservação. Em particular, a restrição de activação $f_4 = \mathbf{G}(\diamond a_1 \Rightarrow (x \vee (\neg y) \vee (\neg z)))$ é induzida por $min(Fc_{eob_1}^{x \vee y \xrightarrow{a_1} x \vee y}) = \{\{x\}, \{\neg y\}, \{\neg z\}\}$ e consequentemente é mais liberal que qualquer outra explicação em $E_{RActv}(Fc_{eob_1}^{x \vee y \xrightarrow{a_1} x \vee y})$.

No entanto, no âmbito do problema que se pretende resolver, isto é, assegurar que $x \vee y$ é sempre satisfeito, se num dado instante $\neg y$ é satisfeito, como se pretende que $x \vee y$ também o seja, então x será necessariamente satisfeito. Assim, neste contexto, a restrição de activação $f_5 = \mathbf{G}(\diamond a_1 \Rightarrow (x \vee (\neg z)))$, induzida por $\{\{x\}, \{\neg z\}\}$, não restringirá mais a ocorrência de a_1 do que f_4 porque não existirá nenhum instante em que $\neg x$ e $\neg y$ sejam ambos satisfeitos. A restrição de activação $f_5 \in E_{RActv}(Fc_{eob_1}^{x \vee y \xrightarrow{a_1} x \vee y})$ e, sendo sintacticamente mais simples, pode dizer-se que contém a mesma informação que f_4 sobre a possibilidade de ocorrência de a_1.

No final desta subsecção descreve-se uma forma de reconhecer situações deste tipo a partir da análise de fechos de tableaux.

2.2. A acção a_2 preserva $x \vee y$ em eob_1.

2.3. O conjunto

$$\{\mathbf{G}(\diamond a_1 \Rightarrow (x \vee (\neg z)))\}$$

é explicação para $sp_{seg}(f)$ em eob_1.

3. O conjunto

$$\{x,\ \mathbf{G}(\diamond a_1 \Rightarrow (x \vee (\neg z)))\}$$

é explicação para o problema de segurança $\mathbf{G}(x \vee y)$.

4. Na Figura 3.8 está representado um fragmento de um possível modelo da especificação eob'_1 que se obtém enriquecendo eob_1 com a explicação apresentada em **3.** Para cada

$$\underset{(0)}{\boxed{\boldsymbol{x}, \neg y, z}} \xrightarrow{\nabla a_1} \underset{(1)}{\boxed{\neg x, \boldsymbol{y}, \neg z}} \xrightarrow{\nabla a_1} \underset{(2)}{\boxed{\boldsymbol{x}, \neg y, z}} \xrightarrow{\nabla a_2} \underset{(3)}{\boxed{\boldsymbol{x}, \boldsymbol{y}, \neg z}} \xrightarrow{\nabla a_1} \underset{(4)}{\boxed{\boldsymbol{x}, \boldsymbol{y}, z}} \xrightarrow{\nabla a_2} \underset{(5)}{\boxed{\neg x, \boldsymbol{y}, \neg z}} \ldots$$

Figura 3.8: Modelo de eob'_1

$0 \leq k \leq 5$ referem-se os atributos que são ou não satisfeitos. ■

Exemplo 3.78 Considere-se a especificação de objecto $eob_4 = (\Sigma_4, AxF_4, AxS_4)$ com

$$\Sigma_4 = (\{a_1, a_2\}, \{x, y, z\})$$

$$AxF_4 = \{x, y\} \qquad AxS_4 = \{\mathbf{G}((\nabla a_1 \wedge \alpha\, {}^{x}_{\neg z}\, {}^{y}_{x}\, {}^{z}_{\neg z}) \Rightarrow (\mathbf{X}\,\alpha)),$$
$$\mathbf{G}((\nabla a_2 \wedge \alpha\, {}^{y}_{z}\, {}^{z}_{\neg x}) \Rightarrow (\mathbf{X}\,\alpha))\}$$

A fórmula $f = \mathbf{G}(x \wedge y)$ é um problema de segurança em eob_4.

1. Tem-se que $sp_{CI}(f) = x \wedge y$ e $eob_4 \models sp_{CI}(f)$.

2. Tem-se que $sp_{seg}(f) = \mathbf{G}((x \wedge y) \Rightarrow (\mathbf{X}(x \wedge y)))$ e $eob_4 \not\models sp_{seg}(f)$.

2.1. A acção a_1 não preserva $x \wedge y$ em eob_4. O tableau representado na Figura 3.9 é um tableau de decisão em $T_{\Sigma_4}(G_{eob_4}^{x\wedge y \xrightarrow{a_1} x\wedge y})$ e consequentemente $min(Fc_{eob_4}^{x\wedge y \xrightarrow{a_1} x\wedge y}) = \{\{\neg x\}, \{\neg y\}, \{\neg z\}\}$.

As restrições de activação

$$f_{a_1}^1 = \mathbf{G}(\diamond a_1 \Rightarrow (\neg x)) \qquad f_{a_1}^2 = \mathbf{G}(\diamond a_1 \Rightarrow (\neg y)) \qquad f_{a_1}^3 = \mathbf{G}(\diamond a_1 \Rightarrow (\neg z))$$
$$f_{a_1}^4 = \mathbf{G}(\diamond a_1 \Rightarrow ((\neg x) \vee (\neg y) \vee (\neg z)))$$

são elementos de $E_{RActv}(Fc_{eob_4}^{x\wedge y \xrightarrow{a_1} x\wedge y})$ e, portanto, explicações para a garantia de preservação de $x \wedge y$ por a_1 em eob_4.

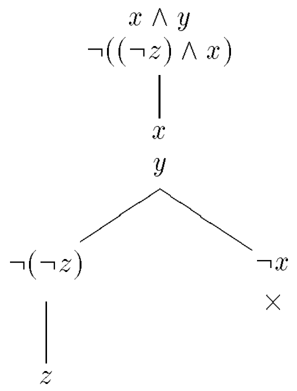

Figura 3.9: Tableau de decisão para $\{x \wedge y, \neg((\neg z) \wedge x)\}$

As restrições de activação $f_{a_1}^1$ e $f_{a_1}^2$ asseguram trivialmente a preservação de $x \wedge y$ dado que só permitem a ocorrência de a_1 quando se tem $\neg(x \wedge y)$.

Dado que após ocorrência de a_1 se tem que x e y se verificam sempre que, respectivamente, $\neg z$ e x se verificarem no instante em que a_1 ocorre, o facto de $f_{a_1}^3$ obrigar que a_1 só possa ocorrer quando se tem $\neg z$ assegura a preservação de $x \wedge y$.

A restrição de activação $f_{a_1}^4$ permite a ocorrência de a_1 quanto se verificar alguma das situações descritas nos dois parágrafos anteriores. É estritamente mais liberal que qualquer uma das outras e é induzida por $min(Fc_{eob_4}^{x \wedge y \xrightarrow{a_1} x \wedge y})$.

Refira-se, no entanto, que dadas as características do problema que se pretende resolver, isto é, assegurar que $x \wedge y$ se verifica em todos os instantes, não são muito interessantes as explicações que contribuem para a preservação de $x \wedge y$ porque só permitem a ocorrência de a_1 quando se tem $\neg(x \wedge y)$, ou seja, $f_{a_1}^1$ e $f_{a_1}^2$. Na verdade, dado que se pretende precisamente que $\neg(x \wedge y)$ nunca seja satisfeita, a_1 nunca chegaria a poder ocorrer com tais explicações. Por outro lado, neste contexto, as explicações $f_{a_1}^3$ e $f_{a_1}^4$ restringem a ocorrência de a_1 da mesma forma, isto é, a_1 apenas poderá ocorrer quando $\neg z$ se verifique.

No final desta subsecção descreve-se uma forma de reconhecer este tipo de situações a partir dos fechos de tableaux.

2.2. A acção a_2 não preserva $x \wedge y$ em eob_4. O tableau representado na Figura 3.10 é um tableau de decisão em $T_{\Sigma_4}(G_{eob_4}^{x \wedge y \xrightarrow{a_2} x \wedge y})$ e consequentemente $min(Fc_{eob_4}^{x \wedge y \xrightarrow{a_2} x \wedge y}) = \{\{\neg x\}, \{\neg y\}, \{z\}\}$.

As restrições de activação

$$f_{a_2}^1 = \mathbf{G}(\diamond a_2 \Rightarrow (\neg x)) \qquad f_{a_2}^2 = \mathbf{G}(\diamond a_2 \Rightarrow (\neg y)) \qquad f_{a_2}^3 = \mathbf{G}(\diamond a_2 \Rightarrow z)$$
$$f_{a_2}^4 = \mathbf{G}(\diamond a_2 \Rightarrow ((\neg x) \vee (\neg y) \vee z))$$

são elementos de $E_{RActv}(Fc_{eob_4}^{x \wedge y \xrightarrow{a_2} x \wedge y})$ e, portanto, explicações para a garantia de preservação de $x \wedge y$ por a_2 em eob_4.

Comentário semelhantes aos apresentados em **2.1** relativamente às restrições de activação $f_{a_1}^1$, $f_{a_1}^2$, $f_{a_1}^3$ e $f_{a_1}^4$ podem também ser feitos relativamente às restrições de activação

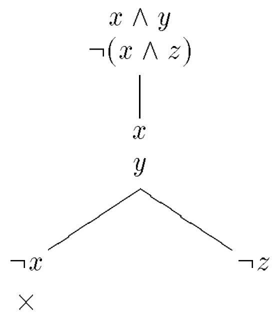

Figura 3.10: Tableau de decisão para $\{x \wedge y, \neg(x \wedge z)\}$

$f_{a_2}^1$, $f_{a_2}^2$, $f_{a_2}^3$ e $f_{a_2}^4$.

2.3. O conjunto

$$\{\mathbf{G}(\diamond a_1 \Rightarrow (\neg z)),\ \mathbf{G}(\diamond a_2 \Rightarrow z)\}$$

é explicação para $sp_{seg}(f)$ em eob_4.

3. O conjunto

$$\{\mathbf{G}(\diamond a_1 \Rightarrow (\neg z)),\ \mathbf{G}(\diamond a_2 \Rightarrow z)\}$$

é explicação para o problema de segurança $\mathbf{G}(x \wedge y)$.

4. Na Figura 3.11 está representado um fragmento de um possível modelo da especificação eob_4' que se obtém enriquecendo eob_4 com a explicação referida em **3.**

$$\underset{(0)}{\boxed{\boldsymbol{x},\boldsymbol{y},\neg z}} \xrightarrow{\nabla a_1} \underset{(1)}{\boxed{\boldsymbol{x},\boldsymbol{y},z}} \xrightarrow{\nabla a_2} \underset{(2)}{\boxed{\boldsymbol{x},\boldsymbol{y},\neg z}} \xrightarrow{\nabla a_1} \underset{(3)}{\boxed{\boldsymbol{x},\boldsymbol{y},z}} \xrightarrow{\nabla a_2} \underset{(4)}{\boxed{\boldsymbol{x},\boldsymbol{y},\neg z}} \ \ldots$$

Figura 3.11: Modelo de eob_4'

Para cada $0 \leq k \leq 4$ referem-se os atributos que são ou não satisfeitos. ■

As explicações para problemas de segurança do tipo $\mathbf{G}(r \Rightarrow (q_1\, \mathbf{W}\, q_2))$ baseiam-se novamente em explicações para problemas do tipo $\mathbf{G}(p \Rightarrow (\mathbf{X}\, q))$ mas agora, em vez de explicações que garantam apenas certas condições iniciais, é necessário considerar também explicações para um certo invariante.

Definição 3.79 Seja $f = \mathbf{G}(r \Rightarrow (q_1\ \mathbf{W}\ q_2)) \in O_\Sigma$. Os *subproblemas para a explicação de* f são as fórmulas

- $sp_{seg_1}(f) = \mathbf{G}(r \Rightarrow (q_1 \vee q_2))$;
- $sp_{seg_2}(f) = \mathbf{G}((q_1 \wedge (\neg q_2)) \Rightarrow (\mathbf{X}(q_1 \vee q_2)))$.

O conjunto dos subproblemas para a explicação de f é o conjunto constituído pelas fórmulas anteriores e denota-se por $Sp(f)$.

Para cada $a \in Acc$, denota-se por $Gr_a(Sp(f))$ o conjunto

$$\{gr_a(sp_{seg_1}(f)), gr_a(sp_{seg_2}(f))\}$$

dito *conjunto das garantias induzidas por* $Sp(f)$ *relativamente à acção* a. ■

Proposição 3.80 Seja $\mathbf{G}(r \Rightarrow (q_1 \mathbf{W}\, q_2))$ um problema de segurança em eob. Seja

$$X = \{sp \in Sp(\mathbf{G}(r \Rightarrow (q_1 \mathbf{W}\, q_2))) : eob \not\models sp\}$$

e para cada $sp \in X$ seja E_{sp} uma explicação para sp em eob. Se

$$E = \bigcup_{sp \in X} E_{sp}$$

é eob-possível então E é uma explicação para o problema $\mathbf{G}(r \Rightarrow (q_1 \mathbf{W}\, q_2))$ em eob.

Prova: Seja eob' o enriquecimento de eob com E.

(a) Tem-se que $eob' \models sp$ para todo $sp \in Sp(\mathbf{G}(r \Rightarrow (q_1 \mathbf{W}\, q_2)))$ tal que $sp \notin X$.

Seja $sp \in X$. Seja eob'' o enriquecimento de eob com E_{sp}. Pela Definição 3.4, $eob'' \models sp$ e portanto $eob' \models sp$. Pela Proposição 3.70, $eob' \models \mathbf{G}(r \Rightarrow (q_1 \mathbf{W}\, q_2))$.

(b) Pelas Definições 2.22 e 2.23, dado que E é eob-possível, tem-se que eob' é coerente.

(c) Por (a), (b) e Definição 3.4, E é uma explicação para $\mathbf{G}(r \Rightarrow (q_1 \mathbf{W}\, q_2))$. ■

Exemplo 3.81 Considere-se a especificação de objecto eob_3 descrita no Exemplo 3.46. A fórmula

$$f = \mathbf{G}(y \Rightarrow (z \mathbf{W}\, u))$$

é um problema de segurança em eob_3.

1. Tem-se que $sp_{seg_1}(f) = \mathbf{G}(y \Rightarrow (z \vee u))$ e $eob_3 \not\models sp_{seg_1}(f)$. Seja $f_1' = sp_{seg_1}(f)$.

1.1. Tem-se que $sp_{CI}(f_1') = y \Rightarrow (z \vee u)$ e $eob_3 \not\models sp_{CI}(f_1')$. Do Exemplo 3.62 decorre que, em particular, o conjunto

$$\{z \vee u\}$$

é explicação para $sp_{CI}(f_1')$ em eob_3.

1.2. Tem-se que $sp_{seg}(f_1') = \mathbf{G}((y \Rightarrow (z \vee u)) \Rightarrow (\mathbf{X}(y \Rightarrow (z \vee u))))$ e $eob_3 \not\models sp_{seg}(f_1')$.

1.2.1. As acções a_1 e a_3 preservam $y \Rightarrow (z \vee u)$ em eob_3.

1.2.2. A acção a_2 não preserva $y \Rightarrow (z \vee u)$ em eob_3. O tableau representado na Figura 3.1, no âmbito do Exemplo 3.20, é tableau de decisão em $T_{\Sigma_3}(G_{eob_3}^{y \Rightarrow (z \vee u) \stackrel{a_2}{-} y \Rightarrow (z \vee u)})$ e portanto $min(Fc_{eob_3}^{y \Rightarrow (z \vee u) \stackrel{a_2}{-} y \Rightarrow (z \vee u)}) = \{\{z\}, \{y, \neg u\}\}$. A restrição de activação $\mathbf{G}(\diamond a_2 \Rightarrow (z \vee (y \wedge (\neg u))))$ é explicação para a preservação de $y \Rightarrow (z \vee u)$ por a_2 em eob_3.

Note-se que também aqui se tem uma situação análoga à do Exemplo 3.77. Como se pretende ter a satisfação de $y \Rightarrow (z \vee u)$ em todos os estados, sempre que $y \wedge (\neg u)$

fôr satifeito também z o deverá ser. Assim, as restrições de activação $\mathbf{G}(\diamond a_2 \Rightarrow z)$ e $\mathbf{G}(\diamond a_2 \Rightarrow (z \vee (y \wedge (\neg u))))$ são explicações para a garantia da preservação de $y \Rightarrow (z \vee u)$ por a_2 em eob_3 e ambas restringem a ocorrência de a_2 da mesmo modo.

1.2.3. O conjunto

$$\{\mathbf{G}(\diamond a_2 \Rightarrow z)\}$$

é explicação para $sp_{seg}(f_1')$ em eob_3.

1.3 O conjunto

$$\{z \vee u, \mathbf{G}(\diamond a_2 \Rightarrow z)\}$$

é explicação para $sp_{seg_1}(f)$ em eob_3.

2. Tem-se que $sp_{seg_2}(f) = \mathbf{G}((z \wedge (\neg u)) \Rightarrow (\mathbf{X}(z \vee u)))$ e $eob_3 \not\models sp_{seg_2}(f)$.
Seja $f_2' = sp_{seg_2}(f)$.

2.1. A acção a_1 não garante $z \vee u$ a partir de $z \wedge (\neg u)$ em eob_3. No Exemplo 3.76 foi encontrada a explicação $\mathbf{G}(\diamond a_1 \Rightarrow (x \vee (\neg z) \vee u))$ para esta garantia.

2.2. As acções a_2 e a_3 garantem $z \vee u$ a partir de $z \wedge (\neg u)$ em eob_3.

2.3. O conjunto

$$\{\mathbf{G}(\diamond a_1 \Rightarrow (x \vee (\neg z) \vee u))\}$$

é explicação para $sp_{seg_2}(f)$ em eob_3.

3. O conjunto

$$\{z \vee u,\ \mathbf{G}(\diamond a_1 \Rightarrow (x \vee (\neg z) \vee u)),\ \mathbf{G}(\diamond a_2 \Rightarrow z)\}$$

é explicação para o problema de segurança $y \Rightarrow (z\,\mathbf{W}\,u)$ em eob_3.

4. Na Figura 3.12 estão representados fragmentos de dois possíveis modelos da especificação eob_3' que se obtém enriquecendo eob_3 com a explicação referida em **3**.

$$\underset{(0)}{\boxed{\neg x, \boldsymbol{y}, \boldsymbol{z}, \neg u}} \xrightarrow{\nabla a_3} \underset{(1)}{\boxed{x, y, \boldsymbol{z}, \neg u}} \xrightarrow{\nabla a_1} \underset{(2)}{\boxed{x, \neg y, \boldsymbol{z}, \neg u}} \xrightarrow{\nabla a_2} \underset{(3)}{\boxed{x, y, \neg z, \boldsymbol{u}}} \xrightarrow{\nabla a_3} \underset{(4)}{\boxed{\neg x, y, \neg z, \boldsymbol{u}}}$$

$$\xrightarrow{\nabla a_1} \underset{(5)}{\boxed{\neg x, \neg \boldsymbol{y}, \neg z, \neg u}} \ \ldots$$

$$\underset{(0)}{\boxed{x, \boldsymbol{y}, \boldsymbol{z}, \neg u}} \xrightarrow{\nabla a_3} \underset{(1)}{\boxed{\neg x, y, \boldsymbol{z}, \neg u}} \xrightarrow{\nabla a_3} \underset{(2)}{\boxed{x, y, \boldsymbol{z}, \neg u}} \xrightarrow{\nabla a_1} \underset{(3)}{\boxed{x, \neg y, \boldsymbol{z}, \neg u}} \xrightarrow{\nabla a_3} \underset{(4)}{\boxed{\neg x, \neg y, \boldsymbol{z}, \neg u}} \ldots$$

Figura 3.12: Modelos de eob_3'

Comparando este exemplo com o Exemplo 3.76, pretende-se agora ter $y \Rightarrow (z\,\mathbf{W}\,u)$ em qualquer instante. O primeiro dos modelos representados na Figura 3.12 é idêntico ao modelo representado na Figura 3.7 até $k = 3$. Mas, contrariamente ao que aí acontecia, agora já não é permitida a ocorrência de a_2 no instante (3) pois tal levaria a que no instante (4) se não tivesse $y \Rightarrow (z\,\mathbf{W}\,u)$.

O segundo modelo ilustra um caso em que a_2 nunca ocorre: após duas ocorrências consecutivas de a_3 tem-se uma ocorrência de a_1 seguida novamente de duas ocorrências consecutivas de a_3. ∎

Exemplo 3.82 Considere-se novamente a especificação de objecto eob_3 descrita no Exemplo 3.46. A fórmula

$$f = \mathbf{G}((\neg y) \Rightarrow (x\,\mathbf{W}\,(\neg z)))$$

é um problema de segurança em eob_3.

1. Tem-se que $sp_{seg_1}(f)=\mathbf{G}((\neg y)\Rightarrow(x \vee (\neg z)))$ e $eob_3 \not\models sp_{seg_1}(f)$. Seja $f_1'=sp_{seg_1}(f)$.

1.1. Tem-se que $sp_{CI}(f_1')=(\neg y)\Rightarrow(x \vee (\neg z))$ e $eob_3 \models sp_{CI}(f_1')$.

1.2. Tem-se $sp_{seg}(f_1')=\mathbf{G}(((\neg y)\Rightarrow(x\vee(\neg z)))\Rightarrow(\mathbf{X}((\neg y)\Rightarrow(x\vee(\neg z)))))$ e $eob_3 \not\models sp_{seg}(f_1')$.

1.2.1. As acções a_1 e a_2 preservam $(\neg y) \Rightarrow (x \vee (\neg z))$ em eob_3.

1.2.2. A acção a_3 não preserva $(\neg y) \Rightarrow (x \vee (\neg z))$ em eob_3. O tableau representado na Figura 3.14 é tableau de decisão em $T_{\Sigma_3}(G_{eob_3}^{(\neg y)\Rightarrow(x\vee(\neg z))\xrightarrow{a_3}(\neg y)\Rightarrow(x\vee(\neg z))})$ e consequentemente

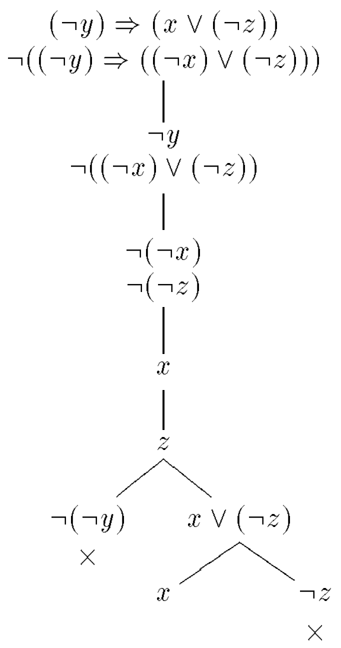

Figura 3.13: Tableau de decisão para $\{(\neg y) \Rightarrow (x \vee (\neg z)), \neg((\neg y) \Rightarrow ((\neg x) \vee (\neg z)))\}$

$min(Fc_{eob_3}^{(\neg y)\Rightarrow(x\vee(\neg z))\xrightarrow{a_3}(\neg y)\Rightarrow(x\vee(\neg z))})=\{\{\neg x\},\{y\},\{\neg z\}\}$.

2. Tem-se que $sp_{seg_2}(f) = \mathbf{G}((x \wedge (\neg(\neg z))) \Rightarrow (\mathbf{X}(x \vee (\neg z))))$ e $eob_3 \not\models sp_{seg_2}(f)$.
Seja $f_2'=sp_{seg_2}(f)$.

2.1. As acções a_1 e a_2 garantem $x \vee (\neg z)$ a partir de $x \wedge (\neg(\neg z))$ em eob_3.

2.2. A acção a_3 não garante $x \vee (\neg z)$ a partir de $x \wedge (\neg(\neg z))$ em eob_3. O tableau representado na Figura 3.14 é tableau de decisão em $T_{\Sigma_3}(G_{eob_3}^{x\wedge(\neg(\neg z))\xrightarrow{a_3}x\vee(\neg z)})$ e consequentemente

$$
\begin{array}{c}
x \wedge (\neg(\neg z)) \\
\neg((\neg x) \vee (\neg z)) \\
| \\
x \\
\neg((\neg z) \\
| \\
\neg(\neg x) \\
\neg(\neg z) \\
| \\
z \\
| \\
x \\
| \\
z
\end{array}
$$

Figura 3.14: Tableau de decisão para $\{x \wedge (\neg(\neg z)), \neg((\neg x) \vee (\neg z))\}$

$min(Fc_{eob_3}^{x\wedge(\neg(\neg z)) \overset{a_3}{\to} x\vee(\neg z)}) = \{\{\neg x\}, \{\neg z\}\}$.

3. Neste exemplo, o conjunto das garantias induzidas por $Sp(f)$ relativamente à acção a_3, $Gr_{a_3}(Sp(f))$, é constituído por duas fórmulas as quais não são satisfeitas por eob_3. Com o objectivo de encontrar restrições de activação para explicar cada uma das garantias em $Gr_{a_3}(Sp(f))$ foram construídos em **1.2.2** e **2.2** dois tableaux.

Escolhendo uma restrição de activação relativa a cada uma dessas garantias (de tal modo que constituam um conjunto eob_3-possível) obtém-se, neste caso, uma explicação para $sp_{seg_1}(f)$ e $sp_{seg_2}(f)$ e consequentemente para f.

Uma outra forma de proceder consiste em encontrar uma única restrição de activação que assegure ambas as garantias relativas a a_3. Neste exemplo isso é trivial dado que o conjunto dos fechos minimais do tableau construído em **2.2** está contido no conjunto dos fechos minimais do tableau construído em **1.2.2** e portanto, em particular, a restrição de activação $\mathbf{G}(\diamond a_3 \Rightarrow ((\neg x) \vee (\neg z)))$ é simultaneamente uma explicação para a garantia referida em **1.2.2** e para a garantia referida em **2.2**. No final desta subsecção far-se-á referência ao modo de obter uma única restrição de activação noutros casos.

Assim, o conjunto

$$\{\mathbf{G}(\diamond a_3 \Rightarrow ((\neg x) \vee (\neg z)))\}$$

é explicação para $sp_{seg_1}(f)$ e $sp_{seg_2}(f)$ em eob_3 e, consequentemente, é explicação para o problema de segurança $\mathbf{G}((\neg y) \Rightarrow (x \mathbf{W} (\neg z)))$. ∎

A terminar esta subsecção fazem-se agora alguns comentários quanto a critérios de escolha de explicações no âmbito de problemas de segurança.

Para resolver problemas de segurança há que resolver, em geral, vários problemas mais simples que vão envolver construção de explicações para garantias iniciais de constrangimentos de estado e/ou garantias de constrangimentos de estado a partir de outros constrangimentos de estado através de acções. Assim, os critérios anteriormente mencionados para tais casos podem ser aqui utilizados para a escolha das várias explicações envolvidas. É possível, contudo, reconhecer mais alguns critérios.

Critérios para invariantes

1. Tal como foi ilustrado no Exemplo 3.78, no caso de problemas de segurança $\mathbf{G}\,q$ com $q \in CE^{\mathbf{tf}}_{\Sigma}$, existem situações em que nem sempre é mais interessante escolher explicações mais liberais para a garantia da preservação de q por uma dada acção a. Suponha-se que *Fc é um fecho em $Fc^{q \xrightarrow{a} q}_{eob}$ e existe $Fc' \in Fc(\{q\})$ tal que $Fc' \subseteq Fc$.* Nestas circunstâncias, pela Proposição 3.21, o conjunto $\{q\} \cup Fc$ é incoerente. Como o objectivo é conseguir que q seja satisfeito em todos os estados, o conjunto Fc nunca virá a ser satisfeito por nenhum estado. Consequentemente, neste contexto, não é de grande utilidade a informação de que a pode ocorrer quando o conjunto Fc fôr satisfeito. Podem eliminar-se a geração deste tipo de explicações eliminando de $Fc^{q \xrightarrow{a} q}_{eob}$ este tipo de fechos.

2. Nos Exemplos 3.77 e 3.81 foram ilustradas duas outras situações, também para o caso de (sub)problemas de segurança $\mathbf{G}\,q$, em que nem sempre será mais interessante seguir apenas o critério das explicações mais liberais. Suponha-se $F \subseteq Fc^{q \xrightarrow{a} q}_{eob}$. Pode *eliminar-se de F um fecho Fc quando existem $\{l\} \in F$ e $Fc' \in Fc(\{q\})$ tais que $Fc' \subseteq Fc \cup \{\bar{l}\}$.* Nestas circunstâncias, se f_1 é uma restrição de activação induzida por F, então a ocorrência de a é permitida, em particular, quando Fc é satisfeito ou l é satisfeito. Mas, pela Proposição 3.21, o conjunto $\{q\} \cup Fc \cup \{\bar{l}\}$ é incoerente. Assim, o facto de a ocorrência de a ser permitida quando se verifica $Fc \cup \{\bar{l}\}$ não é muito relevante neste contexto pois, como se pretende que q seja sempre verificada, não haverá nenhum instante em que se verifique $Fc \cup \{\bar{l}\}$. Logo, apenas $Fc \cup \{l\}$ pode vir a ser eventualmente satisfeito o que significa que sempre que Fc fôr satisfeito l também o será. É de algum modo redundante ter a informação simultânea de que a pode ocorrer quando se verifica Fc ou quando se verifica l. Embora f_1 seja mais liberal que qualquer restrição de activação f_2 induzida por $F \backslash \{Fc\}$, f_2 restringe a ocorrência de a do mesmo modo que f_1.

Existência de várias garantias relativamente a uma acção

No caso de problemas de segurança $f = \mathbf{G}(r \Rightarrow (q_1 \mathbf{W} q_2))$, para cada $a \in Acc$, o conjunto das garantias induzidas por $Sp(f)$ relativamente a a, $Gr_a(Sp(f))$, é constituído por duas fórmulas. Consequentemente, podem encontrar-se situações, tal como a do Exemplo 3.82, em que existe uma acção a para a qual nenhuma das fórmulas em $Gr_a(Sp(f))$ é satisfeita pela especificação de objecto *eob* dada. Associada a cada garantia em $Gr_a(Sp(f))$ está a construção de um certo tableau cujos fechos permitirão construir restrições de activação que assegurem as referidas garantias. A escolha de uma restrição de activação associada a cada uma das garantias contribui para a explicação final do problema. Se os fechos de um dos tableau são também fechos do outro, qualquer restrição de activação construída a partir do primeiro tableau pode também ser construída a partir do segundo e, consequentemente, qualquer restrição de activação que assegure a garantia associada ao primeiro tableau também assegura a garantia associada ao segundo. Se tal situação não se verifica, uma forma de construir uma única restrição de activação que assegure ambas as garantias em $Gr_a(Sp(f))$ é a que a seguir se descreve. Sejam t_1 e t_2 os tableaux construídos, F_1 e F_2 conjuntos (não vazios) de fechos de t_1 e t_2, respectivamente, $Fc^1_1 \ldots Fc^1_{n_1} \in Enm(F_1)$, $Fc^2_1 \ldots Fc^2_{n_2} \in Enm(F_2)$ e

> *F o subconjunto de $\wp(LE_\Sigma)$ tal que $Fc \in F$ sse $Fc \cap \overline{F}c = \emptyset$ e existem $1 \leq k_1 \leq n_1$ e $1 \leq k_2 \leq n_2$ tal que $Fc = Fc^1_{k_1} \cup Fc^2_{k_2}$.*

Conclui-se facilmente que *qualquer restrição de activação induzida por $F' \subseteq F$, se fôr eob-possível, é explicação para as duas garantias em $Gr_a(Sp(f))$.* Se, em particular, F' é constituído pelos conjuntos minimais de F e f é restrição de activação induzida por F' então f é mais liberal que qualquer outra restrição de activação induzida por algum subconjunto de F.

3.5.2 Problemas de resposta

Nesta subsecção descreve-se o modo como explicações para problemas de resposta em *eob* podem ser obtidas. As explicações para este tipo de problemas incluem não apenas restrições de activação mas também alguns requisitos de justiça. Como tem vindo a ser referido, o modo de calcular explicações para este tipo de problemas foi motivado pelas técnicas descritas na literatura para verificação de propriedades de resposta [41] e animação [39]. A ideia base é que se existe uma acção a que garante um constrangimento de estado q então assegura-se que q é satisfeito um número infinto de vezes sempre que se assegurar a ocorrência de a um número infinto de vezes. A aplicação directa desta ideia conduz ao que se designa por *explicações em um passo.* Alternativamente descrevem-se também *explicações em vários passos.* Neste caso existem asserções intermédias que irão sendo progressivamente estabelecidas por certas acções até se chegar à satisfação de q. Estas asserções podem ser vistas como constituindo uma espécie de "medida" de quão longe se está de satisfazer q. Cada acção que ocorra não deverá aumentar tal "distância" e terão necessariamente de ocorrer acções que a façam diminuir até se chegar à satisfação de q.

Na primeira subsubsecção apresentam-se as explicações num passo e na segunda subsubsecção as explicações em vários passos.

3.5.2.1 Explicações num passo

Nesta subsubsecção descreve-se o modo de construir explicações para problemas de resposta em *eob* em um passo.

Proposição 3.83 Se

(i) $eob \models \mathbf{G}(r \Rightarrow (q_1\, \mathbf{W}\, q_2))$;

(ii) existe $a \in Acc$ que tal que

- $eob \models \mathbf{G}((\triangledown a \wedge q_1 \wedge (\neg q_2)) \Rightarrow (\mathbf{X}\, q_2))$,

– $eob \models \mathbf{G}((q_1 \wedge (\neg q_2)) \Rightarrow \diamond a)$,

– $eob \models RJst_\Sigma^a$,

então $eob \models \mathbf{G}(r \Rightarrow (q_1 \,\mathbf{U}\, q_2))$.

Prova: Sejam λ modelo de eob e $k \in I\!N_0$ tal que $\lambda, k \models r$. Pela hipótese (i), $\lambda, k \models q_1 \,\mathbf{W}\, q_2$ o que significa que: (a) $\lambda, k \models q_1 \,\mathbf{U}\, q_2$ ou (b) $\lambda, k \models \mathbf{G}(q_1 \wedge (\neg q_2))$.

No caso (a), tem-se que $\lambda, k \models r \Rightarrow (q_1 \,\mathbf{U}\, q_2)$.

No caso (b), e pela segunda condição da hipótese (ii), $\lambda, k \models \mathbf{G}(\diamond a)$ e portanto $\lambda, 0 \models \mathbf{G}(\mathbf{F} \diamond a))$. Pela terceira condição da hipótese (ii) e pela Definição 2.24, $eob \models (\mathbf{G}(\mathbf{F} \diamond a)) \Rightarrow (\mathbf{G}(\mathbf{F} \nabla a))$ e portanto também $\lambda, 0 \models \mathbf{G}(\mathbf{F} \nabla a)$. Então existe $k' \geq k$ tal que $\lambda, k' \models \nabla a$. Dado que se tem também que $\lambda, k' \models q_1 \wedge (\neg q_2)$, a primeira condição da hipótese (ii) permite concluir que $\lambda, k'+1 \models q_2$, contradizendo assim a possibilidade de se verificar (b).

Conclui-se então que $\lambda \models \mathbf{G}(r \Rightarrow (q_1 \,\mathbf{U}\, q_2))$ e portanto $eob \models \mathbf{G}(r \Rightarrow (q_1 \,\mathbf{U}\, q_2))$. ∎

Corolário 3.84 Se existe $a \in Acc$ que tal que

- $eob \models \mathbf{G}((\nabla a \wedge (\neg q)) \Rightarrow (\mathbf{X}\, q))$,
- $eob \models \mathbf{G}((\neg q) \Rightarrow \diamond a)$,
- $eob \models RJst_\Sigma^a$,

então $eob \models \mathbf{G}(\mathbf{F}\, q))$.

Prova: Pela Proposição 3.83 fazendo $r = q_1 = \mathbf{t}$ e $q_2 = q$. ∎

A Proposição 3.83 mostra que é possível concluir que são *eob*-válidas observações de resposta $\mathbf{G}(r \Rightarrow (q_1 \,\mathbf{U}\, q_2))$ a partir do conhecimento de que existe uma certa observação de segurança que é *eob*-válida e de que existe uma acção a que verifica certas condições. A observação de segurança tem por objectivo assegurar que a ocorrência de cada acção não destrói a possibilidade de a observação de resposta vir a ser cumprida (*nada de mau acontece*). Em particular assegura que sempre que r é satisfeito então ou se tem sempre q_1 de aí em diante ou, efectivamente, alguma vez se terá q_2. As condições que a acção a tem de verificar têm por objectivo assegurar que, de facto, q_2 virá a ser satisfeito neste contexto (*algo de bom acontecerá*).

Definição 3.85 Sejam $f = \mathbf{G}(r \Rightarrow (q_1 \,\mathbf{U}\, q_2)) \in O_\Sigma$ e $a \in Acc$. Os *subproblemas para a explicação num passo de f com base em a* são as fórmulas

- $sp_{seg}(f) = \mathbf{G}(r \Rightarrow (q_1 \,\mathbf{W}\, q_2))$;
- $sp_{\nabla a}(f) = \mathbf{G}((\nabla a \wedge q_1 \wedge (\neg q_2)) \Rightarrow (\mathbf{X}\, q_2))$;
- $sp_{\diamond a}(f) = \mathbf{G}((q_1 \wedge (\neg q_2)) \Rightarrow \diamond a)$;
- $sp_{RJst_\Sigma^a}(f)$ é o requisito de justiça para a.

O conjunto dos subproblemas para a explicação num passo de f *com base em* a é o conjunto constituído pelas fórmulas anteriores e denota-se por $Sp_a(f)$.

Para cada $a' \in Acc$, o *conjunto das garantias induzidas por* $Sp_a(f)$ *relativamente à acção* a', $Gr_{a'}(Sp_a(f))$, define-se como sendo o conjunto

$$Gr_{a'}(Sp(sp_{seg}(f))) \cup C$$

onde $C = \{sp_{\nabla a}(f)\}$ se $a' = a$ e $C = \emptyset$ caso contrário.

No que se segue, dada a especificação de objecto eob, por *explicação para* $sp_{\nabla a}(f)$ *em* eob entende-se um conjunto $\{f_a\}$ onde f_a é explicação para a garantia de q_2 a partir de $q_1 \wedge (\neg q_2)$ por a em eob. ∎

O subproblema $sp_{\nabla a}(f)$ corresponde à garantia de q_2 a partir de $q_1 \wedge (\neg q_2)$ por a em eob. Neste contexto, quando se pretende uma explicação com base em a isto significa que a é responsável pela satisfação de q_2. A sua ocorrência estabelecerá q_2. Se a já satisfaz esta garantia em eob não é necessária, como é óbvio, nenhuma explicação para $sp_{\nabla a}(f)$. Caso contrário, explicações para a garantia de q_2 a partir de $q_1 \wedge (\neg q_2)$ em eob permitem restringir a ocorrência da acção a por forma a que se tenha tal garantia. Neste caso, as restrições de activação que contribuem para a garantia pretendida porque impedem a ocorrência de a (como, por exemplo, $\mathbf{G}(\diamond a \Rightarrow \mathbf{f})$ ou análogas à restrição de activação mencionada no Exemplo 3.39) não têm obviamente nenhuma utilidade e nunca poderão fazer parte de nenhuma explicação para o problema de resposta em causa.

Proposição 3.86 Sejam $f = \mathbf{G}(r \Rightarrow (q_1 \,\mathbf{U}\, q_2))$ um problema de resposta em eob e $a \in Acc$. Seja

$$X = \{sp \in Sp_a(f) \colon eob \not\models sp\}$$

e para cada $sp \in X' = X \setminus \{sp_{\diamond a}(f), sp_{RJst^a_\Sigma}(f)\}$ seja E_{sp} uma explicação para sp em eob. Se

$$E = (\bigcup_{sp \in X'} E_{sp}) \cup (X \cap \{sp_{\diamond a}(f), sp_{RJst^a_\Sigma}(f)\})$$

é eob-possível então E é uma explicação para o problema $\mathbf{G}(r \Rightarrow (q_1 \,\mathbf{U}\, q_2))$ em eob.

Prova: Seja eob' o enriquecimento de eob com E e $f = \mathbf{G}(r \Rightarrow (q_1 \,\mathbf{U}\, q_2))$.

(a) Tem-se que $eob \models sp$ para todo $sp \in Sp_a(f)$ tal que $sp \notin X$.

Seja $sp \in X$. Se $sp \in \{sp_{RJst^a_\Sigma}(f), sp_{\diamond a}(f)\}$ então trivialmente $eob' \models sp$. Se $sp = sp_{\nabla a}(f)$, e sendo eob'' o enriquecimento de eob com E_{sp}, pela Definição 3.7, $eob'' \models sp$ e portanto $eob' \models sp$. Se $sp = sp_{seg}(f)$, e sendo eob'' o enriquecimento de eob com E_{sp}, pela Definição 3.4, $eob'' \models sp$ e novamente $eob' \models sp$.

Conclui-se assim, pela Proposição 3.83, que $eob' \models \mathbf{G}(r \Rightarrow (q_1 \,\mathbf{U}\, q_2))$.

(b) Pelas Definições 2.22 e 2.23, dado que E é eob-possível, tem-se que eob' é coerente.

(c) Por (a), (b) e Definição 3.4, E é uma explicação para $\mathbf{G}(r \Rightarrow (q_1 \,\mathbf{U}\, q_2))$. ∎

Observação 3.87 Seja $f = \mathbf{G}(r \Rightarrow (q_1 \,\mathbf{U}\, q_2))$ um problema de resposta em eob. Como é natural, se $q_1 \wedge (\neg q_2)$ é equivalente a $p \in CE_\Sigma$ então, no contexto da Proposição 3.86, $sp_{\diamond a}(f) \in Sp_a(f)$ pode ser substituída nos conjuntos X e E por $\mathbf{G}(p \Rightarrow \diamond a)$. ∎

Exemplo 3.88 Considere-se a especificação de objecto eob_3 descrita no Exemplo 3.46. A fórmula

$$f = \mathbf{G}(y \Rightarrow (z\, \mathbf{U}\, u))$$

é um problema de resposta em eob_3. Pretende-se encontrar explicações num passo com base em a_2.

1. Tem-se que $sp_{seg}(f) = \mathbf{G}(y \Rightarrow (z\, \mathbf{W}\, u))$ e $eob_3 \not\models sp_{seg}(f)$. No Exemplo 3.81 foi encontrada uma explicação para o problema $sp_{seg}(f)$ em eob_3.

2. Tem-se que $sp_{\nabla a_2}(f) = \mathbf{G}((\nabla a_2 \wedge z \wedge (\neg u)) \Rightarrow (\mathbf{X}(z \vee u)))$ e $eob_3 \models sp_{\nabla a_2}(f)$.

3. Tem-se que $sp_{\diamond a_2}(f) = \mathbf{G}((z \wedge (\neg u)) \Rightarrow \diamond a_2)$ e $eob_3 \not\models sp_{\diamond a_2}(f)$.

4. Tem-se que $eob_3 \not\models sp_{RJst^{a_2}_{\Sigma_3}}(f)$.

5. O conjunto

$$E = \{z \vee u,\ \mathbf{G}(\diamond a_1 \Rightarrow (x \vee (\neg z) \vee u)),\ \mathbf{G}(\diamond a_2 \Rightarrow z),$$
$$\mathbf{G}((z \wedge (\neg u)) \Rightarrow \diamond a_2),\ (\mathbf{G}(\mathbf{F}\diamond a_2)) \Rightarrow (\mathbf{G}(\mathbf{F}\nabla a_2))\}$$

é explicação para o problema de resposta $\mathbf{G}(y \Rightarrow (z\, \mathbf{U}\, u))$ num passo com base em a_2.

No Exemplo 3.81 foram construídas explicações para o problema $\mathbf{G}(y \Rightarrow (z\, \mathbf{W}\, u))$ em eob_3. A segunda estrutura de interpretação representada na Figura 3.12, no âmbito do referido exemplo, já não é modelo do enriquecimento de eob_3 com a explicação E que aqui se construiu para o problema $\mathbf{G}(y \Rightarrow (z\, \mathbf{U}\, u))$ em eob_3. Nessa estrutura de interpretação a_2 nunca ocorre apesar de o constrangimento de estado $z \wedge (\neg u)$ ser sempre satisfeito e, consequentemente, a_2 estar sempre activada. ∎

Sejam $f = \mathbf{G}(r \Rightarrow (q_1\, \mathbf{U}\, q_2))$ e $a \in Acc$. Relativamente a critérios de preferência no âmbito da construção de explicações em um passo com base em a para f, são aplicáveis os critérios anteriormente referidos, nomeadamente no que diz respeito à construção de explicações associadas a $sp_{seg}(f)$ e $sp_{\nabla a}(f)$. Neste caso, sendo $a' \in Acc$, o conjunto $Gr_{a'}(Sp_a(f))$ poderá ter três fórmulas. Quando nenhuma delas fôr satisfeita por eob, uma forma de encontrar uma única restrição de activação relativa a a' que assegure as garantias em $Gr_{a'}(Sp_a(f))$ é uma simples generalização daquela que foi indicada anteriormente no âmbito dos problemas de segurança. Mais detalhes sobre esta generalização podem ser encontrados no final da próxima subsubsecção.

3.5.2.2 Explicações em vários passos

Nesta subsubsecção descreve-se o modo de construir explicações em vários passos para problemas de resposta em eob.

Proposição 3.89 Se existem $p_0, \ldots, p_n \in CE^{\mathbf{tf}}_{\Sigma}$, onde $n \geq 1$ e $p_0 = q_2$, e $a_1, \ldots, a_n \in Acc$ tais que

(i) $eob \models \mathbf{G}(r \Rightarrow (q_2 \vee (q_1 \wedge (p_0 \vee \ldots \vee p_n))))$,

(ii) para cada $1 \leq i \leq n$

– $eob \models \mathbf{G}((q_1 \wedge p_i \wedge (\neg q_2)) \Rightarrow (\mathbf{X}(q_2 \vee (q_1 \wedge (p_0 \vee \ldots \vee p_i)))))$,
– $eob \models \mathbf{G}((\triangledown a_i \wedge q_1 \wedge p_i \wedge (\neg q_2)) \Rightarrow (\mathbf{X}(q_2 \vee (q_1 \wedge (p_0 \vee \ldots \vee p_{i-1})))))$,
– $eob \models \mathbf{G}((q_1 \wedge p_i \wedge (\neg q_2)) \Rightarrow \diamond a_i)$,
– $eob \models RJst^{a_i}_{\Sigma}$,

então $eob \models \mathbf{G}(r \Rightarrow (q_1 \, \mathbf{U} \, q_2))$.

Prova: Seja λ modelo de eob e seja $k \in I\!N_0$ tal que $\lambda, k \models r$. Pela hipótese (i) tem-se que $\lambda, k \models q_2 \vee (q_1 \wedge (p_0 \vee \ldots \vee p_n))$.

(a) Se $\lambda, k \models q_2$, então $\lambda, k \models q_1 \, \mathbf{U} \, q_2$.

(b) Suponha-se que $\lambda, k \not\models q_2$. Então, $\lambda, k \models q_1 \wedge p_i$ para algum $1 \leq i \leq n$. Na alínea (b.i) prova-se um resultado intermédio e na alínea (b.ii) prova-se que $\lambda, k \models q_1 \, \mathbf{U} \, q_2$.

(b.i) Prova-se seguidamente que se para algum $1 \leq j \leq n$ existe $k_j \in I\!N_0$ tal que $\lambda, k_j \models q_1 \wedge p_j \wedge (\neg q_2)$ então $\lambda, k_j \models (q_1 \wedge p_j \wedge (\neg q_2)) \, \mathbf{U} \, (q_2 \vee (q_1 \wedge (p_0 \vee \ldots \vee p_{j-1})))$.

(b.i.i) Suponha-se, por absurdo, que $\lambda, k' \models (\neg q_2) \wedge ((\neg q_1) \vee ((\neg p_0) \wedge \ldots \wedge (\neg (p_{j-1}))))$ para todo $k' \geq k_j$.

Prova-se por indução em k' que $\lambda, k' \models q_1 \wedge p_j \wedge (\neg q_2)$ para todo $k' \geq k_j$.

Base: $k' = k_j$. O resultado verifica-se por hipótese.

Passo: $k' \geq k_j$. Por hipótese de indução, $\lambda, k' \models q_1 \wedge p_j \wedge (\neg q_2)$. Pela primeira condição da hipótese (ii), $\lambda, k'+1 \models q_2 \vee (q_1 \wedge (p_0 \vee \ldots \vee p_j))$. A assumpção (b.i.i) leva a que se tenha necessariamente que $\lambda, k'+1 \models q_1 \wedge p_j \wedge (\neg q_2)$.

Estabelecido este resultado, a terceira condição da hipótese (ii) permite agora concluir que $\lambda, k' \models \diamond a_j$ para todo $k' \geq k_j$. Assim, $\lambda, k_j \models \mathbf{G}(\diamond a_j)$ e $\lambda, 0 \models \mathbf{G}(\mathbf{F}(\diamond a_j))$. Tendo em conta a quarta condição da hipótese (ii) tem-se que $\lambda, 0 \models \mathbf{G}(\mathbf{F}(\triangledown a_j))$ e portanto existe $k' \geq k_j$ tal que $\lambda, k' \models \triangledown a_j$. Pela segunda condição da hipótese (ii), $\lambda, k'+1 \models q_2 \vee (q_1 \wedge (p_0 \vee \ldots \vee p_{j-1}))$ contradizendo a assumpção (b.i.i).

(b.i.ii) Suponha-se agora, novamente por absurdo, que existe $k' \geq k_j$ tal que $\lambda, k' \models q_2 \vee (q_1 \wedge (p_0 \vee \ldots \vee p_{j-1})))$ mas que para todos k' nestas condições existe $k_j \leq k'' < k'$ tal que $\lambda, k'' \models (\neg q_1) \vee (\neg p_j) \vee q_2$.

Seja k'' o menor natural tal que $k'' \geq k_j$ e $\lambda, k'' \models (\neg q_1) \vee (\neg p_j) \vee q_2$. Tem-se que $k'' \neq k_j$ e $\lambda, k''-1 \models q_1 \wedge p_j \wedge (\neg q_2)$. Pela primeira condição da hipótese (ii) tem-se que $\lambda, k'' \models q_2 \vee (q_1 \wedge (p_0 \vee \ldots \vee p_j)))$. Se $\lambda, k'' \models q_2$ então $\lambda, k'' \models q_2 \vee (q_1 \wedge (p_0 \vee \ldots \vee p_{j-1})))$ e, pela definição de k'', $\lambda, k''' \models q_1 \wedge p_j \wedge (\neg q_2)$ para todo $k_j \leq k''' < k''$ o que contradiz a assumpção (b.i.ii). Se $\lambda, k'' \not\models q_2$ então $\lambda, k'' \models q_1 \wedge (p_0 \vee \ldots \vee p_j)$, e, dado que $\lambda, k'' \models (\neg q_1) \vee (\neg p_j)$, tem-se que $\lambda, k'' \models q_1 \wedge (p_0 \vee \ldots \vee p_{j-1})$ e, obviamente, $\lambda, k'' \models q_2 \vee (q_1 \wedge (p_0 \vee \ldots \vee p_{j-1}))$. Novamente se chega a uma contradição com a assumpção (b.i.ii).

De (b.i.i) e (b.i.ii) conclui-se que se $k_j \in I\!N_0$ é tal que verifica $\lambda, k_j \models q_1 \wedge p_j \wedge (\neg q_2)$ para algum $1 \leq j \leq n$ então $\lambda, k_j \models (q_1 \wedge p_j \wedge (\neg q_2)) \, \mathbf{U} \, (q_2 \vee (q_1 \wedge (p_0 \vee \ldots \vee p_{j-1})))$.

(b.ii) Prova-se agora que $\lambda, k \models q_1 \, \mathbf{U} \, q_2$. Recorde-se que $\lambda, k \models q_1 \wedge p_i \wedge (\neg q_2)$ para certo $1 \leq i \leq n$. Suponha-se, por absurdo, que $\lambda, k \not\models q_1 \, \mathbf{U} \, q_2$.

(b.ii.i) Prova-se por indução em k' que para todo $k' \geq k$: (1) existe $0 < j' \leq i$ tal que $\lambda, k' \models q_1 \wedge p_{j'} \wedge (\neg q_2)$, (2) qualquer que seja $0 < j' \leq i$ tal que $\lambda, k' \models q_1 \wedge p_{j'} \wedge (\neg q_2)$

existem $k'' \geq k'$ e $0 < j'' < j'$ tal que $\lambda, k'' \models q_1 \wedge p_{j''} \wedge (\neg q_2)$ e (3) $\lambda, k''' \models q_1$ para todo $k \leq k''' < k'$.

Base: $k' = k$. Por hipótese, $\lambda, k' \models q_1 \wedge p_i \wedge (\neg q_2)$ e portanto tem-se (1). Seja $0 < j' \leq i$ tal que $\lambda, k' \models q_1 \wedge p_{j'} \wedge (\neg q_2)$. Por (b.i), $\lambda, k' \models (q_1 \wedge p_{j'} \wedge (\neg q_2)) \mathbf{U}\, q_2$ ou $\lambda, k' \models (q_1 \wedge p_{j'} \wedge (\neg q_2)) \mathbf{U}\, (q_1 \wedge p_{j''} \wedge (\neg q_2))$ com $0 < j'' < j'$. O primeiro caso contradiz a assumpção $\lambda, k \not\models q_1 \mathbf{U}\, q_2$. Assim tem-se necessariamente o segundo caso do qual decorre que k' satisfaz a condição (2). A condição (3) é satisfeita vacuosamente.

Passo: seja $k' > k$. Por hipótese de indução existe $0 < \overline{j} \leq i$ tal que $\lambda, k' - 1 \models q_1 \wedge p_{\overline{j}} \wedge (\neg q_2)$. Pela primeira condição da hipótese (ii) alguma das duas asserções seguintes é satisfeita: $\lambda, k' \models q_2$ ou $\lambda, k' \models q_1 \wedge p_{j'} \wedge (\neg q_2)$ com $0 < j' \leq \overline{j} \leq i$. Se $\lambda, k' \models q_2$, uma vez que, por hipótese de indução, $k' - 1$ satisfaz a condição (3), tem-se que $\lambda, k \models q_1 \mathbf{U}\, q_2$ o que contradiz a assumpção $\lambda, k \not\models q_1 \mathbf{U}\, q_2$. Se $\lambda, k' \models q_1 \wedge p_{j'} \wedge (\neg q_2)$ com $0 < j' \leq i$ então k' satisfaz a condição (1) e, dado que $k' - 1$ satisfaz a condição (3), k' também satisfaz a condição (3). Sendo $0 < j' \leq i$ tal que $\lambda, k' \models q_1 \wedge p_{j'} \wedge (\neg q_2)$, por (b.i), $\lambda, k' \models (q_1 \wedge p_{j'} \wedge (\neg q_2)) \mathbf{U}\, q_2$ ou $\lambda, k' \models (q_1 \wedge p_{j'} \wedge (\neg q_2)) \mathbf{U}\, (q_1 \wedge p_{j''} \wedge (\neg q_2))$ com $0 < j'' < j'$. No primeiro caso, dado que k' satisfaz a condição (3), então $\lambda, k \models q_1 \mathbf{U}\, q_2$ o que contradiz a assumpção $\lambda, k \not\models q_1 \mathbf{U}\, q_2$. Assim tem-se necessariamente o segundo caso do qual decorre que k' satisfaz a condição (2).

(b.ii.ii) Por (b.ii.i) é possível construir duas sucessões de naturais $k_0, k_1, \ldots, k_n, \ldots$ e $j_0, j_1, \ldots, j_n, \ldots$ tais que, para cada $n \geq 0$, $\lambda, k_n \models q_1 \wedge p_{j_n} \wedge (\neg q_2)$ com $0 < j_n \leq i$, $k_0 = k$, $j_0 = i$, $k_{n+1} \geq k_n$ e $j_{n+1} < j_n$. Chega-se a uma contradição porque $j_0, j_1, \ldots, j_n, \ldots$ é uma sucessão de naturais estritamente decrescente.

De (b.ii.i) e (b.ii.ii) conclui-se então que $\lambda, k \models q_1 \mathbf{U}\, q_2$.

(c) De (a) e (b) resulta que $\lambda, k \models r \Rightarrow (q_1 \mathbf{U}\, q_2)$, logo $\lambda \models \mathbf{G}(r \Rightarrow (q_1 \mathbf{U}\, q_2))$ e portanto $eob \models \mathbf{G}(r \Rightarrow (q_1 \mathbf{U}\, q_2))$. ■

Corolário 3.90 Se existem $p_0, \ldots, p_n \in CE_{\Sigma}^{\mathbf{tf}}$, onde $n \geq 1$ e $p_0 = q$, e $a_1, \ldots, a_n \in Acc$ tais que

(i) $eob \models \mathbf{G}(r \Rightarrow (q \vee (p_0 \vee \ldots \vee p_n)))$,

(ii) para cada $1 \leq i \leq n$

- $eob \models \mathbf{G}((p_i \wedge (\neg q)) \Rightarrow (\mathbf{X}(q \vee (p_0 \vee \ldots \vee p_i))))$,
- $eob \models \mathbf{G}((\nabla a_i \wedge p_i \wedge (\neg q)) \Rightarrow (\mathbf{X}(q \vee (p_0 \vee \ldots \vee p_{i-1}))))$,
- $eob \models \mathbf{G}((p_i \wedge (\neg q)) \Rightarrow \diamond a_i)$,
- $eob \models RJst_{\Sigma}^{a_i}$,

então $eob \models \mathbf{G}(r \Rightarrow (\mathbf{F}\, q))$.

Prova: Pela Proposição 3.89 fazendo $q_1 = \mathbf{t}$ e $q_2 = q$. ■

A Proposição 3.89 mostra que se pode concluir que uma dada observação de resposta $\mathbf{G}(r \Rightarrow (q_1 \mathbf{U}\, q_2))$ é eob-válida a partir do conhecimento de que certas observações de segurança são eob-válidas e de que existem certas acções que vão contribuir para a verificação progressiva de determinados constrangimentos de estado. Suponha-se que um dado estado satisfaz o constrangimento de estado r. Os constrangimentos de estado $q_1 \wedge p_1, \ldots, q_1 \wedge p_n$ representam situações intermédias que irão sendo atingidas (não necessariamente todas) até se chegar a um estado que verifique $q_2(p_0)$.

Umas das obervações de segurança que tem de ser verificada está relacionada com a necessidade de assegurar que, sempre que r se verifica, então ou se verifica já q_2 ou então é satisfeita alguma das condições intermédias $q_1 \wedge p_i$ para algum $0 < i \leq n$.

As outras observações de segurança têm por objectivo assegurar que: se ainda se não tem q_2 mas já se atingiu um estado intermédio no qual $q_1 \wedge p_i$ para algum $0 < i \leq n$ se verifica, então o estado seguinte não corresponde a uma "pior" situação (face à desejada satisfação de q_2), isto é, ou se mantém a satisfação $q_1 \wedge p_i$ ou se está "mais perto" da satisfação de q_2 porque ou já se tem q_2 ou se tem $q_1 \wedge p_j$ para algum $0 < j < i$.

As asserções que envolvem explicitamente cada uma das acções a_i, $1 \leq i \leq n$, têm como objectivo assegurar que se se chegar a um estado que verifique a condição intermédia $q_1 \wedge p_i \wedge (\neg q_2)$, não é possível que esta seja continuamente satisfeita por todos os estados futuros, isto é, não é possível que a situção (face à desejada satisfação de q_2) não "melhore". Chegar-se-á a um estado, eventualmente através da ocorrência de a_i, correspondente a uma "melhor" situação, ou seja, a um estado no qual ou já se verifica q_2 ou se tem $q_1 \wedge p_j$ para algum $0 < j < i$.

Definição 3.91 Sejam $f = \mathbf{G}(r \Rightarrow (q_1 \, \mathbf{U} \, q_2)) \in O_\Sigma$, $p_0, \ldots, p_n \in CE_\Sigma^{\mathbf{tf}}$, com $n > 0$ e $p_0 = q_2$, e $a_1, \ldots, a_n \in Acc$. Os *subproblemas para a explicação em vários passos de f com base em $p_1, \ldots, p_n$ e $a_1, \ldots, a_n$* são as fórmulas

- $sp_{seg}(f) = \mathbf{G}(r \Rightarrow (q_2 \vee (q_1 \wedge (p_0 \vee \ldots \vee p_n))))$;
- $sp_{seg}^{p_i}(f) = \mathbf{G}((q_1 \wedge p_i \wedge (\neg q_2)) \Rightarrow (\mathbf{X}(q_2 \vee (q_1 \wedge (p_0 \vee \ldots \vee p_i))))))$ para cada $1 \leq i \leq n$;
- $sp_{\nabla a_i}(f) = \mathbf{G}((\nabla a_i \wedge q_1 \wedge p_i \wedge (\neg q_2)) \Rightarrow (\mathbf{X}(q_2 \vee (q_1 \wedge (p_0 \vee \ldots \vee p_{i-1}))))))$ para cada $1 \leq i \leq n$;
- $sp_{\diamond a_i}(f) = \mathbf{G}((q_1 \wedge p_i \wedge (\neg q_2)) \Rightarrow \diamond a_i)$ para cada $1 \leq i \leq n$;
- $sp_{RJst_\Sigma^{a_i}}(f)$ é o requisito de justiça para a_i para cada $1 \leq i \leq n$.

O conjunto dos subproblemas para a explicação em vários passo de f *com base em* $p_1, \ldots, p_n$ *e* $a_1, \ldots, a_n$ é o conjunto constituído pelas fórmulas anteriores e denota-se por $Sp_{a_1 \ldots a_n}^{p_1 \cdots p_n}(f)$.

Para cada $a' \in Acc$, o *conjunto das garantias induzidas por* $Sp_{a_1 \ldots a_n}^{p_1 \cdots p_n}(f)$ *relativamente à acção* a', $Gr_{a'}(Sp_{a_1 \ldots a_n}^{p_1 \cdots p_n}(f))$, define-se como sendo o conjunto

$$\{gr_{a'}(sp_{seg}(f))\} \cup (\textstyle\bigcup_{1 \leq i \leq n} \{gr_{a'}(sp_{seg}^{p_i}(f))\}) \cup C$$

onde $C = \{sp_{\nabla a_i}(f)\}$ se $a' = a_i$ para algum $1 \leq i \leq n$ e $C = \emptyset$ caso contrário.

No que se segue, dada a especificação *eob* e sendo $1 \leq i \leq n$, por *explicação para* $sp_{\nabla a_i}(f)$ em *eob* entende-se um conjunto $\{f_{a_i}\}$ onde f_{a_i} é explicação para a garantia de $q_2 \vee (q_1 \wedge (p_0 \vee \ldots \vee p_{i-1}))$ a partir de $q_1 \wedge p_i \wedge (\neg q_2)$ por a_i em *eob*. ■

Proposição 3.92 Seja $f = \mathbf{G}(r \Rightarrow (q_1 \mathbf{U}\, q_2))$ um problema de resposta em eob e sejam $p_0, \ldots, p_n \in CE_\Sigma^{\mathbf{tf}}$, com $n > 0$ e $p_0 = q_2$, e $a_1, \ldots, a_n \in Acc$. Seja

$$X = \{sp \in Sp_{a_1 \ldots a_n}^{p_1 \ldots p_n}(f) \colon eob \not\models sp\}$$

e para cada $sp \in X' = X \backslash (\bigcup_{1 \leq i \leq n} \{sp_{\diamond a_i}(f), sp_{RJst_\Sigma^{a_i}}(f)\})$ seja E_{sp} uma explicação para sp em eob. Se

$$E = (\bigcup_{sp \in X'} E_{sp}) \cup (X \cap (\bigcup_{1 \leq i \leq n} \{sp_{\diamond a_i}(f), sp_{RJst_\Sigma^{a_i}}(f)\}))$$

é eob-possível então E é uma explicação para o problema $\mathbf{G}(r \Rightarrow (q_1 \mathbf{U}\, q_2))$.

Prova: Sejam eob' o enriquecimento de eob com E e $f = \mathbf{G}(r \Rightarrow (q_1 \mathbf{U}\, q_2)))$.

(a) Tem-se que $eob \models sp$ para todo $sp \in Sp_{a_1 \ldots a_n}^{p_1 \ldots p_n}(f) \backslash X$.

Seja $sp \in X$. Se $sp \in \bigcup_{1 \leq i \leq n} \{sp_{\diamond a_i}(f), sp_{RJst_\Sigma^{a_i}}(f)\}$ então trivialmente $eob' \models sp$. Se $1 \leq i \leq n$ e $sp = sp_{\nabla a_i}(f)$, e sendo eob'' o enriquecimento de eob com E_{sp}, pela Definição 3.7, $eob'' \models sp$ e portanto $eob' \models sp$. Se $sp \in \{sp_{seg}(f)\} \cup \{sp_{seg}^{p_i}(f) : 1 \leq i \leq n\}$, e sendo eob'' o enriquecimento de eob com E_{sp}, pela Definição 3.4, $eob'' \models sp$ e novamente $eob' \models sp$.

Conclui-se assim, pela Proposição 3.89, que $eob' \models \mathbf{G}(r \Rightarrow (q_1 \mathbf{U}\, q_2))$.

(b) Pelas Definições 2.22 e 2.23, dado que E é eob-possível, tem-se que eob' é coerente.

(c) Por (a), (b) e Definição 3.4, E é uma explicação para $\mathbf{G}(r \Rightarrow (q_1 \mathbf{U}\, q_2))$. ■

Observação 3.93 Seja $f = \mathbf{G}(r \Rightarrow (q_1 \mathbf{U}\, q_2))$ um problema de resposta em eob. Como é natural, se para algum $1 \leq i \leq n$ a fórmula $q_1 \wedge p_i \wedge (\neg q_2)$ é equivalente a $q_i' \in CE_\Sigma$ então, no contexto da Proposição 3.92, $sp_{\diamond a_i}(f) \in Sp_{a_1 \ldots a_n}^{p_1 \ldots p_n}(f)$ pode ser substituída nos conjuntos X e E por $\mathbf{G}(q_i' \Rightarrow \diamond a_i)$. ■

Exemplo 3.94 Considere-se a especificação de objecto $eob_5 = (\Sigma_5, AxF_5, AxS_5)$ com

$$\Sigma_5 = (\{a_1, a_2, a_3\}, \{x, y, z, u\})$$

$$AxF_5 = \emptyset \qquad AxS_5 = \{\mathbf{G}((\nabla a_1 \wedge \alpha\,{}_x^z) \Rightarrow (\mathbf{X}\,\alpha)), \mathbf{G}((\nabla a_2 \wedge \alpha\,{}_x^y) \Rightarrow (\mathbf{X}\,\alpha)), \mathbf{G}((\nabla a_3 \wedge \alpha\,{}_{\neg u}^{u}) \Rightarrow (\mathbf{X}\,\alpha))\}$$

A fórmula $f = \mathbf{G}(x \Rightarrow (\mathbf{F}(x \wedge y \wedge z)))$ é um problema de resposta em eob_5.

Pretende-se encontrar explicações em vários passos com base em $p_1 = x \wedge y$, $p_2 = x$ e a_1, a_2. Sejam $q = x \wedge y \wedge z$ e, de acordo com a Proposição 3.92, $p_0 = q$. Note-se que neste caso $q_1 = \mathbf{t}$.

1. Tem-se que $sp_{seg}(f) = \mathbf{G}(x \Rightarrow (q \vee (p_0 \vee p_1 \vee p_2)))$ e $eob_5 \models sp_{seg}(f)$.

2. Tem-se que $sp_{seg}^{p_1}(f) = \mathbf{G}((p_1 \wedge (\neg q)) \Rightarrow (\mathbf{X}(q \vee p_1)))$ e $eob_5 \models sp_{seg}^{p_1}(f)$.

3. Tem-se que $sp_{seg}^{p_2}(f) = \mathbf{G}((p_2 \wedge (\neg q)) \Rightarrow (\mathbf{X}(q \vee p_1 \vee p_2)))$ e $eob_5 \models sp_{seg}^{p_2}(f)$.

4. Tem-se que $sp_{\nabla a_1}(f) = \mathbf{G}((\nabla a_1 \wedge p_1 \wedge (\neg q)) \Rightarrow (\mathbf{X}\,q))$ e $eob_5 \models sp_{\nabla a_1}(f)$.

5. Tem-se que $sp_{\nabla a_2}(f) = \mathbf{G}((\nabla a_2 \wedge p_2 \wedge (\neg q)) \Rightarrow (\mathbf{X}(q \vee p_1)))$ e $eob_5 \models sp_{\nabla a_2}(f)$.

6. Tem-se que $sp_{\diamond a_1}(f) = \mathbf{G}(((x \wedge y) \wedge (\neg(x \wedge y \wedge z))) \Rightarrow \diamond a_1)$ e $eob_5 \not\models sp_{\diamond a_1}(f)$.

7. Tem-se que $sp_{\diamond a_2}(f) = \mathbf{G}((x \wedge (\neg(x \wedge y \wedge z))) \Rightarrow \diamond a_2)$ e $eob_5 \not\models sp_{\diamond a_2}(f)$.

8. Tem-se que $eob_5 \not\models sp_{RJst^{a_1}_{\Sigma_5}}(f)$.

9. Tem-se que $eob_5 \not\models sp_{RJst^{a_2}_{\Sigma_5}}(f)$.

10. O conjunto

$$\{\mathbf{G}((x \wedge y \wedge (\neg z)) \Rightarrow \diamond a_1),\ \mathbf{G}((x \wedge ((\neg y) \vee (\neg z))) \Rightarrow \diamond a_2),$$
$$(\mathbf{G}(\mathbf{F} \diamond a_1)) \Rightarrow (\mathbf{G}(\mathbf{F} \triangledown a_1)),\ (\mathbf{G}(\mathbf{F} \diamond a_2)) \Rightarrow (\mathbf{G}(\mathbf{F} \triangledown a_2))\}$$

é explicação para $\mathbf{G}(x \Rightarrow (\mathbf{F}(x \wedge y \wedge z))$ tendo em conta a Observação 3.93.

11. Na Figura 3.15 está representado um fragmento de um possível modelo da especificação eob'_5 que se obtém enriquecendo eob_5 com a explicação referida em **10**. Para cada $0 \leq k \leq 5$ referem-se os atributos que são ou não satisfeitos.

$$\underset{(0)}{\boxed{\boldsymbol{x}, \neg y, \neg z, \neg u}} \xrightarrow{\triangledown a_3} \underset{(1)}{\boxed{x, \neg y, \neg z, u}} \xrightarrow{\triangledown a_2} \underset{(2)}{\boxed{x, y, \neg z, u}} \xrightarrow{\triangledown a_3} \underset{(3)}{\boxed{x, y, \neg z, \neg u}} \xrightarrow{\triangledown a_1} \underset{(4)}{\boxed{\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}, \neg u}}$$

$$\xrightarrow{\triangledown a_3} \underset{(5)}{\boxed{x, y, z, u}} \quad \ldots$$

Figura 3.15: Modelo de eob'_5

Não é possível, por exemplo, ter a partir do instante (2) apenas as ocorrências de a_2 e a_3 pois a_1 estaria sempre activado a partir desse instante e o requisito de justiça para a_1 não seria verificado. ∎

Exemplo 3.95 Considere-se a especificação de objecto $eob_6 = (\Sigma_6, AxF_6, AxS_6)$ com

$\Sigma_6 = (\{a_1, a_2, a_3\}, \{x, y, z\})$

$AxF_6 = \emptyset$

$$AxS_6 = \{\mathbf{G}((\triangledown a_1 \wedge \alpha\,{}^{z}_{\neg z}) \Rightarrow (\mathbf{X}\,\alpha)),$$
$$\mathbf{G}((\triangledown a_2 \wedge \alpha\,{}^{y}_{x}\,{}^{z}_{\neg x}) \Rightarrow (\mathbf{X}\,\alpha)),$$
$$\mathbf{G}((\triangledown a_3 \wedge \alpha\,{}^{x}_{\neg x}) \Rightarrow (\mathbf{X}\,\alpha))\}$$

A fórmula $f = \mathbf{G}(x \Rightarrow (\mathbf{F}(x \wedge y \wedge z)))$ é um problema de resposta em eob_6.

Pretende-se encontrar explicações em vários passos com base em $p_1 = x \wedge y$, $p_2 = x$ e a_1, a_2. Sejam $q = x \wedge y \wedge z$ e, de acordo com a Proposição 3.92, $p_0 = q$. Note-se que neste caso $q_1 = \mathbf{t}$.

1. Tem-se que $sp_{seg}(f) = \mathbf{G}(x \Rightarrow (q \vee (p_0 \vee p_1 \vee p_2)))$ e $eob_6 \models sp_{seg}(f)$.

2. Tem-se que $sp^{p_1}_{seg}(f) = \mathbf{G}((p_1 \wedge (\neg q)) \Rightarrow (\mathbf{X}(q \vee p_1)))$ e $eob_6 \not\models sp^{p_1}_{seg}(f)$.

2.1. As acções a_1 e a_2 garantem $q \vee p_1$ a partir de $p_1 \wedge (\neg q)$ em eob_6.

2.2. A acção a_3 não garante $q \vee p_1$ a partir de $p_1 \wedge (\neg q)$ em eob_6. Conclui-se que

$$min(Fc_{eob_6}^{p_1\wedge(\neg q)\overset{a_3}{\rightarrow} q\vee p_1}) = \{\{\neg x\},\{\neg y\},\{z\}\}$$

construindo um tableau de decisão em $T_{\Sigma_6}(G_{eob_6}^{p_1\wedge(\neg q)\overset{a_3}{\rightarrow} q\vee p_1})$.

3. Tem-se que $sp_{seg}^{p_2}(f) = \mathbf{G}((p_2 \wedge (\neg q)) \Rightarrow (\mathbf{X}(q \vee p_1 \vee p_2)))$ e $eob_6 \not\models sp_{seg}^{p_2}(f)$.

3.1. As acções a_1 e a_2 garantem $q \vee p_1 \vee p_2$ a partir de $p_2 \wedge (\neg q)$ em eob_6.

3.2. A acção a_3 não garante $q \vee p_1 \vee p_2$ a partir de $p_2 \wedge (\neg q)$ em eob_6. Conclui-se que

$$min(Fc_{eob_6}^{p_2\wedge(\neg q)\overset{a_3}{\rightarrow} q\vee p_1\vee p_2}) = \{\{\neg x\},\{y,z\}\}$$

construindo um tableau de decisão em $T_{\Sigma_6}(G_{eob_6}^{p_2\wedge(\neg q)\overset{a_3}{\rightarrow} q\vee p_1\vee p_2})$.

4. O conjunto $Gr_{a_3}(Sp_{a_1a_2}^{p_1p_2}(f))$ é constituído por três fórmulas das quais só uma, a fórmula $gr_{a_3}(sp_{seg}(f))$, é satisfeita por eob_6. Em **2.2** e **3.2** encontraram-se os fechos minimais dos tableaux associados à construção de explicações para as outras duas garantias em $Gr_{a_3}(Sp_{a_1a_2}^{p_1p_2}(f))$. O conjunto $\{y,z\} \notin Fc_{eob_6}^{p_1\wedge(\neg q)\overset{a_3}{\rightarrow} q\vee p_1}$ e portanto, neste caso, há restrições de activação em $E_{RActv}(Fc_{eob_6}^{p_2\wedge(\neg q)\overset{a_3}{\rightarrow} q\vee p_1\vee p_2})$ que não pertencem a $E_{RActv}(Fc_{eob_6}^{p_1\wedge(\neg q)\overset{a_3}{\rightarrow} q\vee p_1})$. Para construir uma restrição de activação que seja explicação para ambas as garantias pode proceder-se como foi indicado no final da subsecção 3.5.1: a partir dos fechos minimais indicados constrói-se o conjunto

$$F = \{\{\neg x\},\{\neg x, y, z\},\{\neg x,\neg y\},\{\neg x, z\},\{y,z\}\}$$

e considera-se a restrição de activação $\mathbf{G}(\diamond a_3 \Rightarrow ((\neg x) \vee (y \wedge z)))$ induzida pelo conjunto dos elementos minimais de F. Esta restrição de activação é eob_6-possível e portanto o conjunto

$$\{\mathbf{G}(\diamond a_3 \Rightarrow ((\neg x) \vee (y \wedge z)))\}$$

é explicação para as garantias referidas **2.2** e **3.2**. É também, neste caso, explicação para $sp_{seg}^{p_1}(f)$ e $sp_{seg}^{p_2}(f)$ em eob_6.

5. Tem-se que $sp_{\nabla a_1}(f) = \mathbf{G}((\nabla a_1 \wedge p_1 \wedge (\neg q)) \Rightarrow (\mathbf{X}\, q))$ e $eob_6 \models sp_{\nabla a_1}(f)$.

6. Tem-se que $sp_{\nabla a_2}(f) = \mathbf{G}((\nabla a_2 \wedge p_2 \wedge (\neg q)) \Rightarrow (\mathbf{X}(q \vee p_1)))$ e $eob_6 \models sp_{\nabla a_2}(f)$.

7. Tem-se que $sp_{\diamond a_1}(f) = \mathbf{G}(((x \wedge y) \wedge (\neg(x \wedge y \wedge z))) \Rightarrow \diamond a_1)$ e $eob_6 \not\models sp_{\diamond a_1}(f)$.

8. Tem-se que $sp_{\diamond a_2}(f) = \mathbf{G}((x \wedge (\neg(x \wedge y \wedge z))) \Rightarrow \diamond a_2)$ e $eob_6 \not\models sp_{\diamond a_2}(f)$.

9. Tem-se que $eob_6 \not\models sp_{RJst_{\Sigma_6}^{a_1}}(f)$.

10. Tem-se que $eob_6 \not\models sp_{RJst_{\Sigma_6}^{a_2}}(f)$.

11. O conjunto

$$\begin{aligned}&\{\mathbf{G}(\diamond a_3 \Rightarrow ((\neg x) \vee (y \wedge z)))\\ &\ \mathbf{G}((x \wedge y \wedge (\neg z)) \Rightarrow \diamond a_1),\ \mathbf{G}((x \wedge ((\neg y) \vee (\neg z))) \Rightarrow \diamond a_2),\\ &\ (\mathbf{G}(\mathbf{F}\diamond a_1)) \Rightarrow (\mathbf{G}(\mathbf{F}\nabla a_1)),\ (\mathbf{G}(\mathbf{F}\diamond a_2)) \Rightarrow (\mathbf{G}(\mathbf{F}\nabla a_2))\}\end{aligned}$$

$$\underset{(0)}{\boxed{\boldsymbol{x}, \neg y, \neg z}} \xrightarrow{\nabla a_1} \underset{(1)}{\boxed{\boldsymbol{x}, \neg y, z}} \xrightarrow{\nabla a_2} \underset{(2)}{\boxed{\boldsymbol{x},\boldsymbol{y}, \neg z}} \xrightarrow{\nabla a_1} \underset{(3)}{\boxed{\boldsymbol{x},\boldsymbol{y},\boldsymbol{z}}} \xrightarrow{\nabla a_3} \underset{(4)}{\boxed{\neg \boldsymbol{x}, y, z}} \xrightarrow{\nabla a_1} \underset{(5)}{\boxed{\neg \boldsymbol{x}, y, \neg z}} \ \ldots$$

Figura 3.16: Modelo de eob'_6

é explicação para $\mathbf{G}(x \Rightarrow (\mathbf{F}(x \wedge y \wedge z))$ tendo em conta a Observação 3.93.

12. Na Figura 3.16 está representado um fragmento de um possível modelo da especificação eob'_6 que se obtém enriquecendo eob_6 com a explicação descrita em **11**.

Para cada $0 \leq k \leq 5$ referem-se os atributos que são ou não satisfeitos. ■

Sejam $f = \mathbf{G}(r \Rightarrow (q_1 \mathbf{U}\, q_2))$, $a_1, \ldots, a_n \in Acc$ e $p_1, \ldots, p_n \in CE_\Sigma^{\mathbf{tf}}$. Relativamente a critérios de preferência no âmbito da construção de explicações para f em vários passos com base em $a_1, \ldots, a_n$ e $p_1, \ldots, p_n$, são aplicáveis os critérios anteriormente referidos, nomeadamente no que diz respeito à construção de explicações associadas a $sp_{seg}(f)$, $sp_{seg}^{p_i}(f)$ e $sp_{\nabla a_i}(f)$, $1 \leq i \leq n$.

Neste caso, sendo $a' \in Acc$, o conjunto $Gr_{a'}(Sp_{a_1 \ldots a_n}^{p_1 \cdots p_n}(f))$ poderá ter várias fórmulas. Pode generalizar-se a sugestão descrita no final da subsecção 3.5.1 para encontrar uma única restrição de activação que assegure as várias garantias em $Gr_{a'}(Sp_{a_1 \ldots a_n}^{p_1 \cdots p_n}(f))$. Suponha-se que existem $m \in I\!N$ garantias em $Gr_{a'}(Sp_{a_1 \ldots a_n}^{p_1 \cdots p_n}(f))$ que não são satisfeitas por eob e sejam: $t_1, \ldots, t_m$ os tableaux construídos para cada uma delas, $F_1, \ldots, F_m$, conjuntos (não vazios) de fechos de $t_1, \ldots, t_m$, respectivamente, $Fc_1^i \ldots Fc_{n_i}^i \in Enm(F_i)$ para cada $1 \leq i \leq m$ e

> *F o subconjunto de $\wp(LE_\Sigma)$ tal que $Fc \in F$ sse $Fc \cap \overline{F}c = \emptyset$ e, para cada $1 \leq i \leq m$, existe $1 \leq k_i \leq n_i$ tal que $Fc = \bigcup_{1 \leq i \leq m} Fc_{k_i}^i$.*

Conclui-se facilmente que *qualquer restrição de activação induzida por $F' \subseteq F$, se fôr eob-possível, é explicação para as m garantias em $Gr_a(Sp(f))$* que não são satisfeitas por eob. Se, em particular, F' é constituído pelos conjuntos minimais de F e f é restrição de activação induzida por F' então f é mais liberal que qualquer outra restrição de activação induzida por algum subconjunto de F.

3.5.3 Problemas de garantia

Nesta subsubsecção descreve-se o modo como explicações para problemas de garantia em eob podem ser obtidas. Tal como no caso de problemas de resposta existe a possibilidade de construir explicações num passo e a possibilidade de construir explicações em vários passos.

3.5.3.1 Explicações num passo

Nesta subsecção descreve-se o modo de construir explicações para problemas de garantia num passo.

Proposição 3.96 Se

(i) $eob \models r \Rightarrow (q_1 \mathbf{W}\, q_2)$,

(ii) existe $a \in Acc$ que tal que

– $eob \models \mathbf{G}((\nabla a \wedge q_1 \wedge (\neg q_2)) \Rightarrow (\mathbf{X}\, q_2))$,

– $eob \models \mathbf{G}((q_1 \wedge (\neg q_2)) \Rightarrow \diamond a)$,

– $eob \models RJst^a_\Sigma$,

então $eob \models r \Rightarrow (q_1 \mathbf{U}\, q_2)$.

Prova: Seja λ modelo de eob e suponha-se que $\lambda, 0 \models r$. A prova é semelhante à apresentada para a Proposição 3.83. ■

Definição 3.97 Seja $f = r \Rightarrow (q_1 \mathbf{U}\, q_2) \in O_\Sigma$ e $a \in Acc$. Os *subproblemas para a explicação num passo de f com base em a* são as fórmulas

- $sp_{seg}(f) = r \Rightarrow (q_1 \mathbf{W}\, q_2)$,
- $sp_{\nabla a}(f) = \mathbf{G}((\nabla a \wedge q_1 \wedge (\neg q_2)) \Rightarrow (\mathbf{X}\, q_2))$,
- $sp_{\diamond a}(f) = \mathbf{G}((q_1 \wedge (\neg q_2)) \Rightarrow \diamond a)$,
- $sp_{RJst^a_\Sigma}(f)$ é o requisito de justiça para a.

O conjunto dos subproblemas para a explicação num passo de f *com base em a*, $Sp_a(f)$, é o conjunto constituído pelas fórmulas anteriores.

As definições de conjunto das garantias induzidas por $Sp_a(f)$ relativamente à acção a' para cada $a' \in Acc$ e de explicações para $sp_{\nabla a}(f)$ em eob são análogas às apresentadas na Definição 3.85. ■

Proposição 3.98 Sejam $f = r \Rightarrow (q_1 \mathbf{U}\, q_2)$ um problema de garantia em eob e $a \in Acc$. Seja

$$X = \{sp \in Sp_a(f) \colon eob \not\models sp\}$$

e para cada $sp \in X' = X \setminus \{sp_{\diamond a}(f), sp_{RJst^a_\Sigma}(f)\}$ seja E_{sp} uma explicação para sp. Se

$$E = (\bigcup_{sp \in X'} E_{sp}) \cup (X \cap \{sp_{\diamond a}(f), sp_{RJst^a_\Sigma}(f)\})$$

é eob-possível então E é uma explicação para o problema $r \Rightarrow (q_1 \mathbf{U}\, q_2)$.

Prova: A prova é semelhante à apresentada para a Proposição 3.86 considerando agora a Proposição 3.97. ■

Observação 3.99 Seja $f = r \Rightarrow (q_1 \mathbf{U}\, q_2)$ um problema de garantia em eob. Se $q_1 \wedge (\neg q_2)$ é equivalente a $p \in CE_\Sigma$ então, no contexto da Proposição 3.98, $sp_{\diamond a}(f) \in Sp_a(f)$ pode ser substituída nos conjuntos X e E por $\mathbf{G}(p \Rightarrow \diamond a)$. ■

Exemplo 3.100 Considere-se a especificação de objecto eob_3 descrita no Exemplo 3.46. A fórmula

$$f = y \Rightarrow (z\,\mathbf{U}\,u)$$

é um problema de garantia em eob_3. Pretende-se encontrar explicações num passo com base em a_2.

1. Tem-se que $sp_{seg}(f) = y \Rightarrow (z\,\mathbf{W}\,u)$ e $eob_3 \not\models sp_{seg}(f)$. No Exemplo 3.76 foi calculada uma explicação para $sp_{seg}(f)$.

2. Tem-se que $sp_{\nabla a_2}(f) = \mathbf{G}((\nabla a_2 \wedge z \wedge (\neg u)) \Rightarrow (\mathbf{X}\,u))$ e $eob_3 \models sp_{\nabla a_2}(f)$.

3. Tem-se que $sp_{\diamond a_2}(f) = \mathbf{G}((z \wedge (\neg u)) \Rightarrow \diamond a_2)$ e $eob_3 \not\models sp_{\diamond a_2}(f)$.

4. Tem-se que $eob_3 \not\models sp_{RJst^{a_2}_{\Sigma_3}}(f)$.

5. O conjunto

$$\{z \vee u,\ \mathbf{G}(\diamond a_1 \Rightarrow (x \vee (\neg z) \vee u)),\ \mathbf{G}((z \wedge (\neg u)) \Rightarrow \diamond a_2),\ (\mathbf{G}(\mathbf{F}\,\diamond a_2)) \Rightarrow (\mathbf{G}(\mathbf{F}\,\nabla a_2))\}$$

é explicação para o problema de garantia $y \Rightarrow (z\,\mathbf{U}\,u)$ num passo com base em a_2.

6. Na Figura 3.17 encontra-se representado um fragmento de um modelo da especificação eob'_3 que se obtém enriquecendo eob_3 com a explicação apresentada em **5**. No instante inicial y é verdadeiro, u é verdadeiro em (3) e tem-se z verdadeiro desde o instante inicial até ao primeiro instante que verifica u. A especificação eob'_3 só verifica $y \Rightarrow (z\,\mathbf{U}\,u)$ no instante inicial pois em (4) y é verdadeiro mas aí já não se verifica $z\,\mathbf{U}\,u$.

$$\underset{(0)}{\boxed{\neg x, \boldsymbol{y}, \boldsymbol{z}, \neg u}} \xrightarrow{\nabla a_3} \underset{(1)}{\boxed{x, y, \boldsymbol{z}, \neg u}} \xrightarrow{\nabla a_1} \underset{(2)}{\boxed{x, \neg y, \boldsymbol{z}, \neg u}} \xrightarrow{\nabla a_2} \underset{(3)}{\boxed{x, y, \neg z, \boldsymbol{u}}} \xrightarrow{\nabla a_2} \underset{(4)}{\boxed{x, y, \neg z, \neg u}} \ \ldots$$

Figura 3.17: Modelo de eob'_3

Com o tipo de explicações que se constroem nunca se pode ter um modelo em que y seja satisfeito num certo instante $k > 0$, $z \wedge (\neg u)$ seja sempre satisfeito a partir desse instante e a_2 nunca ocorra. Esta situação não seria incompatível com a satisfação de $y \Rightarrow (z\,\mathbf{U}\,u)$ pela nova especificação mas nunca terá lugar nas especificações que se obtêm à custa das explicações aqui construídas. ■

Relativamente a critérios de preferência aplicam-se também aqui as considerações feitas anteriormente para o caso das explicações num passo para problemas de resposta.

3.5.3.2 Explicações em vários passos

Nesta subsubsecção descreve-se o modo de construir explicações em vários passos para problemas de garantia.

Proposição 3.101 Se existem $p_0, \ldots, p_n \in CE^{\mathbf{tf}}_{\Sigma}$, onde $n \geq 1$ e $p_0 = q_2$, e $a_1, \ldots, a_n \in Acc$ tais que

(i) $eob \models r \Rightarrow (q_2 \vee (q_1 \wedge (p_0 \vee \ldots \vee p_n)))$,

(ii) para cada $1 \leq i \leq n$

- $eob \models \mathbf{G}((q_1 \wedge p_i \wedge (\neg q_2)) \Rightarrow (\mathbf{X}(q_2 \vee (q_1 \wedge (p_0 \vee \ldots \vee p_i)))))$,
- $eob \models \mathbf{G}((\triangledown a_i \wedge q_1 \wedge p_i \wedge (\neg q_2)) \Rightarrow (\mathbf{X}(q_2 \vee (q_1 \wedge (p_0 \vee \ldots \vee p_{i-1})))))$,
- $eob \models \mathbf{G}((q_1 \wedge p_i \wedge (\neg q_2)) \Rightarrow \diamond a_i)$,
- $eob \models RJst_{\Sigma}^{a_i}$,

então $eob \models r \Rightarrow (q_1 \mathbf{U}\, q_2)$.

Prova: Seja λ modelo de eob e suponha-se que $\lambda, 0 \models r$. A prova é idêntica à prova apresentada para a Proposição 3.89. ■

Definição 3.102 Seja $f = r \Rightarrow (q_1 \mathbf{U}\, q_2) \in O_\Sigma$ e sejam $p_0, \ldots, p_n \in CE_{\Sigma}^{\mathbf{tf}}$, com $n > 0$ e $p_0 = q_2$, e $a_1, \ldots, a_n \in Acc$. Os *subproblemas para a explicação em vários passos de f com base em $p_1, \ldots, p_n$ e $a_1, \ldots, a_n$* são as fórmulas

- $sp_{CI}(f) = r \Rightarrow (q_2 \vee (q_1 \wedge (p_0 \vee \ldots \vee p_n)))$
- $sp_{seg}^{p_i}(f) = \mathbf{G}((q_1 \wedge p_i) \Rightarrow (\mathbf{X}(q_2 \vee (q_1 \wedge (p_0 \vee \ldots \vee p_i)))))$ para cada $1 \leq i \leq n$
- $sp_{\triangledown a_i}(f) = \mathbf{G}((\triangledown a_i \wedge q_1 \wedge p_i \wedge (\neg q_2)) \Rightarrow (\mathbf{X}(q_2 \vee (q_1 \wedge (p_0 \vee \ldots \vee p_{i-1})))))$ para cada $1 \leq i \leq n$
- $sp_{\diamond a_i}(f) = \mathbf{G}((q_1 \wedge p_i \wedge (\neg q_2)) \Rightarrow \diamond a_i)$ para cada $1 \leq i \leq n$
- $sp_{RJst_{\Sigma}^{a_i}}(f)$ é o requisito de justiça para a_i para cada $1 \leq i \leq n$.

O conjunto dos subproblemas para a explicação em vários passos de f *com base em* $p_1, \ldots, p_n$ *e* $a_1, \ldots, a_n$, $Sp_{a_1 \ldots a_n}^{p_1 \cdots p_n}(f)$, é o conjunto constituído pelas fórmulas anteriores.

Para cada $a' \in Acc$, o *conjunto das garantias induzidas por $Sp_{a_1 \ldots a_n}^{p_1 \cdots p_n}(f)$ relativamente à acção a'*, $Gr_{a'}(Sp_{a_1 \ldots a_n}^{p_1 \cdots p_n}(f))$, define-se como sendo o conjunto

$$\left(\bigcup_{1 \leq i \leq n} \{gr_{a'}(sp_{seg}^{p_i}(f))\}\right) \cup C$$

onde $C = \{sp_{\triangledown a_i}(f)\}$ se $a' = a_i$ para algum $1 \leq i \leq n$ e $C = \emptyset$ caso contrário.

No que se segue, dada a especificação de objecto eob: por *explicação para $sp_{CI}(f)$ em eob* entende-se um conjunto $\{f_{CI}\}$ onde f_{CI} é explicação para a garantia inicial de $q_2 \vee (q_1 \wedge (p_0 \vee \ldots \vee p_n))$ em eob; para cada $1 \leq i \leq n$, por *explicação para $sp_{\triangledown a_i}(f)$ em eob* entende-se um conjunto $\{f_{a_i}\}$ onde f_{a_i} é explicação para a garantia de $q_2 \vee (q_1 \wedge (p_0 \vee \ldots \vee p_{i-1}))$ a partir de $q_1 \wedge p_i \wedge (\neg q_2)$ por a_i em eob. ■

Proposição 3.103 Seja $f = r \Rightarrow (q_1 \mathbf{U}\, q_2)$ um problema de garantia em eob e, sendo $n > 0$ e $p_0 = q_2$, sejam $p_0, \ldots, p_n \in CE_{\Sigma}^{\mathbf{tf}}$, e $a_1, \ldots, a_n \in Acc$. Seja

$$X = \{sp \in Sp_{a_1 \ldots a_n}^{p_1 \cdots p_n}(f) \colon eob \not\models sp\}$$

e para cada $sp \in X' = X \backslash (\bigcup_{1\leq i\leq n}\{sp_{\diamond a_i}(f), sp_{RJst^{a_i}_{\Sigma}}(f)\})$ seja E_{sp} uma explicação para sp. Se

$$E = (\bigcup_{sp\in X'} E_{sp}) \cup (X \cap (\bigcup_{1\leq i\leq n}\{sp_{\diamond a_i}(f), sp_{RJst^{a_i}_{\Sigma}}(f)\}))$$

é *eob*-possível então E é uma explicação para o problema $r \Rightarrow (q_1 \mathbf{U}\, q_2)$.

Prova: A prova é semelhante à prova apresentada para a Proposição 3.92 recorrendo agora à Proposição 3.101 e Definição 3.102. ■

Observação 3.104 Seja $f = r \Rightarrow (q_1 \mathbf{U}\, q_2)$ um problema de garantia em *eob*. Se para algum $1 \leq i \leq n$ a fórmula $q_1 \wedge p_i \wedge (\neg q_2)$ é equivalente a $q'_i \in CE_{\Sigma}$ então, no contexto da Proposição 3.103, $sp_{\diamond a_i}(f) \in Sp^{p_1\cdots p_n}_{a_1\ldots a_n}(f)$ pode ser substituída nos conjuntos X e E por $\mathbf{G}(q'_i \Rightarrow \diamond a_i)$. ■

Relativamente a critérios de preferência aplicam-se aqui as considerações feitas anteriormente para o caso das explicações em vários passos para problemas de resposta.

3.5.4 Problemas de persistência

As explicações para este tipo de problema são encontradas à custa de explicações para um problema de segurança e para um problema de resposta. Uma vez que foram apresentadas diversas formas de encontrar explicações para problemas de resposta, a escolha do modo como se calculam explicações para o problema de resposta inerente a um problema de persistência levará a diferentes tipos de explicações para este problema.

Proposição 3.105 Se

(i) $eob \models \mathbf{G}(q \Rightarrow (\mathbf{X}\, q))$,

(ii) $eob \models \mathbf{G}(r \Rightarrow (\mathbf{F}\, q))$,

então $eob \models \mathbf{G}(r \Rightarrow (\mathbf{F}(\mathbf{G}\, q)))$

Prova: Seja λ modelo de *eob* e $k_1 \in I\!N_0$ tal que $\lambda, k_1 \models r$. Pela hipótese (ii), $\lambda, k_2 \models q$ para algum $k_2 \geq k_1$.

(a) Prova-se por indução em k que para todo $k \geq k_2$, $\lambda, k \models q$.

Base: se $k = k_2$ a afirmação é verdadeira.

Passo: $k \geq k_2$. Por hipótese de indução $\lambda, k \models q$ e, Pela hipótese (i), $\lambda, k \models q \Rightarrow (\mathbf{X}\, q)$. Consequentemente $\lambda, k+1 \models q$.

(b) Tem-se que $\lambda, k_2 \models \mathbf{G}\, q$ e portanto $\lambda, k_1 \models \mathbf{F}(\mathbf{G}\, q)$. Assim $\lambda \models \mathbf{G}(r \Rightarrow (\mathbf{F}(\mathbf{G}\, q)))$ e, consequentemente, $eob \models \mathbf{G}(r \Rightarrow (\mathbf{F}(\mathbf{G}\, q)))$. ■

Definição 3.106 Seja $f = \mathbf{G}(r \Rightarrow (\mathbf{F}(\mathbf{G}\, q))) \in O_{\Sigma}$. Os *subproblemas para a explicação de* f são as fórmulas

- $sp_{seg}(f) = \mathbf{G}(q \Rightarrow (\mathbf{X}\, q))$;

- $sp_{resp}(f) = \mathbf{G}(r \Rightarrow (\mathbf{F}\, q))$.

O conjunto dos subproblemas para a explicação de f, $Sp(f)$, é o conjunto constituído pelas fórmulas anteriores.

Para cada $a \in Acc$, o *conjunto das garantias induzidas por $Sp(f)$ relativamente à acção a*, $Gr_a(Sp(f))$, define-se como sendo o conjunto

$$\{gr_a(sp_{seg}(f))\} \cup C$$

onde $C = Gr_a(Sp_{a'}(sp_{resp}(f)))$ quando se consideram subproblemas para a explicação num passo $sp_{resp}(f)$ com base na acção $a' \in Acc$ e $C = Gr_a(Sp^{p_1 \ldots p_n}_{a_1 \ldots a_n}(sp_{resp}(f)))$ quando se consideram subproblemas para a explicação em vários passos de $sp_{resp}(f)$ com base $p_1, \ldots, p_n \in CE_\Sigma$ e $a_1, \ldots, a_n \in Acc$. ∎

Proposição 3.107 Seja $f = \mathbf{G}(r \Rightarrow \mathbf{F}(\mathbf{G}(q)))$ um problema de persistência em eob. Seja

$$X = \{sp \in Sp(f) \colon eob \not\models sp\}$$

e para cada $sp \in X$ seja E_{sp} uma explicação para sp. Se

$$E = \bigcup_{sp \in X} E_{sp}$$

é eob-possível então E é uma explicação para o problema $\mathbf{G}(r \Rightarrow \mathbf{F}(\mathbf{G}(q)))$.

Prova: A prova é semelhante à apresentada para a Proposição 3.80, recorrendo à Definição 3.106 e Proposição 3.105. ∎

Exemplo 3.108 Considere-se a especificação de objecto $eob_7 = (\Sigma_7, AxF_7, AxS_7)$ com

$$\Sigma_7 = (\{a_1, a_2, a_3, a_4, a_5\}, \{x, y, z, u, v\})$$

$$AxF_7 = \{x, \neg y, \neg z\}$$

$$\begin{aligned} AxS_7 = \{&\mathbf{G}((\nabla a_1 \wedge \alpha\,{}^{z}_{\neg z}) \Rightarrow (\mathbf{X}\,\alpha)),\\ &\mathbf{G}((\nabla a_2 \wedge \alpha\,{}^{y}_{x}\,{}^{z}_{\neg x}) \Rightarrow (\mathbf{X}\,\alpha)),\\ &\mathbf{G}((\nabla a_3 \wedge \alpha\,{}^{x}_{\neg x}) \Rightarrow (\mathbf{X}\,\alpha)),\\ &\mathbf{G}((\nabla a_4 \wedge \alpha\,{}^{\neg u}_{u}) \Rightarrow (\mathbf{X}\,\alpha)),\\ &\mathbf{G}((\nabla a_5 \wedge \alpha\,{}^{\neg v}_{v}) \Rightarrow (\mathbf{X}\,\alpha))\} \end{aligned}$$

A fórmula $f = \mathbf{G}(x \Rightarrow (\mathbf{F}(\mathbf{G}(x \wedge y \wedge z))))$ é um problema de persistência em eob_7.

1. Tem-se que $sp_{seg}(f) = \mathbf{G}((x \wedge y \wedge z) \Rightarrow (\mathbf{X}(x \wedge y \wedge z)))$ e $eob_7 \not\models sp_{seg}(f)$.

1.1. A acção a_1 não preserva $x \wedge y \wedge z$ em eob_7. Conclui-se que

$$min(Fc_{eob_7}^{x \wedge y \wedge z \xrightarrow{a_1} x \wedge y \wedge z}) = \{\{\neg x\}, \{\neg y\}, \{\neg z\}\}$$

construindo um tableau de decisão em $T_{\Sigma_7}(G_{eob_7}^{x \wedge y \wedge z \xrightarrow{a_1} x \wedge y \wedge z})$. É explicação para a garantia de preservação de $x \wedge y \wedge z$ por a_1 a restrição de activação $\mathbf{G}(\diamond a_1 \Rightarrow ((\neg x) \vee (\neg y) \vee (\neg z)))$.

1.2. A acção a_2 não preserva $x \wedge y \wedge z$ em eob_7. Conclui-se que

$$min(Fc_{eob_7}^{x\wedge y\wedge z \xrightarrow{a_2} x\wedge y\wedge z)}) = \{\{\neg x\}, \{\neg y\}, \{\neg z\}\}$$

construindo um tableau de decisão em $T_{\Sigma_7}(G_{eob_7}^{x\wedge y\wedge z \xrightarrow{a_2} x\wedge y\wedge z)})$. É explicação para a garantia de preservação de $x \wedge y \wedge z$ por a_2 a restrição de activação $\mathbf{G}(\diamond a_2 \Rightarrow ((\neg x) \vee (\neg y) \vee (\neg z)))$.

1.3. A acção a_3 não preserva $x \wedge y \wedge z$ em eob_7. Conclui-se que

$$min(Fc_{eob_7}^{x\wedge y\wedge z \xrightarrow{a_3} x\wedge y\wedge z)}) = \{\{\neg x\}, \{\neg y\}, \{\neg z\}\}$$

construindo um tableau de decisão em $T_{\Sigma_7}(G_{eob_7}^{x\wedge y\wedge z \xrightarrow{a_3} x\wedge y\wedge z)})$.

1.4. As acções a_4 e a_5 preservam $x \wedge y \wedge z$ em eob_7.

2. Tem-se que $sp_{resp}(f) = \mathbf{G}(x \Rightarrow (\mathbf{F}(x \wedge y \wedge z)))$ e $eob_7 \not\models sp_{resp}(f)$. Pretende-se encontar explicações com base em $p_1 = x \wedge y$, $p_2 = x$ e a_1, a_2. Sejam $q = x \wedge y \wedge z$ e, de acordo com a Proposição 3.92, $p_0 = q$. Note-se que neste caso $q_1 = \mathbf{t}$. Seja ainda $f' = sp_{resp}(f)$.

2.1. Tem-se que $sp_{seg}(f') = \mathbf{G}(x \Rightarrow (q \vee (p_0 \vee p_1 \vee p_2)))$ e $eob_7 \models sp_{seg}(f)$.

2.2. Tem-se que $eob_7 \models sp_{\nabla a_1}(f')$ e $eob_7 \models sp_{\nabla a_2}(f')$.

2.3. Tem-se que $sp_{\diamond a_1}(f') = \mathbf{G}(((x \wedge y) \wedge (\neg(x \wedge y \wedge z))) \Rightarrow \diamond a_1)$ e $eob_7 \not\models sp_{\diamond a_1}(f')$.

2.4. Tem-se que $sp_{\diamond a_2}(f') = \mathbf{G}((x \wedge (\neg(x \wedge y \wedge z)) \Rightarrow \diamond a_2)$ e $eob_7 \not\models sp_{\diamond a_2}(f')$.

2.5. Tem-se que $eob_7 \not\models sp_{RJst_{\Sigma_7}^{a_1}}(f')$.

2.6. Tem-se que $eob_7 \not\models sp_{RJst_{\Sigma_7}^{a_2}}(f')$.

2.7. Tem-se que $sp_{seg}^{p_1}(f') = \mathbf{G}((p_1 \wedge (\neg q)) \Rightarrow (\mathbf{X}(q \vee p_1)))$ e $eob_7 \not\models sp_{seg}^{p_1}(f')$.

2.7.1. As acções a_1, a_2, a_4 e a_5 garantem $q \vee p_1$ a partir de $p_1 \wedge (\neg q)$ em eob_7.

2.7.2. A acção a_3 não garante $q \vee p_1$ a partir de $p_1 \wedge (\neg q)$. Conclui-se que

$$min(Fc_{eob_7}^{p_1\wedge(\neg q) \xrightarrow{a_3} q\vee p_1}) = \{\{\neg x\}, \{\neg y\}, \{z\}\}$$

construindo um tableau de decisão em $T_{\Sigma_7}(G_{eob_7}^{p_1\wedge(\neg q) \xrightarrow{a_3} q\vee p_1})$.

2.8. Tem-se que $sp_{seg}^{p_2}(f') = \mathbf{G}((p_2 \wedge (\neg q)) \Rightarrow (\mathbf{X}(q \vee p_1 \vee p_2)))$ e $eob_7 \not\models sp_{seg}^{p_2}(f')$.

2.8.1. As acções a_1, a_2, a_4 e a_5 garantem $q \vee p_1 \vee p_2$ a partir de $p_2 \wedge (\neg q)$ em eob_7.

2.8.2. A acção a_3 não garante $q \vee p_1 \vee p_2$ a partir de $p_2 \wedge (\neg q)$ em eob_7. Conclui-se que

$$min(Fc_{eob_7}^{p_2\wedge(\neg q) \xrightarrow{a_3} q\vee p_1\vee p_2}) = \{\{\neg x\}, \{y, z\}\}$$

construindo um tableau de decisão em $T_{\Sigma_7}(G_{eob_7}^{p_2\wedge(\neg q) \xrightarrow{a_3} q\vee p_1\vee p_2})$.

3. O conjunto $Gr_{a_3}(Sp(f))$ contém três fórmulas que não são satisfeitas por eob_7. A partir dos fechos indicados em **1.3**, **2.7.2** e **2.8.2** e procedendo da forma sugerida no final da subsubsecção 3.5.2.2, obtém-se, a restrição de activação $\mathbf{G}(\diamond a_3 \Rightarrow (\neg x))$ a qual é eob_7-possível e assegura as três garantias em $Gr_{a_3}(Sp(f))$.

4. O conjunto

$$E_1 = \{\mathbf{G}(\diamond a_1 \Rightarrow ((\neg x) \vee (\neg y) \vee (\neg z))),\ \mathbf{G}(\diamond a_2 \Rightarrow ((\neg x) \vee (\neg y) \vee (\neg z))),\ \mathbf{G}(\diamond a_3 \Rightarrow (\neg x))\}$$

é explicação para $sp_{seg}(f)$ em eob_7.

5. O conjunto

$$\begin{aligned} E_2 = \{&\mathbf{G}(\diamond a_3 \Rightarrow (\neg x)),\\ &\mathbf{G}((x \wedge y \wedge (\neg z)) \Rightarrow \diamond a_1),\ \mathbf{G}((x \wedge ((\neg y \vee (\neg z))) \Rightarrow \diamond a_2),\\ &(\mathbf{G}(\mathbf{F}\diamond a_1)) \Rightarrow \mathbf{G}(\mathbf{F}\,\nabla a_1),\ (\mathbf{G}(\mathbf{F}\diamond a_2)) \Rightarrow \mathbf{G}(\mathbf{F}\,\nabla a_2)\} \end{aligned}$$

é explicação para $sp_{resp}(f)$ em eob_7.

6. O conjunto

$$E_1 \cup E_2$$

é explicação para o problema de persistência $\mathbf{G}(x \Rightarrow (\mathbf{F}(\mathbf{G}(x \wedge y \wedge z))))$.

7. Na Figura 3.18 encontra-se representado um fragmento de um modelo da especificação eob_7' que se obtém enriquecendo eob_7 com a explicação apresentada em **6**.

$$\underset{(0)}{\boxed{\boldsymbol{x}, \neg y, \neg z, u, v}} \xrightarrow{\nabla a_4} \underset{(1)}{\boxed{x, \neg y, \neg z, \neg u, v}} \xrightarrow{\nabla a_1} \underset{(2)}{\boxed{x, \neg y, z, \neg u, v}} \xrightarrow{\nabla a_1} \underset{(3)}{\boxed{x, \neg y, \neg z, \neg u, v}}$$

$$\xrightarrow{\nabla a_4} \underset{(4)}{\boxed{x, \neg y, \neg z, u, v}} \xrightarrow{\nabla a_2} \underset{(5)}{\boxed{x, y, \neg z, u, v}} \xrightarrow{\nabla a_1} \underset{(6)}{\boxed{\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}, u, v}} \xrightarrow{\nabla a_5} \underset{(7)}{\boxed{\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}, u, \neg v}}$$

$$\xrightarrow{\nabla a_4} \underset{(8)}{\boxed{\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}, \neg u, v}} \quad \ldots$$

Figura 3.18: Modelo de eob_7'

Para cada $0 \leq k \leq 8$ referem-se os atributos que são ou não satisfeitos. ∎

Note-se que as explicações que se propõem para problemas de persistência $\mathbf{G}(r \Rightarrow (\mathbf{F}(\mathbf{G}\,q)))$ não contemplam explicações, também possíveis para este tipo de problema, em que q seja satisfeito num certo instante k, deixe de ser satisfeito num certo instante $k' > k$ e só a partir de um outro instante $k'' > k'$ seja continuamente satisfeito. As explicações aqui consideradas são tais que assim que q seja satisfeito pela primeira vez então ter-se-á q em todos os instantes ulteriores.

Dado que as explicações para problemas de persistência se constroem à custa de explicações para problemas de segurança e de resposta, critérios de preferência a ter em conta para as explicações para problemas de persistência serão aqueles a que se fez referências nas subsecções 3.5.1 e 3.5.2.

3.6 Conclusões

Neste capítulo foi analisado o problema da verificação no âmbito de uma especificação de objecto de um ângulo que não tem vindo a ser não explorado na literatura: o raciocínio abdutivo sobre uma especificação.

Tradicionalmente, o problema de verificação consiste no desenvolvimento de métodos que permitam averiguar se o comportamento prescrito por uma especificação de objecto verifica ou não uma dada propriedade. Ao raciocinar abdutivamente sobre uma certa especificação de objecto, se o comportamento prescrito pela especificação não verifica uma dada propriedade pode dizer-se que se tem um problema de abdução. Face a um problema de abdução, o que se pretende é encontrar uma ou mais explicações para o problema, ou seja, encontrar um ou mais conjuntos de novos axiomas com os quais se possa enriquecer a especificação por forma a conseguir assegurar a referida propriedade. Ao longo deste capítulo foram descritas técnicas para a construção de explicações para problemas de abdução em especificações de objectos como as descritas no Capítulo 2.

As noções usualmente envolvidas nas tarefas de raciocínio abdutivo são vistas neste particular contexto do seguinte modo: a especificação de objecto desempenha o papel da (apresentação de) teoria que descreve a informação de que já se dispõe sobre o domínio em estudo, isto é, neste caso, o comportamento do objecto; fórmulas caracterizando propriedades relativas ao comportamento do objecto são as observações; constrangimentos de estado, restrições de activação e requisitos de justiça são as fórmulas abdutíveis. Seria também possível considerar os esquemas de valoração como fórmulas abdutíveis. Nesse caso os novos axiomas representariam não só novas restrições à ocorrências das acções mas também uma alteração às modificações que a ocorrência das acções opera nos valores dos atributos. Nesta dissertação não é tratado este caso.

Seguindo a classificação de propriedades relevantes na especificação do comportamento de sistemas reactivos apresentada, em particular, em [41, 42], foram considerados vários tipos de observações: observações de segurança, observações de resposta, observações de garantia e observações de persistência.

A construção das explicações teve por base: (i) técnicas conhecidas na literatura para verificação de propriedades de segurança e propriedades de resposta e animação no âmbito da especificação do comportamento de sistemas reactivos [39, 41, 43] e (ii) a análise (inspirada no trabalho desenvolvido em [45] para raciocínio abdutivo na lógica proposicional) de determinados tableaux proposicionais. As técnicas mencionadas em (i) são constituídas por regras que permitem concluir que as referidas propriedades são verificadas sempre que se verificarem um certo número de premissas mais simples. Estas regras foram aqui adaptadas para o caso particular das especificações de objectos consideradas.

As regras resultantes da referida adaptação incluem, em particular, premissas que exigem a verificação de certas condições iniciais e premissas que exigem a garantia de certos constrangimentos de estado a partir de outros constrangimentos através de acções. Sempre que alguma dessas premissas não é verificada pela especificação, mostrou-se como se constroem fórmulas que vão contribuir para as explicações: (i) é construído um tableau de decisão para um determinado conjunto de fórmulas proposicionais obtido a partir do problema em causa e dos axiomas e axiomas-esquema da especificação; (ii) a partir dos literais presentes nas etiquetas dos ramos abertos desse tableau constroem-se várias fórmulas (constrangimentos de estado ou restrições de activação de tipo 1, conforme o tipo de premissa) que vão contribuir para a construção de diferentes explicações.

Outro tipo de premissas que fazem parte das referidas regras (no caso de propriedades de resposta, garantia e persistência) são as restrições de activação de tipo 2 e os requisitos de justiça. Sempre que estas premissas não são verificadas elas são incluídas directamente nas potenciais explicações.

Os conjuntos de fórmulas obtidas da forma que se acabou de descrever só são de facto explicações se ao enriquecer com eles a especifcação dada se obtêm especificações coerentes. Tal como geralmente acontece nos vários métodos de geração de explicações para problemas de abdução que se encontram na literatura, os conjuntos obtidos após esta fase da construção de explicações não conduzem necessariamente a especificações coerentes. Assim, após esta fase há que passar a uma fase de teste à coerência para determinar quais deles são de facto explicações. Para tal pode recorrer-se aos tableaux temporais referidos no Capítulo 2.

A questão da selecção de explicações foi também analisada. Dado que as técnicas de construção de explicações descritas conduzem geralmente a diferentes explicações, foram mencionados e justificados alguns critérios de selecção de explicações.

Ao longo deste capítulo foram apresentados diversos exemplos ilustrativos das técnicas descritas.

Capítulo 4

Raciocínio abdutivo sobre comunidades de objectos

4.1 Introdução

O objectivo deste capítulo é desenvolver um trabalho semelhante ao apresentado no capítulo anterior mas agora no âmbito de especificações de comunidades de objectos. Uma comunidade de objectos é vista como um conjunto de objectos que comunicam entre si. Os problemas de abdução que neste caso se pretende considerar estão relacionados com propriedades relativas ao comportamento conjunto de vários objectos da comunidade.

Na linha do trabalho desenvolvido em [60, 61], os diferentes objectos de uma comunidade comunicam entre si através da ocorrência das respectivas acções: sob certas condições a ocorrência de uma acção de um certo objecto induz a ocorrência (simultânea) de uma acção de um outro objecto. A especificação desta interacção entre objectos é feita através de fórmulas que envolvem símbolos de acção de ambos os objectos. Como é óbvio, estas fórmulas não se podem escrever exclusivamente a partir da assinatura de um dos objectos. Surge assim a noção de objecto composto cuja assinatura é obtida a partir das assinaturas dos objectos (ditos primários) envolvidos na interacção. A partir desta assinatura já é possível escrever as fórmulas desejadas.

A especificação de uma comunidade de objectos estabelece identificadores e assinaturas para os objectos. Inclui também famílias de conjuntos de fórmulas e famílias de conjuntos de fórmulas-esquema. A assinatura de cada objecto introduz as acções e atributos exclusivos desse objecto. Cada conjunto de fórmulas agrupa as fórmulas associadas a um determinado objecto o mesmo acontecendo com os conjuntos de fórmulas-esquema.

É ainda a partir da noção de objecto composto e respectiva assinatura que é possível a escrita de fórmulas que exprimem propriedades relativas ao comportamento conjunto de vários objectos da comunidade. As propriedades consideradas são novamente classificadas como propriedades de segurança, propriedades de resposta, propriedades de garantia e propriedades de persistência. O problema da verificação de tais propriedades, no âmbito do objecto composto considerado, pode ser tratado de um modo análogo ao apresentado no capítulo anterior. Quando tais propriedades não são satisfeitas tem-se um problema de abdução, no âmbito do objecto composto considerado, para o qual se pretende encontrar explicações. Estas explicações podem incluir, tal como anteriormente, novas condições iniciais, novas restrições de activação e novos requisitos de justiça pertencentes às linguagens dos objectos primários envolvidos. No entanto, neste âmbito, podem ainda incluir novas fórmulas de interacção.

As explicações construídas não são conjuntos de fórmulas, como no capítulo anterior, mas sim famílias de conjuntos de fórmulas. Cada conjunto agrupa as fórmulas da linguagem associada a cada objecto.

As técnicas para geração de explicações são semelhantes às apresentadas no capítulo anterior tendo em conta que agora existem também fórmulas de interacção. Deste modo, os conjuntos de constrangimentos de estado para os quais se constroem os tableaux de decisão que contribuem para a geração das explicações têm agora uma componente relacionada com as fórmulas de interacção especificadas. Os referidos constrangimentos de estado são fórmulas da linguagem de um objecto composto. Consequentemente, os fechos destes tableaux são constituídos por literais provenientes dos vários objectos primários envolvidos. É a partir destes fechos que se constroem, em particular, as novas condições iniciais na linguagem dos vários objectos envolvidos. Para construir uma particular condição inicial que contribua de facto para uma explicação (assegurando uma determinada garantia inicial) não é possível em geral, neste âmbito, tomar vários fechos simultaneamente. Deste modo, as novas condições iniciais são necessariamente conjunções de literais e não disjunções de conjunções de literais como no caso local. Comentários semelhantes se podem fazer relativamente à geração de novas restrições de activação no que respeita aos constrangimentos de estado envolvidos nessas restrições.

À semelhança do que foi proposto anteriormente para o caso local, são discutidos alguns critérios para selecção das explicações geradas pelas técnicas apresentadas.

Este capítulo está organizado da forma que seguidamente se descreve. Nas secções 4.2, 4.3 e 4.4 apresentam-se as noções sintácticas e semânticas relativas à especificação de comunidades de objectos e são apresentados alguns resultados auxiliares. Na secção 4.5 introduzem-se as noções de problema de abdução no âmbito de uma comunidade de objectos e de explicação para tais problemas de abdução. Na secção 4.6 descreve-se a construção de restrições de activação e de fórmulas de interacção que permitem assegurar a garantia de um constrangimento de estado a partir de outro constrangimento de estado por um conjunto de acções. Na secção 4.7 descreve-se a construção de constrangimentos de estado que asseguram a verificação de uma dada condição inicial. Na secção 4.8 mostra-se como se constroem explicações para os problemas apresentados na secção 4.5. Os problemas de segurança são tratados na subsecção 4.8.1, os de resposta na subsecção 4.8.2, os de garantia na subsecção 4.8.3 e os de persistência na subsecção 4.8.4. Na secção 4.9 apresentam-se as conclusões. Ao longo do capítulo são apresentados exemplos que ilustram as ténicas abdutivas descritas. Optou-se também aqui por apresentar uma especificaçãode comunidade de objectos simples e que permitisse ir ilustrando as técnicas relativas às diferentes propriedades analisadas.

4.2 Assinatura

Nesta secção apresenta-se a noção de assinatura de comunidade de objectos. São também introduzidas a noção de fórmula de interacção e uma generalização da noção de esquema de valoração.

A noção de assinatura de comunidade de objectos, bem assim como as noções de estrutura de interpretação de comunidade de objectos e de especificação de comunidade de objectos que serão apresentadas nas secções que se seguem, são baseadas no trabalho desenvolvido em [60, 61] aqui adaptadas/simplificadas ao caso em que não considera a existência de classes de objectos.

Seja P um conjunto finito e não vazio. No que se segue denota-se por C_P o conjunto $\wp(P)\backslash\{\emptyset\}$. Cada $ob \in C_P$ representa um identificador de objecto; ob representa um identificador de objecto primário se é conjunto singular e representa um identificador de objecto composto caso contrário.

Notação 4.1 Para simplificar a notação, no seguimento identificar-se-á em muitas situações o identificador de objecto primário $\{i\}$ com i. ∎

Definição 4.2 Uma *assinatura de objecto* sobre o conjunto finito e não vazio P é um triplo

$$(ob, Acc, Atr)$$

onde

- $ob \in C_P$;
- Acc é um conjunto finito tal que $\perp \in Acc$ se ob é singular; os elementos de Acc dizem-se *símbolos de acção* ou *acções* e $\perp$ diz-se *símbolo de acção (acção) nula*;
- Atr é um conjunto finito cujos elementos são designados por *símbolos de atributo* ou *atributos*;
- $Acc \cap Atr = \emptyset$.

Denota-se por $AsnOb_P$ o conjunto de todas as assinaturas de objecto sobre P. ∎

Exemplo 4.3 Seja $P = \{1, 2, 3, 4\}$. Os tuplos

- $(1, Acc_1, Atr_1)$ onde $Acc_1 = \{a, b, c, \perp\}$ e $Atr_1 = \{x, y, z\}$,
- $(2, Acc_2, Atr_2)$ onde $Acc_2 = \{a, d, e, \perp\}$ e $Atr_2 = \{z, u\}$,
- $(3, Acc_3, Atr_3)$ onde $Acc_3 = \{c, e, \perp\}$ e $Atr_3 = \{x, w\}$,
- $(4, Acc_4, Atr_4)$ onde $Acc_4 = \{a, c, \perp\}$ e $Atr_4 = \{y, u\}$,

são exemplos de assinaturas de objecto sobre P. ■

Definição 4.4 Uma *assinatura de comunidade de objectos* é um par

$$\Sigma_{com} = (P, Asn)$$

onde P é um conjunto finito e não vazio e $Asn : C_P \to AsnOb_P$ é uma função tal que se $ob \in C_P$ é não singular então

$$Asn(ob) = (ob, \bigcup_{i \in ob} \{a^i : a \in Acc_i\}, \bigcup_{i \in ob} \{a^i : a \in Atr_i\})$$

sendo $Asn(i) = (i, Acc_i, Atr_i)$ para cada $i \in ob$. No que se segue, para cada $ob \in C_P$ a assinatura de objecto $Asn(ob)$ será denotada por Σ^{ob}_{com}. ■

Exemplo 4.5 Seja P como no Exemplo 4.3. Seja $\Sigma_{com} = (P, Asn)$ uma assinatura de comunidade de objectos tal que $\Sigma^i_{com} = (i, Acc_i, Atr_i)$, para cada $1 \leq i \leq 4$, é definida como no referido exemplo. Tem-se, em particular, que

$$\Sigma^{\{1,2\}}_{com} = (\{1, 2\}, Acc, Atr)$$

onde $Acc = \{a^1, b^1, c^1, \perp^1, a^2, d^2, \perp^2\}$ e $Atr = \{x^1, y^1, z^1, z^2, u^2\}$. ■

No que resta desta secção assume-se fixada a assinatura de comunidade de objectos $\Sigma_{com} = (P, Asn)$.

Lema 4.6 Sejam $ob \in C_P$ não singular, $\Sigma^{ob}_{com} = (ob, Acc, Atr)$, $\Sigma^i_{com} = (i, Acc_i, Atr_i)$ para cada $i \in ob$ e $i_1 \ldots i_n \in Enm(ob)$.

1. O tuplo $(Acc, (\sigma^{i_1}_{ob})_{Acc}, \ldots, (\sigma^{i_n}_{ob})_{Acc})$, onde, para cada natural $1 \leq j \leq n$, se tem que $(\sigma^{i_j}_{ob})_{Acc} : Acc_{i_j} \to Acc$ é a função tal que $(\sigma^{i_j}_{ob})_{Acc}(a) = a^{i_j}$ para cada $a \in Acc_{i_j}$, é coproduto de $Acc_{i_1}, \ldots, Acc_{i_n}$ na categoria Set.

2. O tuplo $(Atr, (\sigma^{i_1}_{ob})_{Atr}, \ldots, (\sigma^{i_n}_{ob})_{Atr})$, onde, para cada natural $1 \leq j \leq n$, se tem que $(\sigma^{i_j}_{ob})_{Atr} : Acc_{i_j} \to Atr$ é a função tal que $(\sigma^{i_j}_{ob})_{Atr}(o) = o^{i_j}$ para cada $o \in Atr_{i_j}$, é coproduto de $Atr_{i_1}, \ldots, Atr_{i_n}$ na categoria Set. ■

Observação 4.7 Para facilitar a exposição introduzem-se a seguintes convenções, sendo $ob, ob' \in C_P$, $\Sigma^{ob}_{com} = (ob, Acc, Atr)$ e $\Sigma^{ob'}_{com} = (ob', Acc', Atr')$:

- designa-se também por acção nula cada acção $\perp^i \in Acc$ com $i \in ob$ quando ob é não singular;

- sendo ob e ob' não singulares e tais que $ob \subseteq ob'$, considera-se a existência das inclusões $(\sigma^{ob}_{ob'})_{Acc} : Acc \to Acc'$ e $(\sigma^{ob}_{ob'})_{Atr} : Atr \to Atr'$;

- se $ob = ob'$ as funções identidade em Acc e Atr são denotadas por $(\sigma^{ob}_{ob})_{Acc}$ ou $(id_{ob})_{Acc}$ e $(\sigma^{ob}_{ob})_{Atr}$ ou $(id_{ob})_{Atr}$, respectivamente;

- dado que $(\sigma^{ob}_{ob'})^{-1}_{Acc}(a')$ e $(\sigma^{ob}_{ob'})^{-1}_{Atr}(o')$ são conjuntos singulares para cada símbolo $a' \in (\sigma^{ob}_{ob'})_{Acc}(Acc)$ e cada símbolo $o' \in (\sigma^{ob}_{ob'})_{Atr}(Atr)$ identifica-se $(\sigma^{ob}_{ob'})^{-1}_{Acc}(a')$ com o elemento que o constitui, o mesmo se passando com $(\sigma^{ob}_{ob'})^{-1}_{Atr}(o')$. ∎

Definição 4.8 Sejam $ob \in C_P$ e $\Sigma^{ob}_{com} = (ob, Acc, Atr)$. O conjunto das *fórmulas* sobre Σ^{ob}_{com}, F_{ob}, define-se indutivamente a partir de Acc e Atr como na Definição 2.2. ∎

Definição 4.9 Sejam $ob, ob' \in C_P$ tal que $ob \subseteq ob'$, $\Sigma^{ob}_{com} = (ob, Acc, Atr)$ e $\Sigma^{ob'}_{com} = (ob', Acc', Atr')$. A *função tradução* $(\sigma^{ob}_{ob'})_F : F_{ob} \to F_{ob'}$ é definida indutivamente como se segue

- $(\sigma^{ob}_{ob'})_F(\mathbf{t}) = \mathbf{t}$, $(\sigma^{ob}_{ob'})_F(\mathbf{f}) = \mathbf{f}$;
- $(\sigma^{ob}_{ob'})_F(\triangledown a) = \triangledown(\sigma^{ob}_{ob'})_{Acc}(a)$ e $(\sigma^{ob}_{ob'})_F(\diamond a) = \diamond(\sigma^{ob}_{ob'})_{Acc}(a)$ para cada $a \in Acc$;
- $(\sigma^{ob}_{ob'})_F(o) = (\sigma^{ob}_{ob'})_{Atr}(o)$ para cada $o \in Atr$;
- $(\sigma^{ob}_{ob'})_F(\neg f) = \neg(\sigma^{ob}_{ob'})_F(f)$, $(\sigma^{ob}_{ob'})_F(f \wedge f') = (\sigma^{ob}_{ob'})_F(f) \wedge (\sigma^{ob}_{ob'})_F(f')$ quaisquer que sejam $f, f' \in F_{ob}$;
- $(\sigma^{ob}_{ob'})_F(\mathbf{X}\, f) = \mathbf{X}(\sigma^{ob}_{ob'})_F(f)$ e $(\sigma^{ob}_{ob'})_F(f\ \mathbf{U}\ f') = (\sigma^{ob}_{ob'})_F(f)\ \mathbf{U}\ (\sigma^{ob}_{ob'})_F(f')$ quaisquer que sejam $f, f' \in F_{ob}$. ∎

Tendo em conta o Lema 4.6 e a Observação 4.7. facilmente se conclui que se ob não é singular ou $ob = ob'$ então $(\sigma^{ob}_{ob'})_F(f) = f$ para qualquer $f \in F_{ob}$.

Consideram-se as abreviaturas de fórmulas introduzidas nos capítulos anteriores bem como as noções de complexidade de fórmula, de subfórmula, de constrangimento de estado, de literal e literal de estado. O mesmo se passa ainda com as noções de condição inicial, de requisito de justiça, de restrição de activação de ambos os tipos e de substituição de atributos por constrangimentos de estado num dado constrangimento de estado.

Relativamente a notações mantêm-se genericamente as introduzidas nos capítulos anteriores. No entanto, no que respeita à referência à assinatura nas notações e sempre que não haja ambiguidade sobre a assinatura de comunidade em causa, em vez de Σ^{ob}_{com} usa-se, simplesmente, ob. No caso do conjuntos dos constrangimentos de estado, por exemplo, em vez de, em coerência com a notação introduzida no Capítulo 2, se utilizar $CE^{\mathbf{tf}}_{\Sigma^{ob}_{com}}$, usa-se simplesmente $CE^{\mathbf{tf}}_{ob}$.

A noção de esquema de valoração é generalizada a $n \in I\!N$ acções.

Definição 4.10 Sejam $ob \in C_P$ e $\Sigma^{ob}_{com} = (ob, Acc, Atr)$. Sejam $A \subseteq Acc$ não vazio, $a_1, \ldots, a_n \in Enm(A)$, $p_1, \ldots, p_m \in CE^{\mathbf{tf}}_{ob}$ e $o_1, \ldots, o_m \in Atr$ onde $m > 0$ e $o_i \neq o_j$ para quaisquer $1 \leq i, j \leq m$, $i \neq j$.

$$\mathbf{G}((\triangledown a_1 \wedge \ldots \wedge \triangledown a_n \wedge \alpha) \Rightarrow (\mathbf{X}\,\alpha)) \text{ e } \mathbf{G}((\triangledown a_1 \wedge \ldots \wedge \triangledown a_n \wedge \alpha^{o_1 \ldots o_m}_{p_1 \ldots p_m}) \Rightarrow (\mathbf{X}\,\alpha))$$

dizem-se *esquemas de valoração* para A. S^A_{ob} é o conjunto dos esquemas de valoração para A e $S_{ob} = \{S^A_{ob} : A \subseteq Acc,\ A \neq \emptyset\}$. Sempre que $A = \{a\}$ mantém-se a notação S^a_{ob}.

Sendo $q \in CE^{\mathbf{tf}}_{ob}$, a *instância-q* dos esquemas de valoração anteriores é, respectivamente,

$$\mathbf{G}((\triangledown a_1 \wedge \ldots \wedge \triangledown a_n \wedge q) \Rightarrow (\mathbf{X}\, q)) \text{ e } \mathbf{G}((\triangledown a_1 \wedge \ldots \wedge \triangledown a_n \wedge q^{o_1 \ldots o_m}_{p_1 \ldots p_m}) \Rightarrow (\mathbf{X}\, q)).$$

A função $\iota : \wp(S_{ob}) \times \wp(CE^{\mathbf{tf}}_{ob}) \to \wp(F_{ob})$ tal que

$$\iota(S, C) = \{f \in F_{ob} : f \text{ é a instância-}q \text{ de } s \in S \text{ e } q \in C\}$$

para cada $S \subseteq S_{ob}$ e $C \subseteq CE^{\mathbf{tf}}_{ob}$ diz-se *função instanciação.* ∎

Ao longo deste capítulo far-se-á algumas vezes referência a fórmulas $q^{o_1 \ldots o_m}_{p_1 \ldots p_m}$ e a esquemas de valoração $\mathbf{G}((\triangledown a_1 \wedge \ldots \wedge \triangledown a_n \wedge \alpha^{o_1 \ldots o_m}_{p_1 \ldots p_m}) \Rightarrow (\mathbf{X}\, \alpha))$ onde se assume genericamente que $m \in I\!N_0$. O caso $m = 0$ deverá ser entendido como a fórmula q e o esquema $\mathbf{G}((\triangledown a_1 \wedge \ldots \wedge \triangledown a_n \wedge \alpha) \Rightarrow (\mathbf{X}\, \alpha))$, respectivamente.

Ao longo do capítulo será ainda necessária a noção que se segue.

Definição 4.11 Sejam $ob \in C_P$, $\Sigma^{ob}_{com} = (ob, Acc, Atr)$ e $\Sigma^{i}_{com} = (i, Acc_i, Atr_i)$ para cada $i \in ob$. O conjunto $A \subseteq Acc$ diz-se *acção composta* sse $A \cap (\sigma^{i}_{ob})_{Acc}(Acc_i)$ é um conjunto singular para cada $i \in ob$. Para cada $i \in ob$, a acção em $A \cap (\sigma^{i}_{ob})_{Acc}(Acc_i)$ diz-se $\{i\}$*-acção de* A ou i*-acção de* A e denota-se por a^A_i ou $a^A_{\{i\}}$.

ACC_{ob} denota o conjunto de todas as acções compostas contidas em Acc. ∎

Numa comunidade de objectos estes podem comunicar entre si. O tipo de comunicação que aqui se considera é a chamada síncrona condicional, isto é, a ocorrência de uma acção a_1 num objecto leva à ocorrência (simultânea) de uma acção a_2 noutro objecto distinto. Essa chamada pode ser condicional no sentido em que é possível que a ocorrência de a_1 só conduza à ocorrência de a_2 se certas condições forem verificadas pelos atributos do objecto a que pertence a_1 quando tal ocorrência tem lugar. Seguindo [60, 61], este tipo de comunicação é aqui especificada através de certas fórmulas (fórmulas de interacção) sobre uma assinatura de objecto adequada. Segue-se a definição de fórmula de interacção.

Definição 4.12 Seja $ob \in C_P$, $\Sigma^{ob}_{com} = (ob, Acc, Atr)$ e $\Sigma^{i}_{com} = (i, Acc_i, Atr_i)$ para cada para cada $i \in ob$. Sendo $i_1, i_2 \in ob$, a fórmula em F_{ob}

$$\mathbf{G}(q \Rightarrow (\triangledown a \Rightarrow \triangledown b))$$

na qual

- $a \in (\sigma^{i_1}_{ob})_{Acc}(Acc_{i_1})$ e $b \in (\sigma^{i_2}_{ob})_{Acc}(Acc_{i_2})$ são acções não nulas,
- $q \in (\sigma^{i_1}_{ob})_F(CE^{\mathbf{tf}}_{i_1})$,

designa-se por *fórmula de interacção.* As acções a e b dizem-se *gatilho* e *alvo* da fórmula de interação, respectivamente. A fórmula q diz-se *condição* da fórmula de interacção.

Denota-se por $Intr_{ob}$ o conjunto de todas as fórmulas de interacção em F_{ob}. Dada uma fórmula $f \in Intr_{ob}$, o gatilho de f, o alvo de f e a condição de f são denotados por $gt(f)$, $alv(f)$ e $cnd(f)$, respectivamente. Denota-se por $Intr^{a,b}_{ob}$ o conjunto de todas as fórmulas em $f \in Intr_{ob}$ tal que $gt(f) = a$ e $alv(f) = b$. Dado $I \subseteq Intr_{ob}$, denotam-se por $gt(I)$, $alv(I)$ e $cnd(I)$ os conjuntos $\{gt(f) : f \in I\}$, $\{alv(f) : f \in I\}$ e $\{cnf(f) : f \in I\}$, respectivamente. ∎

4.3 Semântica

Nesta secção introduzem-se as noções de estrutura de interpretação de objecto sobre uma assinatura de comunidade e de estrutura de interpretação de comunidade. Introduzem-se ainda as noções de satisfação e validade de fórmulas assim como alguns resultados que são necessários ao longo do capítulo. Ao longo desta secção assume-se fixada a assinatura de comunidade de objectos $\Sigma_{com} = (P, Asn)$.

Definição 4.13 Uma *estrutura de interpretação de objecto sobre* Σ_{com} é um par (ob, λ) onde

- $ob \in C_P$;
- sendo $\Sigma_{com}^{ob} = (ob, Acc, Atr)$, $\lambda : I\!N_0 \to \wp(\nabla Acc \cup \diamond Acc \cup Atr)$ é uma função tal que se ob é singular então
  - $\diamond\bot \in \lambda(k)$ para todo $k \in I\!N_0$,
  - para todo $k \in I\!N_0$ existe um e um só $a \in Acc$ tal que $\nabla a \in \lambda(k)$,
  - para todo $k \in I\!N_0$ se $\nabla a \in \lambda(k)$ então $\diamond a \in \lambda(k)$.

Denota-se por $Intp(\Sigma_{com})$ o conjunto das estruturas de interpretação de objecto sobre a assinatura de comunidade de objectos Σ_{com}. ∎

Definição 4.14 Sejam $ob, ob' \in C_P$ tais que $ob \subseteq ob'$, $\Sigma_{com}^{ob} = (ob, Acc, Atr)$ e $\Sigma_{com}^{ob'} = (ob', Acc', Atr')$. Dada a função $\lambda' : I\!N_0 \to \wp(\nabla Acc' \cup \diamond Acc' \cup Atr')$, define-se a função

$$(\sigma_{ob'}^{ob})^{-1}(\lambda') : I\!N_0 \to \wp(\nabla Acc \cup \diamond Acc \cup Atr)$$

tal que, para cada $k \in I\!N_0$,

$$(\sigma_{ob'}^{ob})^{-1}(\lambda')(k) = \{f \in \nabla Acc \cup \diamond Acc \cup Atr : (\sigma_{ob'}^{ob})_F(f) \in \lambda'(k)\}$$

a qual se designa por *reduto de* λ' *relativamente a* ob. ∎

Definição 4.15 Uma *estrutura de interpretação de comunidade sobre* Σ_{com} é uma função

$$\Lambda : C_P \to Intp(\Sigma_{com})$$

tal que $\Lambda(ob) = (ob, \lambda)$, para cada $ob \in C_P$, é tal que se ob não é singular e $\Lambda(i) = (i, \lambda_i)$ para cada $i \in ob$ então $\lambda(k) = \bigcup_{i \in ob}(\sigma_{ob}^{i})_F(\lambda_i(k))$ para cada $k \in I\!N_0$

Se não há ambiguidade sobre a assinatura de comunidade em questão dir-se-á simplesmente que Λ é uma estrutura de interpretação de comunidade. ∎

Lema 4.16 Seja Λ uma estrutura de interpretação de comunidade e $ob, ob' \in C_P$ tais que $ob \subseteq ob'$, $\Lambda(ob) = (ob, \lambda)$ e $\Lambda(ob') = (ob', \lambda')$. Tem-se que λ é o reduto de λ' relativamente a ob.

Prova: Pelas Definições 4.14 e 4.15 tendo em conta as Definições 4.4 e 4.9. ∎

Definição 4.17 Sejam Λ uma estrutura de interpretação de comunidade sobre Σ_{com} e $ob \in C_P$. A fórmula $f \in F_{ob}$ é *satisfeita por* Λ em k, o que se representa por

$$\Lambda, k \models_{ob} f$$

sse $\Lambda(ob) = (ob, \lambda)$ e $\lambda, k \models f$ no sentido da Definição 2.15. ∎

A noção de satisfação relativa às abreviaturas segue naturalmente o Lema 2.17.

Definição 4.18 Sejam Λ uma estrutura de interpretação de comunidade sobre Σ_{com}, $ob \in C_P$, $f, f' \in F_{ob}$, $A \subseteq F_{ob}$ e $\mathcal{A} = \{A_{ob}\}_{ob \in C}$ com $C \subseteq C_P$ e $A_{ob} \subseteq F_{ob}$ para cada $ob \in C$:

- Λ *satisfaz* ou é *modelo* de f, $\Lambda \models_{ob} f$, sse $\Lambda, 0 \models_{ob} f$; f diz-se *possível* sse tem um modelo e *impossível* caso contrário;
- Λ *satisfaz* ou é *modelo* de A, $\Lambda \models_{ob} A$, sse $\Lambda \models_{ob} f$ qualquer que seja $f \in A$; A diz-se *possível* ou *coerente* sse tem um modelo e *impossível* ou *incoerente* caso contrário;
- Λ *satisfaz* ou é *modelo* de $\mathcal{A}$, $\Lambda \models \mathcal{A}$, sse $\Lambda \models_{ob} A_{ob}$ para todo $ob \in C$;
- f diz-se *válida*, $\models_{ob} f$, sse todas as estruturas de interpretação de comunidade de objectos sobre Σ_{com} são modelos de f;
- f e f' dizem-se equivalentes sse $\models_{ob} f \Leftrightarrow f'$. ∎

Apresentam-se agora três resultados que serão necessários no seguimento.

Lema 4.19 Sejam Λ uma estrutura de interpretação de comunidade sobre Σ_{com}, $ob, ob' \in C_P$ tais que $ob \subseteq ob'$ e $k \in I\!N_0$. Tem-se que $\Lambda, k \models_{ob} f$ sse $\Lambda, k \models_{ob'} (\sigma^{ob}_{ob'})_F(f)$ qualquer que seja $f \in F_{ob}$.

Prova: Sejam $\Sigma^{ob}_{com} = (ob, Acc, Atr)$, $\Sigma^{ob'}_{com} = (ob', Acc', Atr')$, $\Lambda(ob) = (ob, \lambda)$ e $\Lambda(ob') = (ob', \lambda')$. A prova decorre por indução estrutural.

Base: O caso $f \in \{\mathbf{t}, \mathbf{f}\}$ é trivial. Se $f \in \triangledown Acc \cup \diamond Acc \cup Atr$ então $\Lambda, k \models_{ob} f$ sse $f \in \lambda(k)$ sse, pelo Lema 4.16, $(\sigma^{ob}_{ob'})_F(f) \in \lambda'(k)$ sse $\Lambda, k \models_{ob'} (\sigma^{ob}_{ob'})_F(f)$.

Passo: (i) Se $f = f_1 \wedge f_2$ então $\Lambda, k \models_{ob} f$ sse $\Lambda, k \models_{ob} f_1$ e $\Lambda, k \models_{ob} f_2$ sse, por hipótese de indução, $\Lambda, k \models_{ob'} (\sigma^{ob}_{ob'})_F(f_1)$ e $\Lambda, k \models_{ob'} (\sigma^{ob}_{ob'})_F(f_2)$ sse, $\Lambda, k \models_{ob'} (\sigma^{ob}_{ob'})_F(f_1 \wedge f_2)$.

(ii) Se $f = \mathbf{X} f_1$ então $\Lambda, k \models_{ob} f$ sse $\Lambda, k+1 \models_{ob} f_1$ sse, por hipótese de indução, $\Lambda, k+1 \models_{ob'} (\sigma^{ob}_{ob'})_F(f_1)$ sse $\Lambda, k \models_{ob'} (\sigma^{ob}_{ob'})_F(f)$.

(iii) Se $f = f_2 \mathbf{U} f_1$ então $\Lambda, k \models_{ob} f$ sse existe $k' \geq k$ tal que $\Lambda, k' \models_{ob} f_1$ e $\Lambda, k'' \models_{ob} f_2$ para todo $k \leq k'' < k'$ sse, por hipótese de indução, $\Lambda, k' \models_{ob'} (\sigma^{ob}_{ob'})_F(f_1)$ e $\Lambda, k'' \models_{ob'} (\sigma^{ob}_{ob'})_F(f_2)$ para todo $k \leq k'' < k'$ sse $\Lambda, k \models_{ob'} (\sigma^{ob}_{ob'})_F(f)$.

(iv) Se $f = \neg f_1$ então $\Lambda, k \models_{ob} f$ sse $\Lambda, k \not\models_{ob} f_1$ sse, por hipótese de indução, $\Lambda, k \not\models_{ob'} (\sigma^{ob}_{ob'})_F(f_1)$ sse $\Lambda, k \models_{ob'} \neg(\sigma^{ob}_{ob'})_F(f_1)$ sse $\Lambda, k \models_{ob'} (\sigma^{ob}_{ob'})_F(f)$. ∎

Lema 4.20 Sejam $ob \in C_P$ não singular, $\Sigma_{com}^{ob} = (ob, Acc, Atr)$ e, para cada $i \in ob$, $\Sigma_{com}^{i} = (i, Acc_i, Atr_i)$. Sejam Λ uma estrutura de interpretação de comunidade sobre Σ_{com} e $k \in I\!N_0$. Para cada $i \in ob$ sejam $b_i \in Acc_i$, $o_{ji} \in Atr_i$ e $p_{ji} \in LE_i^{\mathbf{tf}}$, com $1 \leq j \leq n_i$ e $n_i \in I\!N_0$ tal que $o_{j'i} \neq o_{j''i}$ quaisquer que sejam $1 \leq j', j'' \leq n_i$, $j' \neq j''$, e

$$\Lambda, k \models_i (\nabla b_i \wedge q_i\,{}^{o_{1i} \ldots o_{n_i i}}_{p_{1i} \ldots p_{n_i i}}) \Rightarrow (\mathbf{X}\, q_i)$$

para todo $q_i \in CE_i^{\mathbf{tf}}$. Sendo $i_1, \ldots, i_m \in Enm(ob)$, tem-se que para todo $q \in CE_{ob}^{\mathbf{tf}}$

$$\Lambda, k \models_{ob} (\nabla a_1 \wedge \ldots \wedge \nabla a_m \wedge q[o/p]) \Rightarrow (\mathbf{X}\, q)$$

onde $q[o/p] = q\,{}^{(\sigma_{ob}^{i_1})_F(o_{1i_1}) \ldots (\sigma_{ob}^{i_1})_F(o_{n_1 i_1}) \ldots (\sigma_{ob}^{i_m})_F(o_{1i_m}) \ldots (\sigma_{ob}^{i_m})_F(o_{n_m i_m})}_{(\sigma_{ob}^{i_1})_F(p_{1i_1}) \ldots (\sigma_{ob}^{i_1})_F(p_{n_1 i_1}) \ldots (\sigma_{ob}^{i_m})_F(p_{1i_m}) \ldots (\sigma_{ob}^{i_m})_F(p_{n_m i_m})}$ e $\nabla a_{j'} = (\sigma_{ob}^{i_{j'}})_F(\nabla b_{i_{j'}})$ para cada $1 \leq j' \leq m$.

Prova: A prova decorre por indução na complexidade de $q \in CE_{ob}^{\mathbf{tf}}$. Pela Definição 4.9 e Lema 4.19, $\Lambda, k \models_{ob} \nabla a_1 \wedge \ldots \wedge \nabla a_m$ sse $\Lambda, k \models_i \nabla b_i$ para todo $i \in ob$. Para facilitar a exposição, seja, para cada $q_i \in Atr_i$, $q_i[o_i/p_i] = q_i\,{}^{o_{1i} \ldots o_{n_i i}}_{p_{1i} \ldots p_{n_i i}}$.

Base: O resultado é trivial se $q \in \{\mathbf{t}, \mathbf{f}\}$. Suponha-se $q \in Atr$, isto é, pela Definição 4.4, $q = x^{i_{j'}}$ para algum $1 \leq j' \leq m$ e $x \in Atr_{i_{j'}}$. Se $x \neq o_{ji_{j'}}$ para todo $1 \leq j \leq n_{i_{j'}}$ então $x[o_{i_{j'}}/p_{i_{j'}}] = x$ e $q[o/p] = x^{i_{j'}}$. Se $\Lambda, k \models_{ob} \nabla a_1 \wedge \ldots \wedge \nabla a_m \wedge q[o/p]$, pelo Lema 4.19, $\Lambda, k \models_{i_{j'}} \nabla b_{i_{j'}} \wedge x$. Então $\Lambda, k \models_{i_{j'}} \mathbf{X}\, x$ e portanto, pelo Lema 4.19, $\Lambda, k \models_{ob} \mathbf{X}\, q$. Se $x = o_{ji_{j'}}$ para algum $1 \leq j \leq n_{i_{j'}}$ então $x[o_{i_{j'}}/p_{i_{j'}}] = p_{ji_{j'}}$ e $q[o/p] = \sigma_{ob\,F}^{i_{j'}}(p_{ji_{j'}})$. Como $\Lambda, k \models_{ob} \nabla a_1 \wedge \ldots \wedge \nabla a_m \wedge q[o/p]$, pelo Lema 4.19, $\Lambda, k \models_{i_{j'}} \nabla b_{i_{j'}} \wedge p_{ji_{j'}}$. Então $\Lambda, k \models_{i_{j'}} \mathbf{X}\, x$ e portanto, pelo Lema 4.19, $\Lambda, k \models_{ob} \mathbf{X}\, q$.

Passo: (i) Suponha-se $q = q_1 \wedge q_2$. Pelo Lema 2.12, $q[o/p] = q_1[o/p] \wedge q_2[o/p]$. Se $\Lambda, k \models_{ob} \nabla a_1 \wedge \ldots \wedge \nabla a_m \wedge q[o/p]$, usando a hipótese de indução, $\Lambda, k \models_{ob} \mathbf{X}\, q_1$ e $\Lambda, k \models_{ob} \mathbf{X}\, q_2$, ou seja, $\Lambda, k \models_{ob} \mathbf{X}\, q$.

(ii) Suponha-se $q = \neg q_1$ e $\Lambda, k \models_{ob} \nabla a_1 \wedge \ldots \wedge \nabla a_m \wedge q[o/p]$. Pelo Lema 2.12, $q[o/p] = \neg(q_1[o/p])$ e portanto $\Lambda, k \not\models_{ob} q_1[o/p]$. O caso $q_1 \in \{\mathbf{t}, \mathbf{f}\}$ é trivial. Segue-se a análise dos outros casos.

(ii.a) Suponha-se $q_1 = x^{i_{j'}} \in Atr$ para algum $1 \leq j' \leq m$ e portanto $x \in Atr_{i_{j'}}$.

(ii.a.1) Se $x \neq o_{ji_{j'}}$ para todo $1 \leq j \leq n_{i_{j'}}$ então $x\, [o_{i_{j'}}/p_{i_{j'}}] = x$ e $q_1[o/p] = x^{i_{j'}}$. Como $\Lambda, k \not\models_{ob} x^{i_{j'}}$, pelo Lema 4.19, $\Lambda, k \not\models_{i_{j'}} x$, isto é, $\Lambda, k \models_{i_{j'}} \neg x$. Pelo Lema 2.12, $(\neg x) = (\neg x)[o_{i_{j'}}/p_{i_{j'}}]$ e assim $\Lambda, k \models_{i_{j'}} \mathbf{X}(\neg x)$. Pelo Lema 4.19, $\Lambda, k \models_{ob} \mathbf{X}(\neg x^{i_{j'}})$, ou seja, $\Lambda, k \models_{ob} \mathbf{X}\, q$.

(ii.a.2) Se $x = o_{ji_{j'}}$ para algum $1 \leq j \leq n_{i_{j'}}$ então $x[o_{i_{j'}}/p_{i_{j'}}] = p_{ji_{j'}}$ e $q_1[o/p] = (\sigma_{ob}^{i_{j'}})_F(p_{ji_{j'}})$. Como $\Lambda, k \not\models_{ob} (\sigma_{ob}^{i_{j'}})_F(p_{ji_{j'}})$, pelo Lema 4.19, $\Lambda, k \not\models_{i_{j'}} p_{ji_{j'}}$, isto é, $\Lambda, k \models_{i_{j'}} \neg p_{ji_{j'}}$. Pelo Lema 2.12, $(\neg p_{ji_{j'}}) = (\neg x)[o_{i_{j'}}/p_{i_{j'}}]$ e assim $\Lambda, k \models_{i_{j'}} \mathbf{X}(\neg x)$. Pelo Lema 4.19, $\Lambda, k \models_{ob} \mathbf{X}(\neg x^{i_{j'}})$, ou seja, $\Lambda, k \models_{ob} \mathbf{X}\, q$.

(ii.b) Suponha-se que $q_1 = \neg q_2$. Pelo Lema 2.12, $q_1[o/p] = (\neg q_2)[o/p] = \neg(q_2[o/p])$. Assim, $\Lambda, k \models_{ob} q_2[o/p]$. Usando a hipótese de indução, tem-se que $\Lambda, k \models_{ob} \mathbf{X}\, q_2$ e portanto $\Lambda, k \models_{ob} \mathbf{X}(\neg(\neg q_2))$, ou seja, $\Lambda, k \models_{ob} \mathbf{X}\, q$.

(ii.c) Suponha-se que $q_1 = q_2 \wedge q_3$. Pelo Lema 2.12, $q_1[o/p] = q_2[o/p] \wedge q_3[o/p]$. Assim, $\Lambda, k \not\models_{ob} q_2[o/p]$ ou $\Lambda, k \not\models_{ob} q_3[o/p]$. Suponha-se $\Lambda, k \not\models_{ob} q_2[o/p]$, ou seja, $\Lambda, k \models_{ob} \neg q_2[o/p]$ (o outro caso é semelhante). Pelo Lema 2.12, $\neg q_2[o/p] = (\neg q_2)[o/p]$. Usando a hipótese de indução, tem-se que $\Lambda, k \models_{ob} \mathbf{X}(\neg q_2)$ e portanto $\Lambda, k \models_{ob} \mathbf{X}(\neg(q_2 \wedge q_3))$, ou seja, $\Lambda, k \models_{ob} \mathbf{X}\, q$. ■

Lema 4.21 Sejam $ob \in C_P$, $\Sigma^{ob}_{com} = (ob, Acc, Atr)$ e $q \in CE^{\mathbf{tf}}_{ob}$.

1. Sejam Λ e Λ' duas estruturas de interpretação de comunidade sobre Σ_{com} com $\Lambda(ob) = (ob, \lambda)$ e $\Lambda(ob') = (ob, \lambda')$ e $k, k' \in I\!N_0$ tal que $\lambda(k) \cap Atr = \lambda'(k') \cap Atr$. Tem-se que $\Lambda, k \models_{ob} q$ sse $\Lambda', k' \models_{ob} \models q$.

2. Existe uma estrutura de interpretação de comunidade sobre Σ_{com} tal que $\Lambda \models_{ob} q$ sse, no sentido das Definições 2.14 e 2.16, existe uma estrutura de interpretação λ sobre $\Sigma = (Acc, Atr)$ tal que $\lambda \models q$.

Prova: (1) Pela Definição 4.17 e Lema 2.18.

(2) (a) Seja Λ tal que $\Lambda \models_{ob} q$, isto é, sendo $\Lambda(ob) = (ob, \lambda_{ob})$ tem-se que $\lambda_{ob} \models q$ no sentido da Definição 2.15. A função $\lambda : I\!N_0 \to \wp(\nabla Acc \cup \diamond Acc \cup Atr)$ tal que $\lambda(k) = (\lambda_{ob}(k) \cap Atr) \cup \{\nabla a, \diamond a\}$ para algum $a \in Acc (\neq \emptyset)$ é uma estrutura de interpretação sobre Σ. Fazendo uma prova semelhante à apresentada para o Lema 2.18, conclui-se que $\lambda \models q$.

(b) Seja λ uma estrutura de interpretação sobre Σ tal que $\lambda \models q$. Sejam $\Sigma^i_{com} = (i, Acc_i, Atr_i)$ para cada $i \in P$ e $i_1 \dots i_m \in Enm(ob)$. Pela Definição 2.14, $\lambda(k) \cap Acc = \{a^k\}$ para cada $k \in I\!N_0$. Pela Definição 4.4, para cada $k \in I\!N_0$ existe $1 \leq j_k \leq m$ tal que $a^k \in (\sigma^{i_{j_k}}_{ob})_{Acc}(Acc_{i_{j_k}})$. Considere-se a interpretação de comunidade Λ definida da seguinte forma: (i) para cada $1 \leq j \leq m$, $\Lambda(i_j) = (i_j, \lambda_{i_j})$ é tal que, para cada $k \in I\!N_0$, $\lambda_{i_j}(k) = \{\nabla b, \diamond b\} \cup \{o \in Atr_{i_j} : (\sigma^{i_j}_{ob})_{Atr}(o) \in \lambda(k)\}$ com $b \in Acc_{i_j}(\neq \emptyset)$ tal que $b = (\sigma^{i_j}_{ob})^{-1}_{Acc}(a^k)$ se $j = j_k$; (ii) para cada $i \in P \backslash \{i_1, \dots, i_m\}$, $\Lambda(i) = (i, \lambda_i)$ é tal que, para cada $k \in I\!N_0$, $\lambda_i(k) = \{\nabla b, \diamond b\}$ com $b \in Acc_i(\neq \emptyset)$. Pela Definição 4.15, sendo $\Lambda(ob) = (ob, \lambda_{ob})$, $\lambda_{ob}(k) \cap Atr = \lambda(k) \cap Atr$ para cada $k \in I\!N_0$. Fazendo uma prova semelhante à apresentada para o Lema 2.18, conclui-se que $\lambda_{ob} \models q$ e portanto $\Lambda \models_{ob} q$. ■

4.4 Especificação

Uma especificação de comunidade de objectos inclui uma assinatura de comunidade de objectos, uma família de conjuntos de fórmulas e uma família de conjuntos de esquemas de valoração ambas indexadas por C_P.

Definição 4.22 Uma *especificação de comunidade de objectos* é um triplo

$$eco = (\Sigma_{com}, \mathcal{A}x\mathcal{F}, \mathcal{A}x\mathcal{S})$$

no qual

- $\Sigma_{com} = (P, Asn)$ é uma assinatura de comunidade de objectos;

- $\mathcal{A}x\mathcal{F} = \{AxF_{ob}\}_{ob \in C_P}$ com $AxF_{ob} \subseteq F_{ob}$ para cada $ob \in C_P$;
- $\mathcal{A}x\mathcal{S} = \{AxS_{ob}\}_{ob \in C_P}$ com $AxS_{ob} \subseteq S_{ob}$ para cada $ob \in C_P$. ■

Definição 4.23 Seja $eco = (\Sigma_{com}, \mathcal{A}x\mathcal{F}, \mathcal{A}x\mathcal{S})$ uma especificação de comunidade de objectos na qual $\mathcal{A}x\mathcal{F} = \{AxF_{ob}\}_{ob \in C_P}$ e $\mathcal{A}x\mathcal{S} = \{AxS_{ob}\}_{ob \in C_P}$. Seja $C \subseteq C_P$ e seja e $\mathcal{A} = \{A_{ob}\}_{ob \in C}$ uma família de conjuntos tal que $A_{ob} \subseteq F_{ob}$ para cada $ob \in C$. O *enriquecimento de eco com* $\mathcal{A}$ é a especificação de comunidade de objectos

$$eco' = (\Sigma, \mathcal{A}x\mathcal{F}', \mathcal{A}x\mathcal{S})$$

onde $\mathcal{A}x\mathcal{F}' = \{AxF'_{ob}\}_{ob \in C_P}$ e $AxF'_{ob} = AxF_{ob} \cup A_{ob}$ se $ob \in C$ e $AxF'_{ob} = AxF_{ob}$ caso contrário. ■

Observação 4.24 No que se segue, trabalhar-se-á no contexto de especificações de comunidade de objectos $eco = (\Sigma, \mathcal{A}x\mathcal{F}, \mathcal{A}x\mathcal{S})$ satisfazendo os requisitos que seguidamente se apresentam. Sendo $\Sigma_{com} = (P, Asn)$, $\mathcal{A}x\mathcal{F} = \{AxF_{ob}\}_{ob \in C_P}$, $\mathcal{A}x\mathcal{S} = \{AxS_{ob}\}_{ob \in C_P}$ e $ob \in C_P$, então

- se ob é singular e $\Sigma^{ob}_{com} = (ob, Acc, Atr)$ então
  - $AxF_{ob} \subseteq CE^{\mathbf{tf}}_{ob} \cup RActv_{ob} \cup RJst_{ob}$,
  - $AxS_{ob} = \bigcup_{a \in Acc}\{s_a\}$ onde $s_a \in S^a_{ob}$ e $s_\perp = \mathbf{G}((\nabla\perp \wedge \alpha) \Rightarrow (\mathbf{X}\,\alpha))$;
- se $ob = \{i_1, i_2\}$, $i_1 \neq i_2$, e $\Sigma^{i_1}_{com} = (i_1, Acc_1, Atr_1)$, $\Sigma^{i_2}_{com} = (i_2, Acc_2, Atr_2)$ então
  - $AxF_{ob} \subseteq Intr_{ob}$ é tal que se $f \in AxF_{ob}$ e $gt(f) \in (\sigma^{i_j}_{ob})_{Acc}(Acc_j)$ para algum $1 \leq j \leq 2$ então $alv(f) \in (\sigma^{i_{j'}}_{ob})_{Acc}(Acc_{j'})$ com $1 \leq j' \leq 2$ e $j \neq j'$,
  - $AxS_{ob} = \emptyset$;
- se ob não está nas condições anteriores então $AxF_{ob} = \emptyset$ e $AxS_{ob} = \emptyset$. ■

Exemplo 4.25 Seja a assinatura de comunidade de objectos considerada no Exemplo 4.5. Sejam $\mathcal{A}x\mathcal{F} = \{AxF_{ob}\}_{ob \in C_P}$ e $\mathcal{A}x\mathcal{S} = \{AxS_{ob}\}_{ob \in C_P}$ tais que

$$AxF_1 = \{\neg z\} \qquad AxS_1 = \{\mathbf{G}((\nabla a \wedge \alpha\,{}^{x}_{\neg y}\,{}^{z}_{\neg z}) \Rightarrow (\mathbf{X}\,\alpha)),\ \mathbf{G}((\nabla b \wedge \alpha\,{}^{y}_{\neg y}) \Rightarrow (\mathbf{X}\,\alpha)),\ \mathbf{G}((\nabla c \wedge \alpha\,{}^{z}_{\mathbf{t}}) \Rightarrow (\mathbf{X}\,\alpha)),\ \mathbf{G}((\nabla\perp \wedge \alpha) \Rightarrow (\mathbf{X}\,\alpha))\}$$

$$AxF_2 = \{z\} \qquad AxS_2 = \{\mathbf{G}((\nabla a \wedge \alpha\,{}^{z}_{\neg z}) \Rightarrow (\mathbf{X}\,\alpha)),\ \mathbf{G}((\nabla d \wedge \alpha\,{}^{u}_{\neg u}) \Rightarrow (\mathbf{X}\,\alpha)),\ \mathbf{G}((\nabla e \wedge \alpha\,{}^{u}_{z}) \Rightarrow (\mathbf{X}\,\alpha)),\ \mathbf{G}((\nabla\perp \wedge \alpha) \Rightarrow (\mathbf{X}\,\alpha))\}$$

$AxF_3 = \{\neg x\}$

$$AxS_3 = \{\mathbf{G}((\nabla c \wedge \alpha\,{}^{x}_{\mathbf{t}}\,{}^{w}_{\neg w}) \Rightarrow (\mathbf{X}\,\alpha)),\ \mathbf{G}((\nabla e \wedge \alpha\,{}^{w}_{\mathbf{f}}) \Rightarrow (\mathbf{X}\,\alpha)),\ \mathbf{G}((\nabla \bot \wedge \alpha) \Rightarrow (\mathbf{X}\,\alpha))\}$$

$AxF_4 = \{y, \neg u\}$

$$AxS_4 = \{\mathbf{G}((\nabla a \wedge \alpha\,{}^{y}_{\mathbf{t}}) \Rightarrow (\mathbf{X}\,\alpha)),\ \mathbf{G}((\nabla c \wedge \alpha\,{}^{y}_{\neg y}\,{}^{u}_{\mathbf{t}}) \Rightarrow (\mathbf{X}\,\alpha)),\ \mathbf{G}((\nabla \bot \wedge \alpha) \Rightarrow (\mathbf{X}\,\alpha))\}$$

$AxF_{\{1,2\}} = \{\mathbf{G}((\neg y^1) \Rightarrow (\nabla c^1 \Rightarrow \nabla d^2))\}$ $\quad AxS_{\{1,2\}} = \emptyset$

$AxF_{\{3,4\}} = \{\mathbf{G}(\mathbf{t} \Rightarrow (\nabla a^4 \Rightarrow \nabla c^3))\}$ $\quad AxS_{\{3,4\}} = \emptyset$

$AxF_{ob'} = AxS_{ob'} = \emptyset$ para cada $ob' \in C_P \backslash \{1, 2, 3, 4, \{1, 2\}, \{3, 4\}\}$.

O tuplo $eco = (\Sigma, \mathcal{A}x\mathcal{F}, \mathcal{A}x\mathcal{S})$ é uma especificação de comunidade de objectos. ∎

Definição 4.26 Seja $eco = (\Sigma_{com}, \mathcal{A}x\mathcal{F}, \mathcal{A}x\mathcal{S})$ uma especificação de comunidade de objectos na qual $\mathcal{A}x\mathcal{F} = \{AxF_{ob}\}_{ob \in C_P}$ e $\mathcal{A}x\mathcal{S} = \{AxS_{ob}\}_{ob \in C_P}$. A estrutura de interpretação de comunidade Λ sobre Σ_{com} *satisfaz* ou é *modelo* de *eco* sse

$$\Lambda \models \{AxF_{ob} \cup \iota(AxS_{ob}, CE_{ob})\}_{ob \in C_P};$$

a especificação *eco* diz-se *coerente* sse tem pelo menos um modelo e *incoerente* caso contrário.

Definição 4.27 Sejam $eco = (\Sigma_{com}, \mathcal{A}x\mathcal{F}, \mathcal{A}x\mathcal{S})$ uma especificação de comunidade de objectos, $ob \in C_P$, $f \in F_{ob}$, $A \subseteq F_{ob}$ e $\mathcal{A} = \{A_{ob}\}_{ob \in C}$ onde $C \subseteq C_P$ e $A_{ob} \subseteq F_{ob}$ para cada $ob \in C$:

- f é *eco-válida*, $eco \models_{ob} f$, sse todos os modelos de *eco* são também modelos de f;
- A é *eco-possível* sse existe um modelo de *eco* que também é modelo de A;
- $\mathcal{A}$ é *eco-possível* sse existe um modelo de *eco* que também é modelo de $\mathcal{A}$. ∎

O lema seguinte mostra como se podem utilizar tableaux temporais para raciocinar sobre uma especificação de comunidade de objectos.

Lema 4.28 Sejam $eco = (\Sigma_{com}, \{AxF_{ob}\}_{ob \in C_P}, \{AxS_{ob}\}_{ob \in C_P})$ uma especificação de comunidade de objectos verificando os requisitos da Observação 4.24, $ob \in C_P$ e, para cada $i \in ob$, $\Sigma^i_{com} = (i, Acc_i, Atr_i)$. Seja $f \in F_{ob}$ e V_{eco} o conjunto

$$(\textstyle\bigcup_{ob \in C_P} (\sigma^{ob}_P)_F(AxF_{ob})) \cup F(\bigcup_{A \in ACC_P} \{s^A\}) \cup$$
$$(\textstyle\bigcup_{i \in P} \{(\sigma^i_P)_F(\mathbf{G}(\nabla b \Rightarrow \diamond b)) : b \in Acc_i\}) \cup$$
$$(\textstyle\bigcup_{i \in P} \{(\sigma^i_P)_F(\mathbf{G}(\neg(\nabla b_1 \wedge \nabla b_2))) : b_1, b_2 \in Acc_i, b_1 \neq b_2\}) \cup$$
$$(\textstyle\bigcup_{i \in P} \{(\sigma^i_P)_F(\mathbf{G}(\diamond \bot))\}) \cup (\bigcup_{i \in P} \{(\sigma^i_P)_F(\mathbf{G}(\nabla b_{i1} \vee \ldots \nabla b_{in_i}))\})$$

onde

- $F(s^A)$, para cada $A \in ACC_P$, tem definição análoga à definição apresentada no contexto da Proposição 2.27 sendo $i_1 \ldots i_m \in Enm(P)$ e

  $$s^A = \mathbf{G}((\nabla a^A_{i_1} \wedge \ldots \wedge \nabla a^A_{i_m} \wedge \alpha[o^A/p^A]) \Rightarrow (\mathbf{X}\,\alpha))$$

  com $\alpha[o^A/p^A] = \alpha\,{}^{(\sigma_P^{i_1})_F(o_{1i_1})\ldots(\sigma_P^{i_1})_F(o_{n_1 i_1})\ldots(\sigma_P^{i_m})_F(o_{1i_m})\ldots,(\sigma_P^{i_m})_F(o_{n_m i_m})}_{(\sigma_P^{i_1})_F(p_{1i_1})\ldots(\sigma_P^{i_1})_F(p_{n_1 i_1})\ldots,(\sigma_P^{i_m})_F(p_{1i_m})\ldots(\sigma_P^{i_m})_F(p_{n_m i_m})}$ e, para cada $1 \leq j \leq m$,

  $$\mathbf{G}(((\sigma_P^{i_j})^{-1}_{Acc}(\nabla a^A_{i_j}) \wedge \alpha^{o_{1i_j}\ldots o_{n_j i_j}}_{p_{1i_j}\ldots p_{n_j i_j i}}) \Rightarrow (\mathbf{X}\,\alpha)) \in AxS_{i_j}$$

- $b_{i1} \ldots b_{in_i} \in Enm(Acc_i)$ para cada $i \in P$.

Sendo $SP_{\Sigma_{com}} = \bigcup_{i \in P}(\sigma_P^i)_F(\{\nabla b, \diamond b : b \in Acc_i\} \cup Atr_i)$, tem-se que $V_{eco} \cup \{\neg(\sigma_P^{ob})_F(f)\}$ é LTPL($SP_{\Sigma_{com}}$)-impossível sse $eco \models_{ob} f$.

Prova: (a) Suponha-se, por absurdo, que $V_{eco} \cup \{\neg(\sigma_P^{ob})_F(f)\}$ é LTPL($SP_{\Sigma_{com}}$)-impossível e existe uma estrutura de interpretação de comunidade Λ que é modelo de eco e verifica $\Lambda \models_{ob} \neg f$. Pelo Lema 4.19, $\Lambda \models_P \neg(\sigma_P^{ob})_F(f)$. Pelas Definições 4.13, 4.15 e 4.26 e pelo Lema 4.19: (i) $\Lambda \models_P \bigcup_{ob \in C_P}(\sigma_P^{ob})_F(AxF_{ob})$, (ii) $\Lambda \models_P \bigcup_{i \in P}\{(\sigma_P^i)_F(\mathbf{G}(\nabla b \Rightarrow \diamond b)) : b \in Acc_i\}$, (iii) $\Lambda \models_P \bigcup_{i \in P}\{(\sigma_P^i)_F(\mathbf{G}(\neg(\nabla b_1 \wedge \nabla b_2))) : b_1, b_2 \in Acc_i, b_1 \neq b_2\}$, (iv) $\Lambda \models_P \bigcup_{i \in P}\{(\sigma_P^i)_F(\mathbf{G}(\diamond\bot))\}$ e (v) $\Lambda \models_P \bigcup_{i \in P}\{(\sigma_P^i)_F(\mathbf{G}(\nabla b_{i1} \vee \ldots \nabla b_{in_i}))\}$. Tendo em conta que o Lema 2.26 pode ser facilmente generalizado para esquemas de valoração envolvendo mais de uma acção, pela Definição 4.26 e pelo Lema 4.20 tem-se que $\Lambda \models_P F(\bigcup_{A \in ACC_P}\{s^A\})$. Sendo $\Lambda(P) = (P, \lambda_P)$, tem-se que λ_P satisfaz os cinco conjuntos anteriores Assim tem-se que $\lambda_P \models V_{eco} \cup \{\neg(\sigma_P^{ob})_F(f)\}$ o que contradiz a hipótese.

(b) Suponha-se, por absurdo, que $eco \models_{ob} f$ e que existe uma LTPL($SP_{\Sigma_{com}}$)-estrutura de interpretação τ tal que τ satisfaz $V_{eco} \cup \{\neg(\sigma_P^{ob})_F(f)\}$. Seja $\Lambda : C_P \to Intp(\Sigma_{com})$ a função tal que, para cada $i \in P$, $\Lambda(i) = (i, \lambda_i)$ com $\lambda_i(k) = \{f \in \nabla Acc_i \cup \diamond Acc_i \cup Atr : (\sigma_P^i)_F(f) \in \tau(k)\}$ para cada $k \in I\!N_0$ e, para cada $ob \in C_P$, $\Lambda(ob) = (ob, \lambda_{ob})$ com $\lambda_{ob}(k) = \bigcup_{i \in ob}(\sigma_{ob}^i)_F(\lambda_i(k))$ para cada $k \in I\!N_0$.

(b.i) Λ é uma estrutura de interpretação de comunidade sobre Σ_{com}. Em particular, para cada $i \in P$, $\Lambda(i)$ satisfaz as condições da Definição 4.13 porque τ satisfaz os conjuntos $\bigcup_{i \in P}\{(\sigma_P^i)_F(\mathbf{G}(\nabla b \Rightarrow \diamond b)) : b \in Acc_i\}$, $\bigcup_{i \in P}\{(\sigma_P^i)_F(\mathbf{G}(\neg(\nabla b_1 \wedge \nabla b_2))) : b_1, b_2 \in Acc_i, b_1 \neq b_2\}$, $\bigcup_{i \in P}\{(\sigma_P^i)_F(\mathbf{G}(\diamond\bot))\}$ e $\bigcup_{i \in P}\{(\sigma_P^i)_F(\mathbf{G}(\nabla b_{i1} \vee \ldots \nabla b_{in_i}))\}$.

(b.ii) Dado que τ satisfaz $\bigcup_{ob \in C_P}(\sigma_P^{ob})_F(AxF_{ob})$ e que $\Lambda(P) = (P, \lambda_P) = (P, \tau)$, pela Definição 4.17, $\Lambda \models_P \bigcup_{ob \in C_P}(\sigma_P^{ob})_F(AxF_{ob})$. Pelo Lema 4.19, $\Lambda \models \{AxF_{ob}\}_{ob \in C_P}$.

(b.iii) Tendo novamente em conta que o Lema 2.26 se pode generalizar ao caso de esquemas de valoração que envolvam mais de uma acção, para cada $A \in ACC_P$, τ satisfaz $\iota(\{s^A\}, CE_P^{\mathbf{tf}})$ e portanto, dado que $\lambda_P = \tau$, tem-se que $\Lambda \models_P \iota(\{s^A\}, CE_P^{\mathbf{tf}})$. Pela Observação 4.24, $AxS_{ob} = \emptyset$ para cada $ob \in C_P$ não singular. Seja $i \in P$, $b \in Acc_i$ e $s = \mathbf{G}((\nabla b \wedge \alpha^{o_1 \ldots o_n}_{p_1 \ldots, p_n}) \Rightarrow (\mathbf{X}\,\alpha)) \in AxS_i$. Suponha-se, por absurdo, que $\Lambda \not\models_i \iota(\{s\}, CE_i^{\mathbf{tf}})$. Então existe $k \in I\!N_0$, $q \in CE_i^{\mathbf{tf}}$ tal que $\Lambda, k \models_i \nabla b \wedge q^{o_1 \ldots o_n}_{p_1 \ldots p_n}$ e $\Lambda, k \not\models_i \mathbf{X}\,q$. Pelo Lema 4.19, $\Lambda, k \models_P (\sigma_P^i)_F(\nabla b) \wedge (\sigma_P^i)_F(q^{o_1 \ldots, o_n}_{p_1 \ldots p_n})$. Por (b.i), $\lambda_P(k) \cap (\sigma_P^i)_F(\nabla Acc_i)$ é singular para cada $i \in P$. Designe-se por $\triangledown a_i^k$ o elemento deste conjunto para cada $i \in P$. Seja a acção composta $A^k = \bigcup_{i\in P}\{a_i^k\} \in ACC_P$. Tem-se então que $\Lambda, k \models_P \triangledown a_{i_1}^{A^k} \wedge \ldots \wedge \triangledown a_{i_m}^{A^k}$. Como $(\sigma_P^i)_F(q_{p_1\ldots p_n}^{o_1\ldots o_n}) = (\sigma_P^i)_F(q)_{(\sigma_P^i)_F(p_1)\ldots(\sigma_P^i)_F(p_n)}^{(\sigma_P^i)_F(o_1)\ldots(\sigma_P^i)_F(o_n)} = (\sigma_P^i)_F(q)[o^{A^k}/p^{A^k}]$ tem-se que $\Lambda, k \models_P (\sigma_P^i)_F(q)[o^{A^k}/p^{A^k}]$. Uma vez que $\Lambda \models_P \mathbf{G}((\triangledown a_{i_1}^{A^k} \wedge \ldots \wedge \triangledown a_{i_m}^{A^k} \wedge (\sigma_P^i)_F(q)[o^{A^k}/p^{A^k}]) \Rightarrow (\mathbf{X}(\sigma_P^i)_F(q)))$ conclui-se que $\Lambda, k \models_P \mathbf{X}(\sigma_P^i)_F(q)$. Pelo Lema 4.19, $\Lambda, k \models_i \mathbf{X}\, q$ o que contradiz a hipótese. Conclui-se assim que $\Lambda \models \{\iota(AxS_{ob}, CE_{ob}^{\mathbf{tf}})\}_{ob\in C_P}$.

(b.iv) Dos parágrafos anteriores resulta que Λ é modelo de *eco*. Dado que $\lambda_P = \tau$, pela Definição 4.17, $\Lambda \models_P \neg(\sigma_P^{ob})_F(f)$. Pelo Lema 4.19, $\Lambda \models_{ob} \neg f$ o que contradiz a hipótese inicial. ■

4.5 Conceitos básicos

Nesta secção introduzem-se os conceitos de observação, de problema de abdução e de explicação para um problema de abdução, tudo isto no âmbito de uma especificação de comunidade de objectos.

A caracterização sintáctica das observações é a introduzida anteriormente para o caso local. Estas observações caracterizam agora propriedades relativas ao comportamento conjunto de vários objectos. Estas propriedades devem ser expressas como fórmulas de uma linguagem adequada que permita fazer referência aos atributos das assinaturas dos vários objectos em questão. A linguagem escolhida é a linguagem associada à assinatura de um objecto composto apropriado.

As explicações são constituídas por novos axiomas que vão introduzir novas restrições ao comportamento dos objectos primários. Estas restrições podem ser traduzidas, por um lado, através de novos axiomas associados à especificação de cada objecto primário *per se* como também, em certos casos, através de novas interacções expressas por fórmulas de interacção apropriadas.

Notação 4.29 Sejam $\Sigma_{com} = (P, Asn)$ uma assinatura de comunidade de objectos e $ob \in C_P$ com $\Sigma_{com}^{ob} = (ob, Acc, Atr)$. Para facilitar a exposição introduz-se a seguinte notação: Sb_{ob}^1 é o conjunto de todos os subconjuntos singulares de *ob* e Sb_{ob}^2 é o conjunto de todos os subconjuntos de *ob* com cardinalidade 2. ■

Definição 4.30 Seja $\Sigma_{com} = (P, Asn)$ uma assinatura de comunidade de objectos e sejam $ob \in C_P$ e $r, q, q_1, q_2 \in CE_{ob}^{\mathbf{tf}}$:

- as fórmulas
  - $\mathbf{G}(r \Rightarrow (\mathbf{X}\, q))$
  - $r \Rightarrow (q_1\, \mathbf{W}\, q_2)$
  - $\mathbf{G}(r \Rightarrow (q_1\, \mathbf{W}\, q_2))$

  dizem-se *observações de segurança sobre* Σ_{com}^{ob};
- a fórmula $\mathbf{G}(r \Rightarrow (q_1\, \mathbf{U}\, q_2))$ diz-se *observação de resposta sobre* Σ_{com}^{ob};

- a fórmula $r \Rightarrow (q_1 \mathbf{U}\, q_2)$ diz-se *observação de garantia sobre* Σ^{ob}_{com};
- a fórmula $\mathbf{G}(r \Rightarrow (\mathbf{F}(\mathbf{G}\, q)))$ diz-se *observação de persistência sobre* Σ^{ob}_{com}.

Qualquer fórmula equivalente a uma observação de segurança, de resposta, de garantia ou de persistência é também considerada observação de segurança, de resposta, de garantia ou de persistência, respectivamente. O conjunto O_{ob} constituído por todas as referidas observações sobre Σ^{ob}_{com} designa-se por *conjunto das observações sobre* Σ^{ob}_{com}. ∎

Definição 4.31 Seja $eco = (\Sigma_{com}, \mathcal{A}x\mathcal{F}, \mathcal{A}x\mathcal{S})$ uma especificação de comunidade de objectos tal que $\Sigma_{com} = (P, Asn)$ e seja $ob \in C_P$. Um *problema de abdução em eco sobre* Σ^{ob}_{com} é uma fórmula $f \in O_{ob}$ tal que $eco \not\models_{ob} f$. ∎

Tal como anteriormente, no que se segue, sempre que a observação relativa a um problema de abdução em *eco* seja uma observação de segurança, de resposta, etc., dir-se-á que é um problema de segurança em *eco*, um problema de resposta em *eco*, etc.

Exemplo 4.32 Considere-se a especificação de comunidade de objectos descrita no Exemplo 4.25. A fórmula $\mathbf{G}(z^2 \vee x^3) \in O_{\{2,3\}}$ é um problema de abdução em *eco*. A fórmula $\mathbf{G}(y^1 \wedge z^2) \in O_{\{1,2\}}$ é um problema de abdução em *eco*.

Neste âmbito, uma explicação para um problema de abdução é uma família $\mathcal{E}$ de conjuntos de novos axiomas construída por forma a que, sendo eco' o enriquecimento da especificação *eco* dada com $\mathcal{E}$, a observação em causa seja eco'-válida e *eco* seja coerente. Os conjuntos de axiomas que constituem a explicação contêm, como anteriormente, novas condições iniciais e/ou novas restrições de activação e/ou novos requisitos de justiça que correspondem a novos requisitos sobre o comportamento dos objectos primários. Por outro lado, podem conter também novos axiomas de interacção que correspondem à especificação de novas formas de comunicação entre os objectos da comunidade.

Definição 4.33 Sejam $eco = (\Sigma_{com}, \mathcal{A}x\mathcal{F}, \mathcal{A}x\mathcal{S})$ uma especificação de comunidade de objectos, $ob \in C_P$ e $f \in O_{ob}$ um problema em *eco*. Uma *explicação* para f é uma família de conjuntos

$$\mathcal{E} = \{E_{ob'}\}_{ob' \in Sb^1_{ob} \cup Sb^2_{ob}}$$

na qual

- $E_{ob'} \subseteq CE^{\mathbf{tf}}_{ob'} \cup RActv_{ob'} \cup RJst_{ob'}$ para todo $ob' \in Sb^1_{ob}$,
- $E_{ob'} \subseteq Intr_{ob'}$ para todo $ob' \in Sb^2_{ob}$,

tal que, sendo eco' o enriquecimento de *eco* com $\mathcal{E}$,

- $eco' \models_{ob} f$,
- eco' é coerente. ∎

Tal como no capítulo anterior, a questão da coerência terá de ser resolvida *a posteriori*. As técnicas de construção de explicações que se apresentam não asseguram que apenas sejam construídas famílias de conjuntos de fórmulas *eco*-possíveis. Assim, essa verificação tem de ser feita para cada família encontrada. Para tal podem usar-se tableaux temporais como mostra o Lema 4.28.

Exemplo 4.34 As famílias

$$\mathcal{E}_1 = \{E^1_{ob'}\}_{ob' \in \{2,3,\{2,3\}\}} \text{ onde}$$
$$E^1_{\{2,3\}} = \{\mathbf{G}(z^2 \Rightarrow (\triangledown a^2 \Rightarrow \triangledown c^3))\}$$
$$E^1_2 = E^1_3 = \emptyset$$

$$\mathcal{E}_2 = \{E^2_{ob'}\}_{ob' \in \{2,3,\{2,3\}\}} \text{ onde}$$
$$E^2_2 = \{\mathbf{G}(\diamond a \Rightarrow (\neg z))\}$$
$$E^2_3 = E^2_{\{2,3\}} = \emptyset$$

são exemplos de explicações para o problema de abdução $\mathbf{G}(z^2 \vee x^3) \in O_{\{2,3\}}$ referido no Exemplo 4.32. A explicação $\mathcal{E}_2$ impede a ocorrência da acção $a \in Acc_2$ quando se tem z. A explicação $\mathcal{E}_1$ permite a ocorrência desta acção quando se tem z desde que se garanta que ocorre simultaneamente a acção $c \in Acc_3$.

4.6 Geração de explicações para a garantia de constrangimento de estado a partir de outro constrangimento de estado por conjunto de acções

À semelhança das explicações construídas no Capítulo 3, para construir explicações para problemas de abdução no âmbito de especificações de comunidades de objectos descreve-se, em primeiro lugar, o modo de obter as restrições que é necessário impôr à ocorrência das acções contidas numa dada acção composta A para que haja garantia de que, se um certo constrangimento de estado é satisfeito quando ocorrem simultaneamente os elementos de A, então as modificações introduzidas por essas ocorrências conduzem à verificação de um outro constrangimento de estado. Neste âmbito, estas restrições podem ser expressas quer através de restrições de activação quer através de fórmulas de interacção adequadas.

Na subsecção 4.6.1 introduz-se a definição de garantia de um constrangimento de estado a partir de outro constrangimento de estado por um conjunto de acções e a definição de explicação para a referida garantia. Tal como no capítulo anterior, as explicações são construídas a partir da análise de certos tableaux. Na subsecção 4.6.2 descrevem-se os tableaux relevantes para a construção das explicações. Na subsecção 4.6.3 mostra-se como a partir dos referidos tableaux se constroem restrições de activação e fórmulas de interacção que constituem possíveis explicações para as garantias consideradas. Por último, na subsecção 4.6.4, apresentam-se alguns critérios de preferência entre explicações.

No que se segue assume-se fixada uma especificação de comunidade de objectos $eco = (\Sigma_{com}, \mathcal{A}x\mathcal{F}, \mathcal{A}x\mathcal{S})$ com $\Sigma = (P, Asn)$, $\Sigma_{com}^{ob} = (ob, Acc_{ob}, Atr_{ob})$ para cada $ob \in C_P$, $\mathcal{A}x\mathcal{F} = \{AxF_{ob}\}_{ob \in C_P}$ e $\mathcal{A}x\mathcal{S} = \{AxS_{ob}\}_{ob \in C_P}$.

4.6.1 Explicações

Definição 4.35 Sejam $ob \in C_P$, $a_1, \ldots, a_n \in Acc_{ob}$ e $q, q' \in CE_{ob}^{\mathbf{tf}}$. Diz-se que $a_1 \ldots a_n$ *garantem q a partir de q' em eco* sempre que

$$eco \models_{ob} \mathbf{G}((\nabla a_1 \wedge \ldots \wedge \nabla a_n \wedge q') \Rightarrow (\mathbf{X}\, q))$$

Dado $A \subseteq Acc_{ob}$ diz-se que A garante q a partir de q' em eco sse $a_1, \ldots, a_n \in Enm(A)$ garantem q a partir de q' em eco. ■

Tal como no capítulo anterior, se $q' = \mathbf{t}$ então dir-se-á que $a_1 \ldots a_n$ *garantem* q e se $q' = q$ dir-se-á que $a_1 \ldots a_n$ *preservam* q. Omitir-se-á, por vezes, a referência à especificação sempre que não haja ambiguidade sobre qual a especificação em questão.

Sendo $ob \in C_P$, da Definição 4.13 e Lema 4.19 decorre que qualquer que seja a estrutura de interpretação de comunidade Λ e $k \in I\!N_0$, para cada $i \in Sb_{ob}^1$ existe um e um só elemento $a' \in (\sigma_{ob}^i)_{Acc}(Acc_i)$ tal que $\Lambda, k \models_{ob} \nabla a'$. Consequentemente, tendo em conta a Definição 4.35, caso existam $i \in Sb_{ob}^1$, $a', a'' \in (\sigma_{ob}^i)_{Acc}(Acc_i)$ com $a' \neq a''$ então sempre que $\{a', a''\} \subseteq A \subseteq Acc_{ob}$ tem-se que A garante q a partir de q' quaisquer que sejam $q, q' \in CE_{ob}^{\mathbf{tf}}$.

No que se segue assumem-se fixados $ob \in C_P$ não singular, $q, q' \in CE_{ob}^{\mathbf{tf}}$ e $A \in ACC_{ob}$.

Definição 4.36 Uma *explicação para a garantia de q a partir de q' por A em eco* é uma família de conjuntos

$$\mathcal{E} = \{E_{ob'}\}_{ob' \in Sb_{ob}^1 \cup Sb_{ob}^2}$$

com

- $E_i \subseteq RActv_i^{(\sigma_{ob}^i)_{Acc}^{-1}(a_i^A)}$ para cada $i \in Sb_{ob}^1$ tal que
  - E_i é singular ou vazio,
  - se $f \in E_i$ então a_i^A é acção não nula e $cnd(f) = \mathbf{f}$ ou $cnd(f) = l_1 \wedge \ldots \wedge l_n$ com $n \geq 1$, $l_j \in LE_i$ para cada $1 \leq j \leq n$ e $l_j \neq \overline{l_{j'}}$ para quaisquer $1 \leq j, j' \leq n$,
- $E_{\{i,i'\}} \subseteq Intr_{\{i,i'\}}^{a_i^A, b_{i'}} \cup Intr_{\{i,i'\}}^{a_{i'}^A, b_i}$ para cada $\{i, i'\} \in Sb_{ob}^2$ tal que
  - $b_i \in (\sigma_{\{i,i'\}}^i)_{Acc}(Acc_i) \backslash A$ e $b_{i'} \in (\sigma_{\{i,i'\}}^{i'})_{Acc}(Acc_{i'}) \backslash A$,
  - se $f \in E_{\{i,i'\}}$ então $cnd(f) = \mathbf{t}$ ou $cnd(f) = \neg(l_1 \wedge \ldots \wedge l_n)$ com $n \geq 1$, $l_j \in LE_{\{i,i'\}}$ para cada $1 \leq j \leq n$ e $l_j \neq \overline{l_{j'}}$ para quaisquer $1 \leq j, j' \leq n$,
- para cada $i \in Sb_{ob}^1$ o conjunto $E_i \cup \{f \in E_{\{i,i'\}} : \{i, i'\} \in Sb_{ob}^2 \text{ e } gt(f) = a_i^A\}$ é singular ou vazio.

tal que, sendo eco' o enriquecimento de eco com $\mathcal{E}$,

- A garante q a partir de q' em eco',
- eco' é coerente.

Em particular, se $q' = \mathbf{t}$ a referida família diz-se *explicação para a garantia de q por A em eco* e se $q' = q$ diz-se *explicação para a preservação de q por A em eco*.

Se $E_{ob'} = \emptyset$ para qualquer $ob' \in Sb^2_{ob}$, $\mathcal{E}$ é uma *explicação por restrição de activação*; se $E_{ob'} = \emptyset$ para qualquer $ob' \in Sb^1_{ob}$, $\mathcal{E}$ é uma *explicação por interacção*. ■

Uma explicação para a garantia de q a partir de q' por A é constituída por restrições de activação ou por fórmulas de interacção. As restrições de activação são impostas sobre acções incluídas na acção composta A. Os gatilhos das fórmulas de interacção são também acções incluídas na acção composta A mas os alvos são acções distintas destas. Tem-se ainda que cada uma das acções em A nunca está envolvida simultaneamente numa restrição de activação e numa fórmula de interacção.

Refira-se que se assume que as condições das restrições de activação e das fórmulas de interacção são conjunções de literais e não disjunções de conjunções de literais como acontecia no caso local (nas condições das restrições de activação). As razões deste facto serão ulteriormente referidas.

Exemplo 4.37 Considere-se a especificação de comunidade de objectos eco descrita no Exemplo 4.25.

A família $\mathcal{E}_1$ apresentada no Exemplo 4.34 é uma explicação por interacção para a preservação de $z^2 \vee x^3 \in CE^{\mathbf{tf}}_{\{2,3\}}$ por $\{a^2, e^3\}$ em eco.

A família $\mathcal{E}_2$ apresentada no Exemplo 4.34 e a família

$$\begin{aligned}\mathcal{E}_3 &= \{E^3_{ob'}\}_{ob' \in \{2,3,\{2,3\}\}} \text{ onde}\\ E^3_3 &= \{\mathbf{G}(\diamond e \Rightarrow x)\}\\ E^3_2 &= E^3_{\{2,3\}} = \emptyset\end{aligned}$$

são explicações por restrição de activação para a preservação de $z^2 \vee x^3 \in CE^{\mathbf{tf}}_{\{2,3\}}$ por $\{a^2, e^3\}$ em eco. Na verdade, como a acção $e \in Acc_3$ não modifica $x \in Atr_3$, a ocorrência de e quando se tem x estabelece $z^2 \vee x^3 \in CE^{\mathbf{tf}}_{\{2,3\}}$ por $\{a^2, e^3\}$. ■

Exemplo 4.38 Considere-se de novo a especificação de comunidade de objectos eco descrita no Exemplo 4.25. A família

$$\begin{aligned}\mathcal{E} &= \{E_{ob'}\}_{ob' \in \{1,3,\{1,3\}\}} \text{ onde}\\ E_1 &= \{\mathbf{G}(\diamond a \Rightarrow (\neg y))\}\\ E_3 &= \{\mathbf{G}(\diamond c \Rightarrow (\neg w))\}\\ E_{\{1,3\}} &= \emptyset\end{aligned}$$

é explicação por restrição de activação para a garantia de $x^1 \wedge w^3 \in CE^{\mathbf{tf}}_{\{1,3\}}$ por $\{a^1, c^3\}$ em eco. ■

Uma forma trivial de assegurar a garantia de q a partir de q' por A é impedir a ocorrência de algum dos elementos de A.

Proposição 4.39 Seja $a \in A$ uma acção não nula e seja

$$\mathcal{RA}_a^{\mathbf{f}} = \{RA_{ob'}^{\mathbf{f}}\}_{ob' \in Sb_{ob}^1 \cup Sb_{ob}^2}$$

tal que $RA_{ob'}^{\mathbf{f}} = \emptyset$ para cada $ob' \in Sb_{ob}^2$ e, para cada $i \in Sb_{ob}^1$, se a é a i-acção de A então $RA_i^{\mathbf{f}} = \{\mathbf{G}(\diamond(\sigma_{ob}^i)_{Acc}^{-1}(a) \Rightarrow \mathbf{f})\}$ e se a não é a i-acção de A então $RA_i^{\mathbf{f}} = \emptyset$. Se $\mathcal{RA}_a^{\mathbf{f}}$ é *eco*-possível então $\mathcal{RA}_a^{\mathbf{f}}$ é explicação para a garantia de q a partir de q' por A.

Prova: Seja eco' o enriquecimento de eco com $\mathcal{RA}_a^{\mathbf{f}}$. Sejam Λ modelo de eco' e $k \in I\!N_0$. Como $\Lambda \models \mathcal{RA}_a^{\mathbf{f}}$ e sendo a a i-acção de A, $i \in Sb_{ob}^1$, tem-se que $\Lambda, k \models_i \neg\nabla(\sigma_{ob}^i)_{Acc}^{-1}(a)$. Assim, $\Lambda, k \models_{ob} \neg\nabla a$ e portanto A garante q a partir de q' em eco'.

Como $\mathcal{RA}_a^{\mathbf{f}}$ é *eco*-possível, existe um modelo Λ de eco que satisfaz $\mathcal{RA}_a^{\mathbf{f}}$ e portanto eco' é coerente. ■

Notação 4.40 No que se segue, sendo $a \in A$ uma acção não nula, denota-se por $\mathcal{RA}_a^{\mathbf{f}}$ a família definida como na Proposição 4.39. Denota-se por

$$(E_{<eco,ob>}^{A,\mathbf{f}})_{RActv}$$

o conjunto de todas as famílias $\mathcal{RA}_a^{\mathbf{f}}$ para alguma acção $a \in A$ não nula e que sejam *eco*-possíveis. ■

Segue-se a noção de explicação por restrição de activação mais liberal relativamente a uma acção.

Definição 4.41 Sejam $\mathcal{RA}_1 = \{RA_{ob'}^1\}_{ob' \in Sb_{ob}^1 \cup Sb_{ob}^2}$ e $\mathcal{RA}_2 = \{RA_{ob'}^2\}_{ob' \in Sb_{ob}^1 \cup Sb_{ob}^2}$ duas explicações por restrição de activação para a garantia de q a partir de q' por A em eco e $a \in A$ uma acção não nula:

- $\mathcal{RA}_1$ é *mais liberal* que $\mathcal{RA}_2$ *relativamente à acção* a sse, sendo a a i-acção de A com $i \in Sb_{ob}^1$, então
  - se $RA_i^2 = \emptyset$ então $RA_i^1 = \emptyset$,
  - se $f_1 \in RA_i^1$ e $f_2 \in RA_i^2$ então $cnd(f_2) \Rightarrow cnd(f_1)$ é válida;
- $\mathcal{RA}_1$ é *estritamente mais liberal que* $\mathcal{RA}_2$ *relativamente à acção* a sse
  - $\mathcal{RA}_1$ é mais liberal que $\mathcal{RA}_2$ relativamente à acção a,
  - $\mathcal{RA}_2$ não é mais liberal que $\mathcal{RA}_1$ relativamente à acção a;
- $\mathcal{RA}_1$ é *(estritamente) mais liberal* que $\mathcal{RA}_2$ sse $\mathcal{RA}_1$ é (estritamente) mais liberal que $\mathcal{RA}_2$ relativamente a a' qualquer que seja acção $a' \in A$ não nula. ■

Proposição 4.42 Seja $\mathcal{RA}$ uma explicação por restrição de activação para a garantia de q a partir de q' por A e $a \in A$ uma acção não nula. A explicação $\mathcal{RA}$ é mais liberal que a explicação $\mathcal{RA}_a^{\mathbf{f}}$ relativamente à acção a.

Prova: Sejam $\mathcal{RA} = \{RA_{ob'}\}_{ob' \in Sb^1_{ob} \cup Sb^2_{ob}}$, $\mathcal{RA}_a^{\mathbf{f}} = \{RA^{\mathbf{f}}_{ob'}\}_{ob' \in Sb^1_{ob} \cup Sb^2_{ob}}$ e suponha-se que a é a i-acção de A, $i \in Sb^1_{ob}$. Por definição, $RA_i^{\mathbf{f}} = \{f\}$ com $cnd(f) = \mathbf{f}$. Se $f' \in RA_i$ então, trivialmente, $\mathbf{f} \Rightarrow cnd(f')$ é válida. ■

Uma outra forma trivial de assegurar a garantia de q a partir de q' por A é impedir que duas acções a_1 e a_2 em A possam ocorrer simultaneamente. Tal pode ser conseguido, por exemplo, através de uma fórmula de interacção que exija que a ocorrência de a_1 assegure também a ocorrência de uma acção a_2' distinta de a_2 e tal que $a_2, a_2' \in (\sigma^i_{ob})_{Acc}(Acc_i)$ para algum $i \in Sb^1_{ob}$.

Proposição 4.43 Sejam $\{i, i'\} \in Sb^2_{ob}$ e $b \in (\sigma^{i'}_{ob})_{Acc}(Acc_{i'})) \backslash A$ uma acção não nula. Seja

$$\mathcal{I}^{\mathbf{t}}_{i,b} = \{I^{\mathbf{t}}_{ob'}\}_{ob' \in Sb^1_{ob} \cup Sb^2_{ob}}$$

a família de conjuntos de fórmulas de interacção tal que $I^{\mathbf{t}}_{\{i,i'\}} = \{\mathbf{G}(\mathbf{t} \Rightarrow (\nabla a_i^A \Rightarrow \nabla b))\}$ e $I^{\mathbf{t}}_{ob'} = \emptyset$ para cada $ob' \in (Sb^1_{ob} \cup Sb^2_{ob}) \backslash \{\{i, i'\}\}$. Se $\mathcal{I}^{\mathbf{t}}_{i,b}$ é *eco*-possível então $\mathcal{I}^{\mathbf{t}}_{i,b}$ é explicação para a garantia de q a partir de q' por A em *eco*.

Prova: Seja *eco'* o enriquecimento de *eco* com $\mathcal{I}^{\mathbf{t}}_{i,b}$. Seja Λ modelo de *eco'* e $k \in I\!N_0$. Dado que $\Lambda \models \mathcal{I}^{\mathbf{t}}_{i,b}$, se $\Lambda, k \models_{\{i,i'\}} \nabla a_i^A$ então $\Lambda, k \models_{\{i,i'\}} \nabla b$. Pelas Definições 4.13, 4.17 e Lema 4.19, $\Lambda, k \models_{ob} \neg \nabla a^A_{i'}$ e portanto A garante q a partir de q' em *eco'*.

Como $\mathcal{I}^{\mathbf{t}}_{i,b}$ é *eco*-possível, existe um modelo Λ de *eco* que satisfaz $\mathcal{I}^{\mathbf{t}}_{i,b}$ e portanto *eco'* é coerente. ■

Notação 4.44 No que se segue, sendo $\{i, i'\} \in Sb^2_{ob}$ e $b \in (\sigma^{i'}_{ob})_{Acc}(Acc_{i'})) \backslash A$ uma acção não nula, denota-se por $\mathcal{I}^{\mathbf{t}}_{i,b}$ a família definida como na Proposição 4.43. Denota-se por

$$(E^{A,\mathbf{t}}_{<eco,ob>})_{Intr}$$

o conjunto das todas famílias $\mathcal{I}^{\mathbf{t}}_{i,b}$ com $\{i, i'\} \in Sb^2_{ob}$ e $b \in (\sigma^{i'}_{ob})_{Acc}(Acc_{i'})) \backslash A$ acção não nula que sejam *eco*-possíveis. ■

Definição 4.45 Sejam $\mathcal{I}_1 = \{I^1_{ob'}\}_{ob' \in Sb^1_{ob} \cup Sb^2_{ob}}$ e $\mathcal{I}_2 = \{I^2_{ob'}\}_{ob' \in Sb^1_{ob} \cup Sb^2_{ob}}$ duas explicações por interacção para a garantia de q a partir de q' por A em *eco*, $i \in Sb^1_{ob}$ tal que a_i^A é acção não nula, $\{i, i'\} \in Sb^2_{ob}$ e $b \in (\sigma^{i'}_{ob})_{Acc}(Acc_{i'})) \backslash A$ acção não nula:

- $\mathcal{I}_1$ é *mais liberal que* $\mathcal{I}_2$ *relativamente ao par de acções* (a_i^A, b) sse
  - se não existe $f \in I^2_{\{i,i'\}}$ tal que $gt(f) = a_i^A$ e $alv(f) = b$ então não existe $f \in I^1_{\{i,i'\}}$ tal que $gt(f) = a_i^A$ e $alv(f) = b$,
  - se $f_1 \in I^1_{\{i,i'\}}$ e $f_2 \in I^2_{\{i,i'\}}$ tal que $gt(f_1) = gt(f_2) = a_i^A$ e $alv(f_1) = alv(f_2) = b$ então $cnd(f_1) \Rightarrow cnd(f_2)$ é válida;

- $\mathcal{I}_1$ é *estritamente mais liberal que* $\mathcal{I}_2$ *relativamente ao par de acções* (a_i^A, b) sse
  - $\mathcal{I}_1$ é mais liberal que $\mathcal{I}_2$ relativamente ao par de acções (a_i^A, b),
  - $\mathcal{I}_2$ não é mais liberal que $\mathcal{I}_1$ relativamente ao par de acções (a_i^A, b);
- $\mathcal{I}_1$ é *(estritamente) mais liberal* que $\mathcal{I}_2$ sse $\mathcal{I}_1$ é (estritamente) mais liberal que $\mathcal{I}_2$ relativamente a qualquer par de acções não nulas (a_j^A, b) com $j \in Sb^1_{ob}$, $\{j, j'\} \in Sb^2_{ob}$ e $b \in (\sigma^{j'}_{ob})_{Acc}(Acc_{j'}))\backslash A$. ∎

Proposição 4.46 Seja $\mathcal{I}$ uma explicação por interacção para a garantia de q a partir de q' por A, $\{i, i'\} \in Sb^2_{ob}$ e $b \in (\sigma^{i'}_{ob})_{Acc}(Acc_{i'}))\backslash A$ uma acção não nula. A explicação $\mathcal{I}$ é mais liberal que a explicação $\mathcal{I}^{\mathbf{t}}_{i,b}$ relativamente ao par de acções (a_i^A, b).

Prova: Sejam $\mathcal{I} = \{I_{ob'}\}_{ob' \in Sb^1_{ob} \cup Sb^2_{ob}}$, $\mathcal{I}^{\mathbf{t}}_{i,b} = \{I^{\mathbf{t}}_{ob'}\}_{ob' \in Sb^1_{ob} \cup Sb^2_{ob}}$. Por definição tem-se que $I^{\mathbf{t}}_{\{i,i'\}} = \{f\}$ com $cnd(f) = \mathbf{t}$. Se $f' \in I_{\{i,i'\}}$ então, trivialmente, $cnd(f') \Rightarrow \mathbf{t}$ é válida. ∎

4.6.2 Fórmulas e tableaux geradores de explicações

Tal como no capítulo anterior, é um determinado conjunto de fórmulas resultantes da especificação *eco* e do problema de garantia em questão, que vai contribuir mais directamente para a construção das explicações. A ideia é novamente escolher um conjunto de constrangimentos de estado cuja incoerência seja condição suficiente para assegurar a garantia em causa.

De novo se assumem fixados $ob \in C_P$, $q, q' \in CE^{\mathbf{tf}}_{ob}$ e $A \in ACC_{ob}$. Assume-se ainda fixada $i_1 \ldots i_m \in Enm(ob)$.

Definição 4.47 O *conjunto de constrangimentos de estado geradores de explicações para garantia de* q *a partir de* q' *por* A *em eco*, $G^{q' \xrightarrow{A} q}_{<eco,ob>}$, define-se do seguinte modo:

$$G^{q' \xrightarrow{A} q}_{<eco,ob>} = G_{RActv} \cup G_{Intr} \cup G_{Obs}$$

onde G_{RActv} é a *componente de* $G^{q' \xrightarrow{A} q}_{<eco,ob>}$ *induzida pelas restrições de activação em eco*, G_{Intr} é a *componente de* $G^{q' \xrightarrow{A} q}_{<eco,ob>}$ *induzida pelas fórmulas de interacção em eco* e G_{Obs} é a *componente de* $G^{q' \xrightarrow{A} q}_{<eco,ob>}$ *induzida pela observação* as quais se definem como segue sendo $b_{i_j} = (\sigma^{i_j}_{ob})^{-1}_{Acc}(a^A_{i_j})$ para cada $1 \leq j \leq m$

- $G_{RActv} = \bigcup_{1 \leq j \leq m} (\sigma^{i_j}_{ob})_F(G^{i_j}_{RActv})$ onde, para cada $1 \leq j \leq m$, $G^{i_j}_{RActv}$ se define indutivamente do seguinte modo:
  - $cnd(AxF_{i_j} \cap RActv1^{b_{i_j}}_{i_j}) \subseteq G^{i_j}_{RActv}$,
  - se $q_1, \ldots, q_n \in G^{i_j}_{RActv}$, $n \geq 1$, e existe $f'_1, \ldots, f'_{n'} \in Enm(AxF_{i_j} \cap RActv2^{b'}_{i_j})$ com $b' \in Acc_{i_j}$, $n' \geq 1$ tal que a fórmula $(q_1 \wedge \ldots \wedge q_n) \Rightarrow (cnd(f'_1) \vee \ldots \vee cnd(f'_{n'}))$ é válida então $cnd(AxF_{i_j} \cap RActv1^{b'}_{i_j}) \subseteq G^{i_j}_{RActv}$;

- $G_{Intr} = \bigcup_{ob' \in Sb^2_{ob}} \{\neg cnd(f) \colon f \in AxF_{ob'} \cap Intr_{ob'}, gt(f) \in A \text{ e } alv(f) \notin A\}$;
- $G_{Obs} = \{q', \neg q[o^A/p^A]\}$ com

$$q[o^A/p^A] = q\,{}^{(\sigma^{i_1}_{ob})_F(o_{1i_1})\ldots(\sigma^{i_1}_{ob})_F(o_{n_1 i_1})\ldots(\sigma^{i_m}_{ob})_F(o_{1i_m})\ldots,(\sigma^{i_m}_{ob})_F(o_{n_m i_m})}_{(\sigma^{i_1}_{ob})_F(p_{1i_1})\ldots(\sigma^{i_1}_{ob})_F(p_{n_1 i_1})\ldots(\sigma^{i_m}_{ob})_F(p_{1i_m})\ldots(\sigma^{i_m}_{ob})_F(p_{n_m i_m})}$$

  sendo

$$\mathbf{G}(\nabla(\sigma^{i_j}_{ob})^{-1}_{Acc}(a^A_{i_j}) \wedge \alpha^{o_{1i_j}\ldots o_{n_j i_j}}_{p_{1i_j}\ldots p_{n_j i_j i}}) \Rightarrow (\mathbf{X}\,\alpha)) \in AxS_{i_j}$$

  para cada $1 \leq j \leq m$. ■

Note-se que, pela Observação 4.24, $AxS_{i_j} \cap S^{b_{i_j}}_{i_j}$ é um conjunto singular para cada símbolo de acção b_{i_j}, para cada $1 \leq j \leq m$. Tem-se também que se $f \in F_{ob'}$ com $ob' \in Sb^2_{ob}$ então $f \in F_{ob}$ e portanto $G_{Intr} \subseteq CE^{\mathbf{tf}}_{ob}$.

Exemplo 4.48 Considere-se uma vez mais a especificação de comunidade de objectos apresentada no Exemplo 4.25. O conjunto de constrangimentos de estado geradores de explicações para a preservação de $z^2 \vee x^3 \in CE^{\mathbf{tf}}_{\{2,3\}}$ por $A' = \{a^2, e^3\}$ em *eco* é

$$G^{z^2 \vee x^3 \xrightarrow{A'} z^2 \vee x^3}_{<eco,\{2,3\}>} = \{z^2 \vee x^3, \neg(z^2 \vee x^3)\,{}^{z^2}_{\neg z^2}\,{}^{w^3}_{\mathbf{f}}\} = \{z^2 \vee x^3, \neg((\neg z^2) \vee x^3)\}.$$

A componente de $G^{z^2 \vee x^3 \xrightarrow{A'} z^2 \vee x^3}_{<eco,\{2,3\}>}$ induzida pelas restrições de activação é $G_{RActv} = \emptyset$, a componente induzida pelas interações é $G_{Intr} = \emptyset$ e a componente induzida pela observação é $G_{Obs} = G^{z^2 \vee x^3 \xrightarrow{A'} z^2 \vee x^3}_{<eco,\{2,3\}>}$. ■

Exemplo 4.49 Considere-se novamente a especificação de comunidade de objectos apresentada no Exemplo 4.25. O conjunto de constrangimentos de estado geradores de explicações para a preservação de $y^1 \wedge z^2 \in CE^{\mathbf{tf}}_{\{1,2\}}$ por $A' = \{c^1, a^2\}$ em *eco* é

$$G^{y^1 \wedge z^2 \xrightarrow{A'} y^1 \wedge z^2}_{<eco,\{1,2\}>} = \{\neg(\neg y^1), y^1 \wedge z^2, \neg(y^1 \wedge z^2)\,{}^{z^1}_{\mathbf{t}}\,{}^{z^2}_{\neg z^2}\} = \{\neg(\neg y^1), y^1 \wedge z^2, \neg(y^1 \vee (\neg z^2))\}.$$

A componente de $G^{y^1 \wedge z^2 \xrightarrow{A'} y^1 \wedge z^2}_{<eco,\{1,2\}>}$ induzida pelas restrições de activação é $G_{RActv} = \emptyset$, a componente induzida pelas interações é $G_{Intr} = \{\neg(\neg y^1)\}$ e a componente induzida pela observação é $G_{Obs} = \{y^1 \wedge z^2, \neg(y^1 \vee (\neg z^2))\}$. ■

Tal como pretendido, a incoerência do conjunto $G^{q' \xrightarrow{A} q}_{<eco,ob>}$ assegura a garantia de q a partir de q' por A em *eco*.

Proposição 4.50 Se $G^{q' \xrightarrow{A} q}_{<eco,ob>}$ é um conjunto impossível então A garante q a partir de q' em *eco*.

Prova: Há que provar que $eco \models_{ob} \mathbf{G}((\nabla a^A_{i_1} \wedge \ldots \wedge \nabla a^A_{i_m} \wedge q') \Rightarrow (\mathbf{X}\,q))$. Seja Λ um modelo de *eco*, $k \in I\!N_0$ e assuma-se que $\Lambda, k \models \nabla a^A_{i_1} \wedge \ldots \wedge \nabla a^A_{i_m} \wedge q'$. Seja $b_{i_j} = (\sigma^{i_j}_{ob})^{-1}_{Acc}(a^A_{i_j})$ para cada $1 \leq j \leq m$ e seja $G^{q' \xrightarrow{A} q}_{<eco,ob>} = G_{RAcvt} \cup G_{Intr} \cup G_{Obs}$ como na Definição 4.47.

(a) Pela Definição 4.26, $\Lambda \models \{AxF_{ob'}\}_{ob' \in C_P}$ e $\Lambda \models \{\iota(AxS_{ob'}, CE_{ob'})\}_{ob' \in C_P}$.

(b) Se, para cada $1 \leq j \leq m$, $\Lambda, k \models_{i_j} G^{i_j}_{RActv}$ então, pelo Lema 4.19, $\Lambda, k \models_{ob} (\sigma^{i_j}_{ob})_F(G^{i_j}_{RActv})$. Seja $1 \leq j \leq m$. A prova de que $\Lambda, k \models_{i_j} G^{i_j}_{RActv}$ decorre por indução estrutural.

Base: seja $p \in cnd(AxF_{i_j} \cap RActv1^{b_{i_j}}_{i_j})$. Dado que $\Lambda, k \models_{ob} \triangledown a^A_{i_j}$, então pelo Lema 4.19, $\Lambda, k \models_{i_j} \triangledown b_{i_j}$. Pela Definição 4.13, $\Lambda, k \models_{i_j} \diamond b_{i_j}$ e consequentemente $\Lambda, k \models_{i_j} p$.

Passo: sejam $q_1, \ldots, q_n \in G^{i_j}_{RActv}$ com $n \geq 1$, $b' \in Acc_{i_j}$ e $f'_1, \ldots, f'_{n'} \in Enm(AxF_{i_j} \cap RActv2^{b'}_{i_j})$, $n' \geq 1$, tal que $(q_1 \wedge \ldots \wedge q_m) \Rightarrow (cnd(f'_1) \vee \ldots \vee cnd(f'_{n'}))$ é válida. Seja $p \in cnd(AxF_{i_j} \cap RActv1^{b'}_{i_j})$. Por hipótese de indução $\Lambda, k \models_{i_j} q_i$ para cada $1 \leq i \leq n$. Pelo Lema 4.21, $\Lambda, k \models_{i_j} q'_{i'}$ para algum $1 \leq i' \leq n'$. Por (a) $\Lambda, k \models_{i_j} q'_{i'} \Rightarrow \diamond b'$ e portanto $\Lambda, k \models_{i_j} \diamond b'$. Novamente por (a) $\Lambda, k \models \diamond b' \Rightarrow p$ e portanto $\Lambda, k \models_{i_j} p$.

(c) Sendo $ob' \in Sb^2_{ob}$ e $f \in F_{ob'}$, $(\sigma^{ob'}_{ob})_F(f) = f$. Seja $p \in G_{Intr}$. Então existe $ob' = \{i_j, i_{j'}\} \in Sb^2_{ob}$, $1 \leq j, j' \leq m$, tal que $f \in AxF_{ob'} \cap Intr_{ob'}$, $p = \neg cnd(f)$, $gt(f) = a^A_{i_j}$ e $alv(f) = b \in (\sigma^{i_{j'}}_{ob'})_{Acc} Acc_{i_{j'}})$. Suponha-se que $\Lambda, k \models_{ob'} cnd(f)$. Então, por (a), e dado que $\Lambda, k \models_{ob} \triangledown a^A_{i_j}$ e consequentemente $\Lambda, k \models_{ob'} \triangledown a^A_{i_j}$, $\Lambda, k \models_{ob'} \triangledown b$. Pelo Lema 4.19, $\Lambda, k \models_{i_{j'}} (\sigma^{i_{j'}}_{ob'})^{-1}_{Acc}(b)$. Dado que $\Lambda, k \models_{ob} \triangledown a^A_{i_{j'}}$, pelo Lema 4.19, $\Lambda, k \models_{i_{j'}} \triangledown(\sigma^{i_{j'}}_{ob'})^{-1}_{Acc}(a^A_{i_{j'}})$. Como $alv(f) \notin A$, então $(\sigma^{i_{j'}}_{ob'})^{-1}_{Acc}(a^A_{i_{j'}}) \neq (\sigma^{i_{j'}}_{ob'})^{-1}_{Acc}(b)$ o que contradiz as Definições 4.13 e 4.17. Conclui-se assim que $\Lambda, k \not\models_{ob'} cnd(f)$, ou seja, $\Lambda, k \models_{ob'} p$ e portanto $\Lambda, k \models_{ob} p$.

(d) Por hipótese, $G^{q' \overset{A}{-} q}_{<eco,ob>}$ é um conjunto impossível e portanto, por (b) e (c), $\Lambda, k \not\models_{ob} G_{Obs}$. Dado que $\Lambda, k \models_{ob} q'$, tem-se que $\Lambda, k \models_{ob} q[o^A/p^A]$ (sendo $q[o^A/p^A]$ como na Definição 4.47). Por (a) e pela Proposição 4.20, $\Lambda, k \models_{ob} (\triangledown a^A_{i_1} \wedge \ldots \wedge \triangledown a^A_{i_m}) \wedge q[o^A/p^A]) \Rightarrow (\mathbf{X}\, q)$. Como, por hipótese, $\Lambda, k \models_{ob} \triangledown a^A_{i_1} \wedge \ldots \wedge \triangledown a^A_{i_m}$, tem-se que $\Lambda, k \models_{ob} \mathbf{X}\, q$. ■

São mantidas todas as notações anteriormente introduzidas relativamente a tableaux e noções associadas simplificando, como se tem vindo a fazer, a referência à assinatura. Assim, em particular, sendo $C \subseteq CE^{\mathbf{tf}}_{ob}$ finito, $T_{ob}(C)$ é o conjunto dos tableaux para C. Recorde-se que o conjunto de todos os fechos sobre $T_{ob}(C)$ é representado por $Fc(C)$.

Proposição 4.51 Se existe $t \in T_{ob}(G^{q' \overset{A}{-} q}_{<eco,ob>})$ fechado então há garantia de q a partir de q' por A em *eco*.

Prova: (a) Pela Proposição 2.41, não existe nenhuma estrutura de interpretação λ sobre $\Sigma = (Acc_{ob}, Atr_{ob})$ tal que $\lambda \models G^{q' \overset{A}{-} q}_{<eco,ob>}$.

(b) Suponha-se, por absurdo, que existe uma estrutura de interpretação de comunidade Λ sobre Σ_{com} tal que $\Lambda \models_{ob} G^{q' \overset{A}{-} q}_{<eco,ob>}$. Pelo Lema 4.21, existe um estrutura de interpretação λ sobre $\Sigma = (Acc_{ob}, Atr_{ob})$ tal que $\lambda \models G^{q' \overset{A}{-} q}_{<eco,ob>}$ o que contradiz (a). Assim, $G^{q' \overset{A}{-} q}_{<eco,ob>}$ é impossível e portanto, pela Proposição 4.50, há garantia de q a partir de q' por A em *eco*. ■

Para além das noções introduzidas na subsubsecção 3.3.3.1, é necessário, neste contexto, introduzir ainda as seguintes noções.

Definição 4.52 Seja $C \subseteq CE_{ob}^{\mathbf{tf}}$ e $Fc \in Fc(C)$. A família de conjuntos de literais

$$\mathcal{F}c = \{Fc_i\}_{i \in Sb_{ob}^1}$$

diz-se *induzida* por $Fc \in Fc(C)$ sse $(\sigma_{ob}^i)_F(Fc_i) = Fc \cap (\sigma_{ob}^i)_F(LE_i)$ para cada $i \in Sb_{ob}^1$. ■

Definição 4.53 Sejam $C \subseteq CE_{ob}^{\mathbf{tf}}$, F um conjunto de famílias de conjuntos de litearis induzidas por elementos de $Fc(C)$ e $i \in Sb_{ob}^1$. A família $\mathcal{F}c = \{Fc_i\}_{i \in Sb_{ob}^1}$ diz-se *família minimal em F relativamente a i* sse

- $\mathcal{F}c \in F$;
- não existe $\mathcal{F}c' \in F$ tal que, sendo $\mathcal{F}c' = \{Fc'_i\}_{i \in Sb_{ob}^1}$, $Fc'_i \subset Fc_i$.

O *conjunto de famílias minimais em F*, $min(F)$, é o conjunto constituído por todas as famílias $\mathcal{F}c = \{Fc_i\}_{i \in Sb_{ob}^1}$ que sejam famílias minimais em F relativamente a todos os elementos de Sb_{ob}^1. ■

As explicações para a garantia de q a partir de q' por A são construídas a partir de fechos de tableaux de decisão abertos para $G_{<eco,ob>}^{q' \xrightarrow{A} q}$.

Proposição 4.54 Se existem tableaux de decisão abertos em $T_{ob}(G_{<eco,ob>}^{q' \xrightarrow{A} q})$ e se tem que $Fc(G_{<eco,ob>}^{q' \xrightarrow{A} q}) = \emptyset$ então A garante $\neg q$ em *eco*.

Prova: (a) Pela Definição 3.24 e Proposição 3.22, qualquer estrutura de interpretação λ sobre $\Sigma = (Acc_{ob}, Atr_{ob})$ é modelo de $G_{<eco,ob>}^{q' \xrightarrow{A} q}$. Suponha-se, por absurdo, que existe uma estrutura de interpretação de comunidade Λ sobre Σ_{com} tal que $\Lambda \not\models_{ob} G_{<eco,ob>}^{q' \xrightarrow{A} q}$. Então $\Lambda \models_{ob} \{p \in G_{<eco,ob>}^{q' \xrightarrow{A} q} : \Lambda \models_{ob} p\} \cup \{\neg p : p \in G_{<eco,ob>}^{q' \xrightarrow{A} q}$ e $\Lambda \not\models_{ob} p\}$. Pelo Lema 4.21 existe uma estrutura de interpretação λ sobre $\Sigma = (Acc_{ob}, Atr_{ob})$ que é modelo deste conjunto e, consequentemente, $\lambda \not\models G_{<eco,ob>}^{q' \xrightarrow{A} q}$. Chega-se deste modo a uma contradição com a asserção inicial, o que significa que qualquer estrutura de interpretação de comunidade Λ sobre Σ_{com} é tal que $\Lambda \models_{ob} G_{<eco,ob>}^{q' \xrightarrow{A} q}$.

(b) Sejam Λ um modelo de *eco*, com $\Lambda(ob) = (ob, \lambda_{ob})$ para cada $ob \in C_P$, e $k \in I\!N_0$ tal que $\Lambda, k \models \nabla a_{i_1}^A \wedge \ldots \wedge a_{i_m}^A$. Pelas Observação 4.24, Definição 4.26 e Proposição 4.20, $\Lambda, k \models \nabla(a_{i_1}^A \wedge \ldots \wedge a_{i_m}^A \wedge p[o^A/p^A]) \Rightarrow (\mathbf{X}\, p)$ qualquer que seja $p \in CE_{ob}^{\mathbf{tf}}$, sendo $p[o^A/p^A]$ como na Definição 4.47. Seja Λ' uma estrutura de interpretação de comunidade sobre Σ_{com} tal que $\Lambda'(ob) = (ob, \lambda'_{ob})$ para cada $ob \in C_P$ com $\lambda'_{ob}(k') = \lambda_{ob}(k' + k)$ para todo $k' \in I\!N_0$. Por (a), $\Lambda' \models_{ob} G_{<eco,ob>}^{q' \xrightarrow{A} q}$ e portanto, em particular $\Lambda, 0 \models_{ob} \neg q[o^A/p^A]$ sendo $q[o^A/p^A]$ como na Definição 4.47. Pelo Lema 2.12, $\Lambda', 0 \models_{ob} (\neg q)[o^A/p^A]$. Pelo Lema 4.21, $\Lambda, k \models (\neg q)[o^A/p^A]$ e portanto $\Lambda, k \models \mathbf{X}(\neg q)$. Pela Definição 4.35 tem-se que A garante $\neg q$ em *eco*. ■

Definição 4.55 A família de conjuntos de literais $\mathcal{F}c = \{Fc_i\}_{i \in Sb_{ob}^1}$ diz-se *família relevante para a geração de explicações para a garantia de q a partir de q' por A em eco* sse $\mathcal{F}c$ é induzida por algum $Fc \in Fc(G_{<eco,ob>}^{q' \xrightarrow{A} q})$ e $Fc_i = \emptyset$ para todo $i \in Sb_{ob}^1$ tal que a_i^A é uma acção nula. O conjunto destas famílias denota-se por $\mathcal{F}c_{<eco,ob>}^{q' \xrightarrow{A} q}$. ■

4.6.3 Geração de explicações

Assumem-se novamente fixados $ob \in C_P$, $q, q' \in CE^{\mathbf{tf}}_{ob}$, $A \in ACC_{ob}$ e $i_1 \ldots i_m \in Enm(ob)$. Nesta subsecção descreve-se o modo de construir explicações para a garantia de q a partir de q' por A em *eco* a partir de famílias em $\mathcal{F}c^{q' \underline{A} q}_{<eco,ob>}$.

Definição 4.56 Seja $\mathcal{L} = \{L_i\}_{i \in Sb^1_{ob}}$ com $L_i \subseteq LE_i$ para cada $i \in Sb^1_{ob}$. A família de conjuntos de restrições de activação e fórmulas de interacção

$$\mathcal{E} = \{E_{ob'}\}_{ob' \in Sb^1_{ob} \cup Sb^2_{ob}}$$

diz-se *induzida por* $\mathcal{L}$ sse

- $E_i \subseteq RActv_i^{(\sigma^i_{ob})^{-1}_{Acc}(a^A_i)}$ para cada $i \in Sb^1_{ob}$
- $E_{\{i,i'\}} \subseteq Intr^{a^A_i, b_{i'}}_{\{i,i'\}} \cup Intr^{a^A_{i'}, b_i}_{\{i,i'\}}$ para cada $\{i, i'\} \in Sb^2_{ob}$, com $b_i \in (\sigma^i_{\{i,i'\}})_{Acc}(Acc_i) \backslash A$ e $b_{i'} \in (\sigma^{i'}_{\{i,i'\}})_{Acc}(Acc_{i'}) \backslash A$,
- para cada $i \in Sb^1_{ob}$
  - $E_i \cup \{f \in E_{\{i,i'\}} : \{i, i'\} \in Sb^2_{ob}$ e $gt(f) = a^A_i\}$ é vazio ou singular;
  - se $L_i = \emptyset$ então o conjunto $E_i \cup \{f \in E_{\{i,i'\}} : \{i, i'\} \in Sb^2_{ob}$ e $gt(f) = a^A_i\}$ é vazio,
  - se $L_i \neq \emptyset$ então alguma das seguintes condições se verifica
    * $E_i = \{\mathbf{G}(\diamond(\sigma^i_{ob})^{-1}_{Acc}(a^A_i) \Rightarrow l_1 \wedge \ldots \wedge l_n)\}$ com $l_1 \ldots l_n \in Enm(L_i)$
    * existem $\{i, i'\} \in Sb^2_{ob}$ e $f \in E_{\{i,i'\}}$ tal que $gt(f) = a^A_i$, $cnd(f) = (\sigma^i_{\{i,i'\}})_F(\overline{l})$ se $L_i = \{l\}$ é singular e $cnd(f) = \neg((\sigma^i_{\{i,i'\}})_F(l_1 \wedge \ldots \wedge l_n))$ com $l_1 \ldots l_n \in Enm(L_i)$ caso contrário.

Se $E_{\{i,i'\}} = \emptyset$ para cada $\{i, i'\} \in Sb^2_{ob}$ dir-se-á que a família $\mathcal{E}$ é uma família de conjuntos de restrições de activação induzida por $\mathcal{L}$. Se $E_i = \emptyset$ para cada $i \in Sb^1_{ob}$ dir-se-á que a família $\mathcal{E}$ é uma família de conjuntos de interacções $\mathcal{L}$. ∎

Note-se que da definição anterior decorre que a família induzida por $\mathcal{L}$ verifica os requisitos sintácticos da Definição 4.36. Tem-se, nomeadamente, que para cada $i \in Sb^1_{ob}$ a acção a^A_i não está simultaneamente envolvida numa restrição de activação e numa fórmula de interacção. Para cada $i \in Sb^1_{ob}$, os literais contidos em cada $L_i \neq \emptyset$ vão dar origem à condição de uma única fórmula a qual poderá ser uma restrição de activação ou uma fórmula de interação.

Exemplo 4.57 O tableau t representado na Figura 4.1 é um tableau de decisão em $T_{\{2,3\}}(G^{z^2 \vee x^3 \underline{A'} z^2 \vee x^3}_{<eco,\{2,3\}>})$ sendo $G^{z^2 \vee x^3 \underline{A'} z^2 \vee x^3}_{<eco,\{2,3\}>}$ o conjunto construído no Exemplo 4.48.

A família $\mathcal{F}c_1 = \{Fc^1_i\}_{i \in \{2,3\}}$ onde $Fc^1_2 = \{\neg z\}$ e $Fc^1_3 = \emptyset$ é induzida pelo fecho $\{\neg z^2\}$ de t, a família $\mathcal{F}c_2 = \{Fc^2_i\}_{i \in \{2,3\}}$ onde $Fc^2_2 = \emptyset$ e $Fc^2_3 = \{x\}$ é induzida pelo fecho $\{x^3\}$ de t e $\mathcal{F}c_1, \mathcal{F}c_2 \in \mathcal{F}c^{z^2 \vee x^3 \underline{A'} z^2 \vee x^3}_{<eco,\{2,3\}>}$.

$$z^2 \vee x^3$$
$$\neg((\neg z^2) \vee x^3)$$
$$\neg(\neg z^2)$$
$$\neg x^3$$
$$z^2$$
$$z^2 \qquad\qquad x^3$$
$$\qquad\qquad\quad \times$$

Figura 4.1: Tableau de decisão para $\{z^2 \vee x^3, \neg((\neg z^2) \vee x^3)\}$

As famílias $\mathcal{E}_2$ e $\mathcal{E}_3$ referidas no Exemplo 4.37 são famílias de conjuntos de restrições de activação induzidas por $\mathcal{F}c_1$ e $\mathcal{F}c_2$, respectivamente.

A família $\mathcal{E}_1$ descrita no Exemplo 4.34 é uma família de fórmulas de interacção induzida por $\mathcal{F}c_1$. ■

Exemplo 4.58 Considere-se a especificação de comunidade de objectos apresentada no Exemplo 4.25. O conjunto de constrangimentos de estado geradores de explicações para a garantia de de $x^1 \wedge w^3 \in CE^{\mathbf{tf}}_{\{1,3\}}$ por $A' = \{a^1, c^3\}$ em eco é

$$G^{\mathbf{t} \stackrel{A'}{\rightarrow} x^1 \wedge w^3}_{<eco,\{1,3\}>} = \{\mathbf{t}, \neg(x^1 \wedge w^3)\,{}^{x^1}_{\neg y^1}\,{}^{z^1}_{\neg z^1}\,{}^{x^3}_{\mathbf{t}}\,{}^{w^3}_{\neg w^3}\} = \{\mathbf{t}, \neg((\neg y^1) \wedge (\neg w^3))\}.$$

Como facilmente se verifica, $Fc = \{\neg y^1, \neg w^3\}$ é o único fecho de qualquer tableau de decisão em $T_{\{1,3\}}(G^{\mathbf{t} \stackrel{A'}{\rightarrow} x^1 \wedge w^3}_{<eco,\{1,3\}>})$. A família $\mathcal{F}c_1 = \{Fc^1_i\}_{i \in \{1,3\}}$ onde $Fc^1_1 = \{\neg y\}$ e $Fc^1_3 = \{\neg w\}$ é induzida pelo fecho Fc. A família $\mathcal{E}$ referida no Exemplo 4.38 é a família de conjuntos de restrições de activação induzida por $\mathcal{F}c$. ■

Proposição 4.59 Se $\mathcal{E} = \{E_{ob'}\}_{ob' \in Sb^1_{ob} \cup Sb^2_{ob}}$ é uma família de conjuntos de restrições de activação e fórmulas de interacção induzida por $\mathcal{F}c \in \mathcal{F}c^{q' \stackrel{A}{\rightarrow} q}_{<eco,ob>}$ e $\mathcal{E}$ é *eco*-possível então $\mathcal{E}$ é uma explicação para a garantia de q a partir de q' por A em *eco*.

Prova: Seja eco' o enriquecimento de eco com $\mathcal{E}$.

(a) Os requisitos sintácticos da Definição 4.36 são satisfeitos pela Definição 4.55 e tendo em conta a Definição 4.56.

(b) Seja $G = G^{q' \stackrel{A}{\rightarrow} q}_{<eco,ob>} \cup (\bigcup_{ob' \in Sb^1_{ob}} \sigma^{ob'}_{ob})_F(cnd(E_{ob'})) \cup (\bigcup_{ob' \in Sb^2_{ob}} \{\neg p : p \in cnd(E_{ob'})\})$. Pela Definição 4.47, para qualquer estrutura de interpretação Λ sobre Σ_{com}, se $\Lambda \models_{ob} G^{q' \stackrel{A}{\rightarrow} q}_{<eco',ob>}$ então $\Lambda \models_{ob} G$. Pelas Proposições 3.21 e 4.21 e sendo $\mathcal{F}c = \{Fc_i\}_{i \in Sb^1_{ob}}$, tem-se que $G^{q' \stackrel{A}{\rightarrow} q}_{<eco,ob>} \cup (\bigcup_{i \in Sb^1_{ob}} \{(\sigma^i_{ob})_F(Fc_i)\})$. Tendo em conta as Definições 4.52, 4.55 e 4.56

tem-se que G é impossível e consequentemente $G^{q' \xrightarrow{A} q}_{<eco',ob>}$ é impossível. Pela Proposição 4.50, A garante q a partir de q' em eco'.

(c) Dado que, por hipótese, $\mathcal{E}$ é *eco*-possível tem-se que eco' é coerente. ∎

Note-se que se se tomassem vários elementos de $\mathcal{F}c^{q' \xrightarrow{A} q}_{<eco,ob>}$ para construir as potenciais explicações de um modo semelhante ao que se fez no caso local, não seria agora possível, em geral, assegurar a garantia desejada.

Definição 4.60 Seja $F \subseteq \mathcal{F}c^{q' \xrightarrow{A} q}_{<eco,ob>}$ não vazio:

- o *conjunto das explicações por restrição de activação para a garantia de q a partir de q′ por A em eco induzido por F* denota-se por

  $$E_{RActv}(F)$$

  e é tal que $\mathcal{RA} \in E_{RActv}(F)$ sse $\mathcal{RA}$ é uma família de conjuntos de restrições de activação induzida por alguma família $\mathcal{F}c \in F$ e $\mathcal{RA}$ é *eco*-possível;

- o *conjunto das explicações por interacção para a garantia de q a partir de q′ por A em eco induzido por F* denota-se por

  $$E_{Intr}(F)$$

  e é tal que $\mathcal{I} \in E_{Intr}(F)$ sse $\mathcal{I}$ é uma família de conjuntos de restrições de activação induzida por $\mathcal{F}c \in F$ e $\mathcal{I}$ é *eco*-possível. ∎

Exemplo 4.61 São elementos de $E_{RActv}(\mathcal{F}c^{z^2 \vee x^3 \xrightarrow{A'} z^2 \vee x^3}_{<eco,\{2,3\}>})$ as famílias $\mathcal{E}_2$ e $\mathcal{E}_3$ referidas no Exemplo 4.57.

A família $\mathcal{E}_1$ do Exemplo 4.34 pertence a $E_{Intr}(\mathcal{F}c^{z^2 \vee x^3 \xrightarrow{A'} z^2 \vee x^3}_{<eco,\{2,3\}>})$. ∎

Exemplo 4.62 A família $\mathcal{E}$ do Exemplo 4.58 pertence a $E_{RActv}(\mathcal{F}c^{\mathbf{t} \xrightarrow{A'} y^1 \wedge w^3}_{<eco,\{1,3\}>})$. ∎

Proposição 4.63 Seja $F \subseteq \mathcal{F}c^{q' \xrightarrow{A} q}_{<eco,ob>}$. Se $\mathcal{RA} \in E_{RActv}(F)$ é induzida por $\mathcal{F}c \in min(F)$ então não existe $\mathcal{RA}' \in E_{RActv}(F)$ estritamente mais liberal que $\mathcal{RA}$.

Prova: Seja $\mathcal{F}c = \{Fc_i\}_{i \in Sb^1_{ob}}$ e suponha-se, por absurdo, que existe $\mathcal{RA}' \in E_{RActv}(F)$ estritamente mais liberal que $\mathcal{RA}$. Seja $\mathcal{RA}'$ induzida por $\mathcal{F}c' = \{Fc'_i\}_{i \in Sb^1_{ob}} \in F$. Tendo em conta as Definições 4.41 e 4.56, $Fc'_i \subseteq Fc_i$ para cada $i \in Sb^1_{ob}$ e $Fc'_i \subset Fc_i$ para algum $i \in Sb^1_{ob}$. Dado que $\mathcal{F}c \in min(F)$, não existem $i'' \in Sb^1_{ob}$ e $\mathcal{F}c'' = \{Fc''_i\}_{i \in Sb^1_{ob}} \in F$ tal que $Fc''_i \subset Fc_i$. Chega-se assim a uma contradição o que permite concluir que não existe $\mathcal{RA}' \in E_{RActv}(F)$ estritamente mais liberal que $\mathcal{RA}$. ∎

Proposição 4.64 Seja $F \subseteq \mathcal{F}c^{q' \xrightarrow{A} q}_{<eco,ob>}$. Se $\mathcal{I} \in E_{Intr}(F)$ é induzida por $\mathcal{F}c \in min(F)$ então não existe $\mathcal{I}' \in E_{Intr}(F)$ estritamente mais liberal que $\mathcal{I}$.

Prova: Semelhante à prova apresentada para a Proposição 4.63 recorrendo agora à Definição 4.45. ∎

Proposição 4.65 Sejam *eco* uma especificação de comunidade de objectos tal que A não garante q a partir de q' em *eco* e $\mathcal{RA} \notin (E^{A,\mathbf{f}}_{<eco,ob>})_{RActv}$ explicação por restrição de activação para a garantia de q a partir de q' por A em *eco*. Se é impossível o conjunto $G^{q' \overset{A}{\to} q}_{<eco,ob>} \cup (\bigcup_{i \in Sb^1_{ob}} (\sigma^i_{ob})_F(cnd(RA_i)))$ então existe $\mathcal{RA}' \in E_{RActv}(\mathcal{F}c^{q' \overset{A}{\to} q}_{<eco,ob>})$ mais liberal que $\mathcal{RA}$.

Prova: Seja $\mathcal{RA} = \{RA_{ob'}\}_{ob' \in Sb^1_{ob} \cup Sb^2_{ob}}$. Pela Definição 4.36, tem-se que $RA_{ob'} = \emptyset$ para cada $ob' \in Sb^2_{ob}$ e, para cada $i \in Sb^1_{ob}$, se $RA_i \neq \emptyset$ então a^A_i não é acção nula e $RA_i = \{f\}$ com $cnd(f) = l_1 \wedge \ldots \wedge l_k$, $k \geq 1$, $l_j \in LE_i$ para cada $1 \leq j \leq k$ e $l_j \neq \overline{l_{j'}}$ quaisquer que sejam $1 \leq j, j' \leq k$.

Seja $t = ((N, \leq), e) \in T_{ob}(G^{q' \overset{A}{\to} q}_{<eco,ob>})$ tableau de decisão. Pela Proposição 4.51, como A não garante q a partir de q' em *eco*, t é tableau aberto. Seja $\rho_1 \ldots \rho_r \in Enm(RAbt(t))$.

Sejam $i'_1 \ldots i'_{m'} \in Enm(\{i \in Sb^1_{ob} : RA_i \neq \emptyset\})$ e $RA_{i'_j} = \{f_{i'_j}\}$ para cada $1 \leq j \leq m'$. Considere-se um tableau de decisão t' para o conjunto $G^{q' \overset{A}{\to} q}_{<eco,ob>} \cup \{p\}$ sendo $p = (\sigma^{i'_1}_{ob})_F(cnd(f_{i'_1})) \wedge \ldots \wedge (\sigma^{i'_{m'}}_{ob})_F(cnd(f_{i'_{m'}})) = l'_1 \wedge \ldots \wedge l'_{n'}$ obtido a partir de t de um modo semelhante ao utilizado na prova da Proposição 3.38 para obter o tableau para o conjunto $G^{q' \overset{a}{\to} q}_{eob} \cup \{q_1 \vee \ldots \vee q_n\}$ a partir do tableau em $T_\Sigma(G^{q' \overset{a}{\to} q}_{eob})$. Dado que o conjunto $G^{q' \overset{A}{\to} q}_{<eco,ob>} \cup (\bigcup_{ob' \in Sb^1_{ob}} (\sigma^{ob'}_{ob})_F(cnd(RA_{ob'})))$ é impossível, pela Proposição 2.41, t' é tableau fechado.

Seguindo raciocínio análogo ao utilizado na prova da Proposição 3.38, conclui-se que para cada $1 \leq k \leq r$ existe $1 \leq j_k \leq n'$ tal que $\overline{l'_{j_k}} \in e_1(\rho_k) \cap LE_{ob}$, l'_{j_k} pertence ao fecho de ρ_k e $Fc = \{l'_{j_1}, \ldots, l'_{j_r}\} \in Fc(G^{q' \overset{A}{\to} q}_{<eco,ob>})$.

Seja $\mathcal{F}c = \{Fc_i\}_{i \in Sb^1_{ob}}$ a família de conjuntos de literais induzida por Fc. Se a^A_i é acção nula para algum $i \in Sb^1_{ob}$ tal que $Fc_i \neq \emptyset$ então ter-se-á que $RA_i \neq \emptyset$ o que contradiz a definição de $\mathcal{RA}$. Pela Definição 4.55, $\mathcal{F}c \in \mathcal{F}c^{q' \overset{A}{\to} q}_{<eco,ob>}$.

Seja $\mathcal{RA}' = \{RA'_{ob'}\}_{ob' \in Sb^1_{ob} \cup Sb^2_{ob}}$ uma família de conjuntos de restrições de activação induzida por $\mathcal{F}c$. Uma vez que $\mathcal{RA}$ é *eco*-possível tem-se que $\mathcal{RA}'$ é também *eco*-possível e consequentemente $\mathcal{RA}' \in E_{RActv}(\mathcal{F}c^{q' \overset{A}{\to} q}_{<eco,ob>})$. Tendo em conta a Definição 4.41, $\mathcal{RA}'$ é mais liberal que $\mathcal{RA}$. ∎

Proposição 4.66 Sejam *eco* uma especificação de comunidade de objectos tal que A não garante q a partir de q' em *eco* e $\mathcal{I} \notin (E^{A,\mathbf{t}}_{<eco,ob>})_{Intr}$ explicação por interacção para a garantia de q a partir de q' por A em *eco*. Se $G^{q' \overset{A}{\to} q}_{<eco,ob>} \cup (\bigcup_{ob' \in Sb^2_{ob}} \{\neg p \colon p \in cnd(I_{ob'})\})$ é impossível então existe $\mathcal{I}' \in E_{Intr}(\mathcal{F}c^{q' \overset{A}{\to} q}_{<eco,ob>})$ mais liberal que $\mathcal{I}$.

Prova: Seja $\mathcal{I} = \{I_{ob'}\}_{ob' \in Sb^1_{ob} \cup Sb^2_{ob}}$. Pela Definição 4.36 tem-se que $I_{ob'} = \emptyset$ para cada $ob' \in Sb^1_{ob}$ e, para cada $ob' \in Sb^2_{ob}$, se $f \in I_{ob'}$ então $gt(f)$ é acção não nula e $cnd(f) = \neg(l_1 \wedge \ldots \wedge l_k)$ com $k \geq 1$, $l_j \in LE_{ob'}$ para cada $1 \leq j \leq k$ e $l_j \neq \overline{l_{j'}}$ quaisquer que sejam $1 \leq j, j' \leq k$. Seja $I = \bigcup_{ob' \in Sb^2_{ob}} I_{ob'}$. Tem-se ainda que para cada $i \in Sb^1_{ob}$ existe no máximo uma fórmula $f \in I$ tal que $gt(f) = a^A_i$. Designe-se tal fórmula, sempre que exista, por $f^{\mathcal{I}}_{a^A_i}$.

Seja $t=((N,\leq),e)\in T_{ob}(G^{q' \xrightarrow{A} q}_{<eco,ob>})$ tableau de decisão. Pela Proposição 4.51, como A não garante q a partir de q' em eco, t é tableau aberto. Seja $\rho_1 \dots \rho_r \in Enm(RAbt(t))$.

Seja $\neg p'_1 \dots \neg p'_{m'} \in Enm(cnd(I))$. Considere-se um tableau de decisão t' para o conjunto $G^{q' \xrightarrow{A} q}_{<eco,ob>} \cup \{p\}$ sendo $p = p_1 \wedge \dots \wedge p_{m'} = l'_1 \wedge \dots \wedge l'_{n'}$ obtido a partir de t de um modo semelhante ao utilizado na prova da Proposição 3.38 para obter o tableau para o conjunto $G^{q' \xrightarrow{a} q}_{eob} \cup \{q_1 \vee \dots \vee q_n\}$ a partir do tableau em $T_\Sigma(G^{q' \xrightarrow{a} q}_{eob})$. Dado que $G^{q' \xrightarrow{A} q}_{<eco,ob>} \cup (\bigcup_{ob' \in Sb^2_{ob}} \{\neg p : p \in (cnd(I_{ob'}))\})$ é impossível, pela Proposição 2.41, t' é tableau fechado.

Seguindo raciocínio análogo ao utilizado na prova da Proposição 3.38, conclui-se que para cada $1 \leq k \leq r$ existe $1 \leq j_k \leq n'$ tal que $\overline{l'_{j_k}} \in e_1(\rho_k) \cap LE_{ob}$, l'_{j_k} pertence ao fecho de ρ_k e $Fc = \{l'_{j_1}, \dots, l'_{j_r}\} \in Fc(G^{q' \xrightarrow{A} q}_{<eco,ob>})$.

Seja $\mathcal{F}c = \{Fc_i\}_{i \in Sb^1_{ob}}$ a família de conjuntos de literais induzida por Fc. Se a^A_i é acção nula para algum $i \in Sb^1_{ob}$ tal que $Fc_i \neq \emptyset$ então existe a fórmula $f^{\mathcal{I}}_{a^A_i}$ o que contradiz a definição de $\mathcal{I}$. Pela Definição 4.55, $\mathcal{F}c \in \mathcal{F}c^{q' \xrightarrow{A} q}_{<eco,ob>}$.

Seja $\mathcal{I}' = \{I'_{ob'}\}_{ob' \in Sb^1_{ob} \cup Sb^2_{ob}}$ uma família de conjuntos de interaccções induzida por $\mathcal{F}c$ tal que para cada $i \in Sb^1_{ob}$ tal que $Fc_i \neq \emptyset$ se tem que sendo $ob' \in Sb^2_{ob}$ tal que $f \in I'_{ob'}$ e $gt(f) = a^A_i$ então $alv(f) = alv(f^{\mathcal{I}}_{a^A_i})$. Uma vez que $\mathcal{I}$ é eco-possível tem-se que $\mathcal{I}'$ é também eco-possível e consequentemente $\mathcal{I}' \in E_{Intr}(\mathcal{F}c^{q' \xrightarrow{A} q}_{<eco,ob>})$. Tendo em conta a Definição 4.45, $\mathcal{I}'$ é mais liberal que $\mathcal{I}$. ∎

4.6.4 Alguns critérios de preferência

Quanto a critérios de preferência entre explicações, para além de se poderem adoptar os critérios referidos anteriormente, podem ainda referir-se alguns critérios mais directamente relacionados com as características específicas deste novo contexto.

Assim, preferindo as explicações mais liberais restringe-se menos a possibilidade de ocorrência das acções envolvidas. Por outro lado, uma explicação por restrição de activação induzida por $\mathcal{F}c \in \mathcal{F}c^{q' \xrightarrow{A} q}_{<eco,ob>}$, onde $\mathcal{F}c$ é uma família de literais induzida por um elemento de $Fc(G_{RActv} \cup G_{Intr})$, é tal que A garante p a partir de p' no enriquecimento de eco com a referida explicação quaisquer que sejam $p, p' \in CE^{\mathbf{tf}}_{ob}$. Estas explicações não são muito interessantes pois não têm em conta a particular garantia que se pretende estabelecer.

Considere-se agora o Exemplo 4.37 no qual se referem as famílias $\mathcal{E}_2$ e $\mathcal{E}_3$ como explicações por restrição de activação para a preservação de $z^2 \vee x^3 \in CE^{\mathbf{tf}}_{\{2,3\}}$ por $\{a^2, e^3\}$ em eco. A família $\mathcal{E}_3$ é menos interessante que a família $\mathcal{E}_2$. Isto deve-se a que $\mathcal{E}_3$ impõe uma restrição ao comportamento de uma acção que não contribui directamente para a não preservação de $z^2 \vee x^3$. Isto não se passa com $\mathcal{E}_2$ dado que, de facto, é a que pode contribuir para a não preservação de $z^2 \vee x^3$. Note-se que existe mais uma acção composta envolvendo a^2, o conjunto $\{a^2, \perp^3\}$, que não preserva $z^2 \vee x^3$ enquanto que todas as acções compostas envolvendo e^3, excepto $\{a^2, e^3\}$, preservam $z^2 \vee x^3$.

No âmbito da construção de explicações para a garantia de $q \in CE_{ob}^{\mathbf{tf}}$ a partir de $q' \in CE_{ob}^{\mathbf{tf}}$ por $A \in ACC_{ob}$, uma forma de detectar situações do tipo da descrita no parágrafo anterior consiste na análise dos outros elementos de ACC_{ob} quanto à referida garantia. Serão mais interessantes as explicações que envolvam restrições de activação sobre acções que façam parte de um maior número de acções compostas que não garantam q a partir de q'.

Pode fazer-se um raciocínio semelhante para o caso de explicações por interacção. Considerando ainda o caso da preservação de $z^2 \vee x^3$ por $\{a^2, e^3\}$, tem-se que a família $\mathcal{E}_4 = \{E_{ob'}^4\}_{ob' \in \{2,3,\{2,3\}\}}$ onde $E_{\{2,3\}}^4 = \{\mathbf{G}((\neg x^3) \Rightarrow (\nabla e^3 \Rightarrow \nabla d^2))\}$ e $E_2^4 = E_3^4 = \emptyset$ é uma explicação por interacção para a preservação referida e é induzida pela família de literais $\mathcal{F}c_2$ referida no Exemplo 4.57. Dado que não é a acção e que contribui para a não preservação de $z^2 \vee x^3$, a explicação $\mathcal{E}_1$ é neste caso mais interessante.

Ainda relativamente a explicações por interacção, considere-se o seguinte exemplo.

Exemplo 4.67 Considere-se a especificação de comunidade de objectos *eco* descrita no Exemplo 4.25. A acção composta $\{a^2, \perp^3\}$ não preserva $z^2 \vee x^3 \in O_{\{2,3\}}$. A família

$$\begin{aligned} \mathcal{I} = \{I_{ob'}\}_{ob' \in \{2,3,\{2,3\}\}} & \text{ onde} \\ & I_{\{2,3\}} = \{\mathbf{G}(z^2 \Rightarrow (\nabla a^2 \Rightarrow \nabla e^3))\} \\ & I_2 = I_3 = \emptyset \end{aligned}$$

é explicação por interacção para a preservação de $z^2 \vee x^3$ por $\{a^2, \perp^3\}$ em *eco*. Mas a acção composta $\{a^2, e^3\}$ não preserva $z^2 \vee x^3$. Se a procura de uma explicação para esta preservação se insere num objectivo mais geral, como por exemplo assegurar a invariância de $z^2 \vee x^3$ (ver Exemplo 4.93), esta explicação não é muito interessante. ■

Assim, não será muito interessante uma explicação $\mathcal{E} = \{E_{ob'}\}_{ob' \in Sb_{ob}^1 \cup Sb_{ob}^2}$ para a garantia de $q \in CE_{ob}^{\mathbf{tf}}$ a partir de $q' \in CE_{ob}^{\mathbf{tf}}$ por $A \in ACC_{ob}$ na qual exista uma fórmula de interacção $f \in E_{ob'}$, $ob' \in Sb_{ob}^2$, tal que $\{gt(f), alv(f)\}$ não está contido em nenhuma acção composta $A' \in ACC_{ob}$ que garanta q a partir de q'. No caso em que não existam acções compostas contendo $gt(f)$ que garantam q a partir de q' não terá interesse considerar explicações por interacção que envolvam $gt(f)$.

Ainda relativamente a fórmulas de interacção, suponha-se que foi construída, a partir de $\mathcal{F}c \in \mathcal{F}c_{<eco,ob>}^{q' \xrightarrow{A} q}$ a explicação $\mathcal{E} = \{E_{ob'}\}_{ob' \in Sb_{ob}^1 \cup Sb_{ob}^2}$ verificando as seguintes condições: (i) $\mathbf{G}((\neg p_i) \Rightarrow (\nabla a^i \Rightarrow \nabla b^{i'})) \in E_{\{i,i'\}}$, $\{i, i'\} \in Sb_{ob}^2$, $a \in Acc_i$, $b \in Acc_{i'}$, $p_i = (\sigma_{\{i,i'\}}^i)_F(p)$, (ii) $f' \in AxF_{\{i,i'\}} \cap Intr_{\{i,i'\}}^{a^i, c^{i'}}$, $c \in Acc_{i'}$, (iii) $(\neg p_i) \Rightarrow cnf(f')$ é válida e (iv) $b \neq c$. Esta explicação não é muito interessante pois no enriquecimento de *eco* com $\mathcal{E}$ sempre que se tenha $\neg p$, a acção a não pode ocorrer. Este tipo de restrição pode ser conseguido de uma forma mais clara através da restrição de activação $\mathbf{G}(\diamond a \Rightarrow p)$ que pode ser também construída a partir de $\mathcal{F}c$.

Quanto à escolha entre explicações que envolvam restrições de activação sobre uma acção e explicações que envolvam fórmulas de interacção tendo essa acção por gatilho, estas últimas podem ser interessantes em situações como as descritas no Exemplo 4.34. Nas situações em que a restrição de activação impede a ocorrência de uma acção $a \in Acc_i$, $i \in ob$, quando se verifica $q \in CE_i^{\mathbf{tf}}$, uma alternativa a esta restrição pode ser conseguida através de uma fórmula de interacção em que se permite a ocorrência de a quando se tem q desde tal implique a ocorrência de uma acção $b \in Acc_{i'}$, $i' \in ob \backslash \{i\}$, e que a ocorrência simultânea destas acções assegure a garantia em causa.

4.7 Geração de explicações para a garantia inicial de um constrangimento de estado

Nesta secção descreve-se o modo de construir famílias de constrangimentos de estado que assegurem que um dado constrangimento de estado é verificado no instante inicial.

No que se segue assumem-se fixados $ob \in C_P$, $i_1 \dots i_m \in Enm(ob)$ e $q \in CE_{ob}^{\mathbf{tf}}$.

Definição 4.68 Diz-se que existe *garantia inicial de q em eco* sempre que $eco \models_{ob} q$. ■

Definição 4.69 Uma *explicação para a garantia inicial de q em eco* é uma família de conjuntos

$$\mathcal{CI} = \{CI_{ob'}\}_{ob' \in Sb^1_{ob} \cup Sb^2_{ob}}$$

onde

- $CI_i \subseteq CE_i^{\mathbf{tf}}$ é um conjunto singular ou vazio para cada $i \in Sb^1_{ob}$ e $CI_{\{i,i'\}}$ é um conjunto vazio para cada $\{i,i'\} \in Sb^2_{ob}$,
- se $p \in CI_i$, $i \in Sb^1_{ob}$, então $p = l_1 \wedge \dots \wedge l_n$ com $n \geq 1$ e $l_j \in LE_i$ para cada $1 \leq j \leq n$

tal que, sendo eco' o enriquecimento de eco com $\mathcal{CI}$,

- existe garantia inicial de q em eco',
- eco' é coerente. ■

Exemplo 4.70 Considere-se uma vez mais a especificação de comunidade de objectos eco descrita no exemplo 4.25. A família

$$\mathcal{CI} = \{CI_{ob'}\}_{ob' \in \{1,2,\{1,2\}\}} \text{ onde}$$
$$CI_1 = \{y\}$$
$$CI_2 = CI_{\{1,2\}} = \emptyset$$

é explicação para a garantia inicial de de $y^1 \wedge z^2 \in CE_{\{1,2\}}^{\mathbf{tf}}$ em eco. ■

Definição 4.71 Sejam $\mathcal{CI}_1 = \{CI^1_{ob'}\}_{ob' \in Sb^1_{ob} \cup Sb^2_{ob}}$ e $\mathcal{CI}_2 = \{CI^2_{ob'}\}_{ob' \in Sb^1_{ob} \cup Sb^2_{ob}}$ duas explicações para a garantia inicial de q em eco e $i \in Sb^1_{ob}$:

- $\mathcal{CI}_1$ é *mais liberal que $\mathcal{CI}_2$ relativamente a i* sse

- se $CI^2_{ob'} = \emptyset$ então $CI^1_{ob'} = \emptyset$
- se $p_1 \in CI^1_i$ e $p_2 \in CI^2_i$ então $p_2 \Rightarrow p_1$ é válida;

- $\mathcal{CI}_1$ é *estritamente mais liberal que* $\mathcal{CI}_2$ *relativamente a* i sse
  - $\mathcal{CI}_1$ é mais liberal que $\mathcal{CI}_2$ relativamente a i
  - $\mathcal{CI}_2$ não é mais liberal que $\mathcal{CI}_1$ relativamente a i;
- $\mathcal{CI}_1$ é *(estritamente) mais liberal que* $\mathcal{CI}_2$ sse $\mathcal{CI}_1$ é (estritamente) mais liberal que $\mathcal{CI}_2$ relativamente a todos os elementos de Sb^1_{ob}. ∎

Definição 4.72 O *conjunto de constrangimentos de estado geradores de explicações para garantia inicial de* q *em* eco, $G^{\overset{ci}{\rightarrow} q}_{<eco,ob>}$, define-se do seguinte modo:

$$G^{\overset{ci}{\rightarrow} q}_{<eco,ob>} = G_{CI} \cup G_{Obs}$$

onde G_{CI} é a *componente de* $G^{\overset{ci}{\rightarrow} q}_{<eco,ob>}$ *induzida pelas condições iniciais em* eco e G_{Obs} é a *componente de* $G^{\overset{ci}{\rightarrow} q}_{<eco,ob>}$ *induzida pela observação* as quais se definem como segue

- $G_{CI} = \bigcup_{1 \leq j \leq m} (\sigma^{i_j}_{ob})_F(G^{i_j}_{CI})$ onde, para cada $1 \leq j \leq m$, $G^{i_j}_{CI}$ se define indutivamente do seguinte modo:
  - $AxF_{i_j} \cap CE^{\mathbf{tf}}_{i_j}$
  - se $q_1, \ldots, q_n \in G^{i_j}_{CI}$, $n \geq 1$, e existem $f'_1, \ldots, f'_{n'} \in Enm(AxF_{i_j} \cap RActv2^b_{i_j})$ com $b \in Acc_{i_j}$, $n' \geq 1$ e tal que a fórmula $(q_1 \wedge \ldots \wedge q_n) \Rightarrow (cnd(f'_1) \vee \ldots \vee cnd(f'_{n'}))$ é válida então $cnd(AxF_{i_j} \cap RActv1^b_{i_j}) \subseteq G^{i_j}_{CI}$;
- $G_{Obs} = \{\neg q\}$. ∎

Proposição 4.73 Se $G^{\overset{ci}{\rightarrow} q}_{<eco,ob>}$ é um conjunto impossível então existe garantia inicial de q em eco.

Prova: Há que provar que $eco \models_{ob} q$. Seja Λ um modelo de eco e $G^{\overset{ci}{\rightarrow} q}_{<eco,ob>} = G_{CI} \cup G_{Obs}$ como na Definição 4.72.

(a) Pela Definição 4.26, $\Lambda \models \{AxF_{ob'}\}_{ob' \in C_P}$.

(b) Se, para cada $1 \leq j \leq m$, $\Lambda, k \models_{i_j} G^{i_j}_{CI}$ então, pelo Lema 4.19, $\Lambda, k \models_{ob} (\sigma^{i_j}_{ob})_F(G^{i_j}_{CI})$. Seja $1 \leq j \leq m$. A prova de que $\Lambda, k \models_{i_j} G^{i_j}_{CI}$ decorre por indução estrutural.

Base: por (a)

Passo: prova semelhante à apresentada na alínea (b) da prova da Proposição 4.50.

(c) Por hipótese, $G^{\overset{ci}{\rightarrow} q}_{<eco,ob>}$ é um conjunto impossível e portanto, por (b), $\Lambda \not\models_{ob} G_{Obs}$, ou seja, $\Lambda \models_{ob} q$. ∎

Proposição 4.74 Se existe $t \in T_{ob}(G^{\overset{ci}{\rightarrow} q}_{<eco,ob>})$ fechado então há garantia de inicial de q em *eco*.

Prova: Prova semelhante à apresentada para a Proposição 4.51 recorrendo agora à Proposição 4.73. ∎

Notação 4.75 O conjunto das famílias de conjuntos de literais induzidas por elementos de $Fc(G^{\overset{ci}{\rightarrow} q}_{<eco,ob>})$ é no seguimento denotado por $\mathcal{F}c^{\overset{ci}{\rightarrow} q}_{<eco,ob>}$. ∎

Definição 4.76 Seja $\mathcal{L} = \{L_i\}_{i \in Sb^1_{ob}}$ com $L_i \subseteq LE_i$ para cada $i \in Sb^1_{ob}$. A família de conjuntos de constrangimentos de estado

$$\mathcal{CI} = \{CI_{ob'}\}_{ob' \in Sb^1_{ob} \cup Sb^2_{ob}}$$

diz-se *induzida por* $\mathcal{L}$ sse $CI_{\{i_1,i_2\}} = \emptyset$ para cada $\{i_1, i_2\} \in Sb^2_{ob}$ e, para cada $i \in Sb^1_{ob}$,

- se $L_i = \emptyset$ então $CI_i = \emptyset$;
- se $L_i \neq \emptyset$ então $CI_i = \{l_1 \wedge \ldots \wedge l_n\}$ com $l_1 \ldots l_n \in Enm(L_i)$. ∎

Tal como no caso da garantia de constrangimentos de estado a partir de outros constrangimentos de estado através de conjuntos de acções, os constrangimentos de estado incluídos nas explicações para a garantia inicial de q são conjunções de literais e não conjunções de disjunções de literais como no caso local.

Proposição 4.77 Se $\mathcal{CI} = \{CI_{ob'}\}_{ob' \in Sb^1 ob \cup Sb^2_{ob}}$ é uma família de conjuntos de constrangimentos de estado induzida por $\mathcal{F}c \in \mathcal{F}c^{\overset{ci}{\rightarrow} q}_{<eco,ob>}$ e $\mathcal{CI}$ é *eco*-possível então $\mathcal{CI}$ é uma explicação para a garantia inicial de q em *eco*.

Prova: Seja eco' o enriquecimento de *eco* com $\mathcal{CI}$.

(a) Os requisitos sintácticos da Definição 4.69 são satisfeitos pelas Definição 4.76.

(b) Pela Definição 4.72, para qualquer estrutura de interpretação Λ sobre Σ_{com}, se $\Lambda \models_{ob} G^{\overset{ci}{\rightarrow} q}_{<eco',ob>}$ então $\Lambda \models_{ob} G^{\overset{ci}{\rightarrow} q}_{<eco,ob>} \cup (\bigcup_{i \in Sb^1_{ob}} (\sigma^i_{ob})_F(CI_i))$. Pelas Proposições 3.21 e 4.21, e sendo $\mathcal{F}c = \{Fc_i\}_{i \in Sb^1_{ob}}$, tem-se que $G^{\overset{ci}{\rightarrow} q}_{<eco,ob>} \cup (\bigcup_{i \in Sb^1(ob)} (\sigma^i_{ob})_F(Fc_i)$ é impossível. Tendo em conta as Definições 4.52 e 4.80 pode concluir-se que o conjunto $G^{\overset{ci}{\rightarrow} q}_{<eco,ob>} \cup (\bigcup_{i \in Sb^1_{ob}} (\sigma^i_{ob})_F(CI_i))$ é impossível e consequentemente $G^{\overset{ci}{\rightarrow} q}_{<eco',ob>}$ é impossível. Pela Proposição 4.73, existe garantia de q em eco'.

(c) Dado que, por hipótese, $\mathcal{CI}$ é *eco*-possível tem-se que eco' é coerente. ∎

Também aqui, se se tomassem vários elementos de $\mathcal{F}c^{\overset{ci}{\rightarrow} q}_{<eco,ob>}$ para construir novas condições iniciais de um modo semelhante ao que se fez no caso local, não seria agora possível assegurar a garantia desejada.

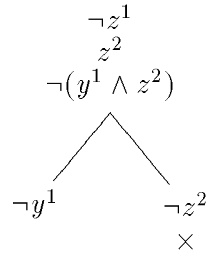

Figura 4.2: Tableau de decisão para $\{\neg z^1, z^2, \neg(y^1 \wedge z^2)\}$

Exemplo 4.78 O tableau t representado na Figura 4.2 é um tableau de decisão em $T_{\{1,2\}}(G^{\overset{ci}{\to} y^1\wedge z^2}_{<eco,\{1,2\}>})$ dado que $G^{\overset{ci}{\to} y^1\wedge z^2}_{<eco,\{1,2\}>} = \{\neg z^1, z^2, \neg(y^1 \wedge z^2)\}$.

A família $\mathcal{F}c = \{Fc_i\}_{i\in\{1,2\}}$ onde $Fc_1 = \{y\}$ e $Fc_2 = \emptyset$ é induzida pelo fecho $\{y^1\}$ de t e $\mathcal{F}c \in \mathcal{F}c^{\overset{ci}{\to} y^1\wedge z^2}_{<eco,\{1,2\}>}$. A família de conjuntos de constrangimentos de estado $\mathcal{CI}$ referida no Exemplo 4.70 é induzida por $\mathcal{F}c$. ∎

Proposição 4.79 Se existem tableaux de decisão abertos em $T_{ob}(G^{\overset{ci}{\to} q}_{<eco,ob>})$ e se tem que $\mathcal{F}c^{\overset{ci}{\to} q}_{<eco,ob>} = \emptyset$ então existe garantia inicial de $\neg q$ em *eco*.

Prova: Raciocinando como na alínea (a) da prova da Proposição 4.54 tem-se que qualquer estrutura de interpretação de comunidade Λ sobre Σ_{com} é tal que $\Lambda \models_{ob} G^{\overset{ci}{\to} q}_{<eco,ob>}$. Tendo em conta a Definição 4.72, conclui-se que existe garantia inicial de $\neg q$ em *eco*. ∎

Definição 4.80 Seja $F \subseteq \mathcal{F}c^{\overset{ci}{\to} q}_{<eco,ob>}$ não vazio. O *conjunto das explicações para a garantia inicial de q em eco induzido por F* denota-se por $E_{CI}(F)$ e é tal que

$$\mathcal{CI} \in E_{CI}(F)$$

sse $\mathcal{CI}$ é uma família de conjuntos de constrangimentos de estado induzida por $\mathcal{F}c \in F$ e $\mathcal{CI}$ é *eco*-possível. ∎

Exemplo 4.81 A família $\mathcal{CI}$ referida no Exemplo 4.78 pertence a $E_{CI}(\mathcal{F}c^{\overset{ci}{\to} y^1\wedge z^2}_{<eco,\{1,2\}>})$. ∎

Proposição 4.82 Seja $\mathcal{F}c \in \mathcal{F}c^{\overset{ci}{\to} q}_{<eco,ob>}$ induzido por $Fc \in Fc(G^{\overset{ci}{\to} q}_{<eco,ob>})$ tal que existe $Fc' \subseteq Fc$ com $Fc' \in Fc(G_{CI})$ onde G_{CI} é a componente de $G^{\overset{ci}{\to} q}_{<eco,ob>}$ induzida pelas condições iniciais. Se $\mathcal{CI}$ é família de conjuntos de constrangimentos de estado induzida por $\mathcal{F}c$ então $\mathcal{CI} \notin E_{CI}(\mathcal{F}c^{\overset{ci}{\to} q}_{<eco,ob>})$.

Prova: (a) Pela Proposição 3.21 e Definição 3.24, não existe estrutura de interpretação λ sobre $\Sigma = (Acc_{ob}, Atr_{ob})$ que seja modelo de $G_{CI} \cup Fc'$ e, consequentemente, que seja modelo de $G_{CI} \cup Fc$.

(b) Suponha-se, por absurdo, que existe um modelo Λ de eco tal que $\Lambda \models \mathcal{CI}$. Sendo $\mathcal{CI} = \{CI_{ob'}\}_{ob' \in Sb^1_{ob} \cup Sb^2_{ob}}$, tem-se que $\Lambda \models_{ob'} CI_{ob'}$ para todo $ob' \in Sb^1_{ob} \cup Sb^2_{ob}$ e portanto, sendo $\mathcal{F}c = \{Fc_i\}_{i \in Sb^1_{ob}}$, $\Lambda \models_i Fc_i$ para todo $i \in Sb^1_{ob}$. Pelo Lema 4.19, $\Lambda \models_{ob} Fc$. Pela Definição 4.72, $\Lambda \models_{ob} G_{CI}$. Pelo Lema 4.21, existe uma estrutura de interpretação λ sobre $\Sigma = (Acc_{ob}, Atr_{ob})$ que é modelo de $G_{CI} \cup Fc$ o que contradiz (a). Conclui-se assim que $\mathcal{CI}$ não é eco-possível e portanto $\mathcal{CI} \notin E_{CI}(\mathcal{F}c^{\overset{ci}{-}q}_{<eco,ob>})$. ■

Proposição 4.83 Seja $F \subseteq \mathcal{F}c^{\overset{ci}{-}q}_{<eco,ob>}$. Se $\mathcal{CI} \in E_{CI}(F)$ é induzida por $\mathcal{F}c \in min(F)$ então não existe $\mathcal{CI}' \in E_{CI}(F)$ estritamente mais liberal que $\mathcal{CI}$.

Prova: Prova semelhante à apresentada para a Proposição 4.63 recorrendo agora às Definições 4.71 e 4.76. ■

Proposição 4.84 Seja eco uma especificação de comunidade de objectos tal que não existe garantia inicial de q em eco e seja $\mathcal{CI}$ uma explicação para a garantia inicial de q em eco. Se o conjunto $G^{\overset{ci}{-}q}_{<eco,ob>} \cup (\bigcup_{ob \in Sb^1_{ob}}((\sigma^{ob'}_{ob})_F(CI_{ob'}))$ é impossível então existe $\mathcal{CI}' \in E_{CI}(\mathcal{F}c^{\overset{ci}{-}q}_{<eco,ob>})$ mais liberal que $\mathcal{CI}$.

Prova: Prova semelhante à apresentada para a Proposição 4.65. ■

Os critérios de preferência mencionados no Capítulo 3 para o caso local podem também ser adoptados neste novo contexto.

4.8 Geração de explicações para problemas de abdução em comunidades de objectos

Nesta secção mostra-se como se constroem explicações para problemas de abdução no âmbito de uma comunidade de objectos. Os problemas de abdução que se consideram são os apresentados na secção 4.5, ou seja, problemas de segurança, problemas de resposta, problemas de persistência e problemas de garantia. A construção das explicações neste contexto é baseada em ideias semelhantes às utilizadas para o caso da construção de explicações para problemas de abdução no âmbito de especificações de objectos. Esta secção é constituída por quatro subsecções. A subsecção 4.8.1 é dedicada aos problemas de segurança. A subsecção 4.8.2 é dedicada aos problemas de resposta. A subsecção 4.8.3 é dedicada aos problemas de persistência. A subsecção 4.8.4 é dedicada aos problemas de garantia.

No que se segue assume-se fixada uma especificação de comunidade de objectos $eco = (\Sigma_{com}, \mathcal{A}x\mathcal{F}, \mathcal{A}x\mathcal{S})$ com $\Sigma = (P, Asn)$, $\Sigma^{ob}_{com} = (ob, Acc_{ob}, Atr_{ob})$ para cada $ob \in C_P$, $\mathcal{A}x\mathcal{F} = \{AxF_{ob}\}_{ob \in C_P}$ e $\mathcal{A}x\mathcal{S} = \{AxS_{ob}\}_{ob \in C_P}$. Assumem-se ainda fixados $ob \in C_P$, $i_1 \dots i_m \in Enm(ob)$ e as fórmulas $r, q, q_1, q_2 \in CE^{\mathbf{tf}}_{ob}$.

4.8.1 Problemas de segurança

Nesta subsecção descreve-se a construção de explicações para problemas de segurança no âmbito de eco.

Proposição 4.85 Se todas as acções compostas $A \in ACC_{ob}$ garantem q a partir de r em *eco* então $eco \models_{ob} \mathbf{G}(r \Rightarrow (\mathbf{X}\, q))$.

Prova: Seja Λ um modelo de *eco*, $k \in I\!N_0$ e suponha-se que $\Lambda, k \models_{ob} r$. Pela Definições 4.13 e 4.17, para cada $1 \leq j \leq m$, existe um e um só $b_j \in Acc_{i_j}$ para o qual se tem que $\Lambda, k \models_{i_j} \nabla b_j$. Pelo Lema 4.19 $\Lambda, k \models_{ob} \nabla(\sigma_{ob}^{i_j})_{Acc}(b_j)$ para cada $1 \leq j \leq m$. Pela Definição 4.11, $A = \bigcup_{1 \leq j \leq m} \{(\sigma_{ob}^{i_j})_{Acc}(b_j)\} \in ACC_{ob}$. Por hipótese e tendo em conta a Definição 4.35, $\Lambda, k \models_{ob} \mathbf{X}\, q$. ∎

Proposição 4.86 Se

(i) $eco \models_{ob} r \Rightarrow (q_1 \vee q_2)$,

(ii) $eco \models_{ob} \mathbf{G}((q_1 \wedge (\neg q_2)) \Rightarrow (\mathbf{X}(q_1 \vee q_2)))$,

então $eco \models_{ob} r \Rightarrow (q_1\, \mathbf{W}\, q_2)$.

Prova: A prova é análoga à apresentada para a Proposição 3.68. ∎

Corolário 4.87 Se

(i) $eco \models_{ob} q$,

(ii) $eco \models_{ob} \mathbf{G}(q \Rightarrow (\mathbf{X}\, q))$,

então $eco \models_{ob} \mathbf{G}\, q$.

Prova: Pela Proposição 4.86 fazendo $r = \mathbf{t}$, $q_1 = q$ e $q_2 = \mathbf{f}$. ∎

Proposição 4.88 Se

(i) $eco \models_{ob} \mathbf{G}(r \Rightarrow (q_1 \vee q_2))$,

(ii) $eco \models_{ob} \mathbf{G}((q_1 \wedge (\neg q_2)) \Rightarrow (\mathbf{X}(q_1 \vee q_2)))$,

então $eco \models_{ob} \mathbf{G}(r \Rightarrow (q_1\, \mathbf{W}\, q_2))$.

Prova: A prova é semelhante à apresentada para a Proposição 3.70. ∎

Nas secções anteriores foram apresentados métodos para construir explicações para a garantia de um constrangimento de estado a partir de outro constrangimento de estado e para a garantia inicial de um constrangimento de estado, os quais são agora utilizados para construir explicações para problemas de segurança.

Definição 4.89 Seja $f = \mathbf{G}(r \Rightarrow (\mathbf{X}\, q)) \in O_{ob}$. Para cada $A \in ACC_{ob}$, a fórmula

$$\mathbf{G}((\nabla a_{i_1}^A \wedge \ldots \wedge \nabla a_{i_m}^A \wedge r) \Rightarrow (\mathbf{X}\, q))$$

designa-se por *garantia induzida por f relativamente a A* e denota-se por $gr_A(f)$. ∎

Proposição 4.90 Seja $f = \mathbf{G}(r \Rightarrow (\mathbf{X}\, q)) \in O_{ob}$ um problema de segurança em *eco*. Seja

$$N = \{A \in ACC_{ob} \colon eco \not\models_{ob} gr_A(f)\}$$

e, para cada $A \in N$, seja $\mathcal{E}_A = \{E^A_{ob'}\}_{ob' \in Sb^1_{ob} \cup Sb^2_{ob}}$ uma explicação para a garantia de q a partir de r por A em *eco*. Se

$$\mathcal{E} = \{E_{ob'}\}_{ob' \in Sb^1_{ob} \cup Sb^2_{ob}}$$

onde $E_{ob'} = \bigcup_{A \in N} E^A_{ob'}$ para cada $ob' \in Sb^1_{ob} \cup Sb^2_{ob}$, é *eco*-possível então $\mathcal{E}$ é uma explicação para o problema de segurança f.

Prova: Seja eco' o enriquecimento de *eco* com $\mathcal{E}$.

(a) Sejam $A \in ACC_{ob}$ e Λ modelo de eco'.

Suponha-se que $A \notin N$. Como Λ também é modelo de *eco* e por definição de N, $\Lambda \models gr_A(f)$.

Suponha-se que $A \in N$. Sendo eco'' o enriquecimento de *eco* com $\mathcal{E}_A$, pelas Definições 4.36 e 4.36, $eco'' \models_{ob} gr_A(f)$. Dado que Λ é também modelo de eco'', tem-se então que $\Lambda \models_{ob} gr_A(f)$.

Dos dois parágrafos anteriores resulta que $eco' \models gr_A(f)$ para cada $A \in ACC_{ob}$.

(b) Por (a) e Proposição 4.85, $eco' \models_{ob} \mathbf{G}(r \Rightarrow (\mathbf{X}\, q))$.

(c) Dado que $\mathcal{E}$ é *eco*-possível, tem-se que eco' é coerente.

(d) Por (b), (c) e Definição 4.33, $\mathcal{E}$ é uma explicação para f. ∎

Definição 4.91 Seja $f = r \Rightarrow (q_1\, \mathbf{W}\, q_2) \in O_{ob}$. Os *subproblemas para a explicação de f* são as fórmulas

- $sp_{CI}(f) = r \Rightarrow (q_1 \vee q_2)$;
- $sp_{seg}(f) = \mathbf{G}((q_1 \wedge (\neg q_2)) \Rightarrow (\mathbf{X}(q_1 \vee q_2)))$.

O conjunto dos subproblemas para a explicação de f, $Sp(f)$, é o conjunto constituído pelas fórmulas anteriores.

Para cada $A \in ACC_{ob}$, a fórmula

$$\mathbf{G}((\nabla a^A_{i_1} \wedge \ldots \wedge \nabla a^A_{i_m} \wedge q_1 \wedge (\neg q_2)) \Rightarrow (\mathbf{X}(q_1 \vee q_2)))$$

designa-se por *garantia induzida por f relativamente a A* e denota-se por $gr_A(f)$.

No que se segue, dada a especificação de comunidade de objectos *eco*, entende-se por *explicação para $sp_{CI}(f)$ em eco* uma explicação para a garantia inicial de $sp_{CI}(f)$ na especificação *eco*. ∎

Proposição 4.92 Seja $f = r \Rightarrow (q_1\, \mathbf{W}\, q_2) \in O_{ob}$ um problema de segurança em *eco*. Seja

$$X = \{sp \in Sp(f) \colon eco \not\models_{ob} sp\}$$

e para cada $sp \in X$ seja $\mathcal{E}_{sp} = \{E^{sp}_{ob'}\}_{ob' \in Sb^1_{ob} \cup Sb^2_{ob}}$ uma explicação para sp em *eco*. Se

$$\mathcal{E} = \{E_{ob'}\}_{ob' \in Sb^1_{ob} \cup Sb^2_{ob}}$$

onde $E_{ob'} = \bigcup_{sp \in X} E^{sp}_{ob'}$ para cada $ob' \in Sb^1_{ob} \cup Sb^2_{ob}$, é *eco*-possível então $\mathcal{E}$ é uma explicação para o problema de segurança f.

Prova: Seja eco' o enriquecimento de eco com $\mathcal{E}$.

(a) Dado que todo o modelo de eco' é também modelo de eco tem-se que $eco \models_{ob} sp$ para todo $sp \in Sp(f)$ tal que $sp \notin X$.

Seja $sp \in X$. Se $sp = sp_{CI}(f)$ e sendo eco'' o enriquecimento de eob com $\mathcal{E}_{sp}$, pela Definição 4.69, $eco'' \models_{ob} sp$ e, dado que todo o modelo de eob' é também modelo de eco'', $eco' \models_{ob} sp$. Se $sp = sp_{seg}(f)$, e sendo eco'' o enriquecimento de eco com $\mathcal{E}_{sp}$, pela Definição 4.33, $eco'' \models_{ob} sp$ e novamente $eco' \models_{ob} sp$.

Pela Proposição 4.86, conclui-se que $eco' \models_{ob} f$.

(b) Dado que $\mathcal{E}$ é *eco*-possível, tem-se que eco' é coerente.

(c) Por (a) e (b) $\mathcal{E}$ é uma explicação para o problema de segurança f. ∎

Exemplo 4.93 Considere-se a especificação de comunidade de objectos eco e o problema de segurança

$$f = \mathbf{G}(z^2 \vee x^3) \in O_{\{2,3\}}$$

referidos no Exemplo 4.32.

1. Tem-se que $sp_{CI}(f) = z^2 \vee x^3$ e $eco \models_{\{2,3\}} sp_{CI}(f)$.

2. Tem-se que $sp_{seg}(f) = \mathbf{G}((z^2 \vee x^3) \Rightarrow (\mathbf{X}(z^2 \vee x^3)))$ e $eco \not\models_{\{2,3\}} sp_{seg}(f)$.

2.1. A acção composta $A' = \{a^2, e^3\}$ não preserva $z^2 \vee x^3$ em eco. As famílias $\mathcal{E}_1$, $\mathcal{E}_2$ e $\mathcal{E}_3$ referidas no Exemplo 4.61 constituem explicações para a referida preservação.

2.2. A acção composta $A'' = \{a^2, \perp^3\}$ não preserva $z^2 \vee x^3$ em eco. O conjunto gerador de explicações para a presevação de $z^2 \vee x^3$ por A'' é

$$G^{z^2 \vee x^3 \xrightarrow{A''} z^2 \vee x^3}_{<eco,\{2,3\}>} = \{z^2 \vee x^3, \neg(z^2 \vee x^3)\,{}^{z^2}_{\neg z^2}\} = \{z^2 \vee x^3, \neg((\neg z^2) \vee x^3)\}.$$

Este conjunto é igual ao conjunto gerador construído no Exemplo 4.48 e consequentemente dá origem ao tableau apresentado no Exemplo 4.57. A família $\mathcal{F}c_1 = \{Fc^1_i\}_{i \in \{2,3\}}$ mencionada neste último exemplo induz as famílias $\mathcal{E}_1$ e $\mathcal{E}_2$ referidas no Exemplo 4.57 mas o fecho $\mathcal{F}c_2 = \{Fc^2_i\}_{i \in \{2,3\}}$ não induz agora nenhuma explicação.

2.3. Todas as acções compostas em $ACC_{\{2,3\}} \backslash \{\{a^2, e^3\}, \{a^2, \perp^3\}\}$ preservam $z^2 \vee x^3$ em eco.

2.4. As famílias

$$\mathcal{E}_1 = \{E^1_{ob'}\}_{ob' \in \{2,3,\{2,3\}\}} \text{ onde}$$
$$E^1_{\{2,3\}} = \{\mathbf{G}(z^2 \Rightarrow (\nabla a^2 \Rightarrow \nabla c^3))\}$$
$$E^1_2 = E^1_3 = \emptyset$$

$$\mathcal{E}_2 = \{E^2_{ob'}\}_{ob' \in \{2,3,\{2,3\}\}} \text{ onde}$$
$$E^2_2 = \{\mathbf{G}(\diamond a \Rightarrow (\neg z))\}$$
$$E^2_3 = E^2_{\{2,3\}} = \emptyset$$

são explicações para $sp_{seg}(f)$ em *eco*.

3. As famílias referidas em **2.4** são explicações para o problema de segurança. ∎

Exemplo 4.94 Considere-se a especificação de comunidade de objectos *eco* e o problema de segurança

$$f = \mathbf{G}(y^1 \wedge z^2) \in O_{\{1,2\}}$$

referidos no Exemplo 4.32.

1. Tem-se que $sp_{CI}(f) = y^1 \wedge z^2$ e $eco \not\models_{\{1,2\}} sp_{CI}(f)$. No Exemplo 4.81 foi encontrada a explicação $\mathcal{CI}$ para a garantia inicial de $sp_{CI}(f)$.

2. Tem-se que $sp_{seg}(f) = \mathbf{G}((y^1 \wedge z^2) \Rightarrow (\mathbf{X}(y^1 \wedge z^2)))$ e $eco \not\models_{\{1,2\}} sp_{seg}(f)$.

2.1. A acção composta $A = \{a^1, a^2\}$ não preserva $y^1 \wedge z^2$ em *eco*. O tableau representado na Figura 4.3 é um tableau de decisão em $T_{\{1,2\}}(G^{y^1\wedge z^2 \xrightarrow{A} y^1 \wedge z^2}_{<eco,\{1,2\}>})$. Os conjuntos $Fc_1 = \{\neg y^1\}$

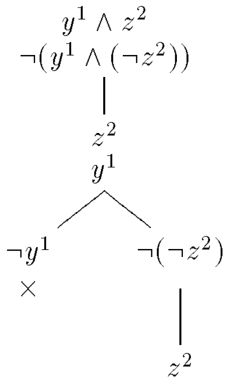

Figura 4.3: Tableau de decisão para $\{y^1 \wedge z^2, \neg(y^1 \wedge (\neg z^2))\}$

e $Fc_2 = \{\neg z^2\}$ são fechos de t. Sejam $\mathcal{F}c_1$ e $\mathcal{F}c_2$ as famílias de conjuntos de literais induzidas por Fc_1 e Fc_2, respectivamente. Seguindo os critérios mencionados na subsecção 4.6.4, a família de conjuntos de restrições de activação

$$\mathcal{E}_1 = \{E^1_{ob'}\}_{ob' \in \{1,2\,\{1,2\}\}} \text{ onde}$$
$$E^1_2 = \{\mathbf{G}(\diamond a \Rightarrow (\neg z))\}$$
$$E^1_1 = E^1_{\{1,2\}} = \emptyset$$

induzida por $\mathcal{F}c_2$ é uma explicação para a preservação de $y^1 \wedge z^2$ por $\{a^1, a^2\}$ mais interessante do que seria a explicação por restrição de activação induzida por $\mathcal{F}c_1$ dado que não é a acção $a \in Acc_1$ que contribui directamente para a não preservação de $y^1 \wedge z^2$. Poder-se-ia considerar uma explicação por interacção envolvendo a^1 como gatilho mas tendo novamente em conta o comentário anterior tal não seria muito interessante. Explicações por interacção envolvendo a^2 como gatilho não são relevantes pois não existe nenhuma acção composta que inclua a^2 e que preserve $y^1 \wedge z^2$.

2.2. As acções compostas $\{b^1, a^2\}$, $\{b^1, d^2\}$, $\{c^1, a^2\}$, $\{b^1, \perp^2\}$ e $\{\perp^1, a^2\}$ não preservam $y^1 \wedge z^2$ e, construindo tableaux de decisão para os conjuntos geradores de explicações respectivos, conclui-se que têm os mesmos fechos que o tableau t apresentado em **2.1**.

2.2.1. No caso de $\{b^1, a^2\}$ e seguindo os critérios mencionados, não faz sentido considerar explicações por interacção. A família $\mathcal{E}_1$ mencionada em **2.1** e a família

$$\begin{aligned}\mathcal{E}_3 = \{E^3_{ob'}\}_{ob' \in \{1,2,\{1,2\}\}} \text{ onde}\\ E^3_1 = \{\mathbf{G}(\diamond b \Rightarrow (\neg y))\}\\ E^3_2 = E^3_{\{1,2\}} = \emptyset\end{aligned}$$

são explicações para a preservação de $y^1 \wedge z^2$ por $\{b^1, a^2\}$.

2.2.2. A explicação $\mathcal{E}_1$ mencionada em **2.1** é explicação para a preservação de $y^1 \wedge z^2$ por $\{b^1, d^2\}$ e, seguindo os critérios referidos, é mais interessante que a induzida por $\mathcal{F}c_2$. Explicações por interacção envolvendo d^2 como gatilho não são muito interessante porque, uma vez mais, não é d^2 que contribui directamente para a não preservação de $y^1 \wedge z^2$.

2.2.3. A explicação $\mathcal{E}_1$ mencionada em **2.1** é explicação para a preservação de $y^1 \wedge z^2$ por $\{c^1, a^2\}$ e, seguindo os critérios referidos, é mais interessante que a induzida por $\mathcal{F}c_2$. Explicações por interacção envolvendo envolvendo c^1 como gatilho não são muito interessante porque novamente não é c^1 que contribui directamente para a não preservação de $y^1 \wedge z^2$.

2.2.4. A explicação $\mathcal{E}_3$ mencionada em **2.2.1** é explicação para a preservação de $y^1 \wedge z^2$ por $\{b^1, \perp^2\}$. Neste caso não são relevantes as explicações por interacção.

2.2.5. A explicação $\mathcal{E}_1$ mencionada em **2.1** é explicação para a preservação de $y^1 \wedge z^2$ por $\{\perp^1, a^2\}$. Neste caso não são relevantes as explicações por interacção.

2.3. Todas as acções compostas em $ACC_{\{1,2\}}$ excepto as mencionadas em **2.1** e **2.2** preservam $y^1 \wedge z^2$.

2.4. A família

$$\begin{aligned}\mathcal{E}' = \{E'_{ob'}\}_{ob' \in \{1,2,\{1,2\}\}} \text{ onde}\\ E'_1 = \{\mathbf{G}(\diamond b \Rightarrow (\neg y))\}\\ E'_2 = \{\mathbf{G}(\diamond a \Rightarrow (\neg z))\}\\ E'_{\{1,2\}} = \emptyset\end{aligned}$$

é explicação para $sp_{seg}(f)$ em *eco*.

3. A família

$$\begin{aligned}\mathcal{E} = \{E_{ob'}\}_{ob' \in \{1,2,\{1,2\}\}} \text{ onde}\\ E_1 = \{y, \mathbf{G}(\diamond b \Rightarrow (\neg y))\}\\ E_2 = \{\mathbf{G}(\diamond a \Rightarrow (\neg z))\}\\ E_{\{1,2\}} = \emptyset\end{aligned}$$

é explicação para o problema de segurança. Como se pretende ter $y^1 \wedge z^2$ como invariante e dada a especificação eco em causa, como seria de esperar, a solução encontrada leva a que as acções $b \in Acc_1$ e $a \in Acc_2$ nunca possam ocorrer.

Definição 4.95 Seja $f = \mathbf{G}(r \Rightarrow (q_1\,\mathbf{W}\,q_2)) \in O_{ob}$. Os *subproblemas para a explicação de* f são as fórmulas

- $sp_{seg_1}(f) = \mathbf{G}(r \Rightarrow (q_1 \vee q_2))$
- $sp_{seg_2}(f) = \mathbf{G}((q_1 \wedge (\neg q_2)) \Rightarrow (\mathbf{X}(q_1 \vee q_2)))$.

O conjunto dos subproblemas para a explicação de f, $Sp(f)$, é o conjunto constituído pelas fórmulas anteriores. ∎

Proposição 4.96 Seja $f = \mathbf{G}(r \Rightarrow (q_1\,\mathbf{W}\,q_2)) \in O_{ob}$ um problema de segurança em eco. Seja

$$X = \{sp \in Sp(f) \colon eco \not\models_{ob} sp\}$$

e para cada $sp \in X$ seja $\mathcal{E}_{sp} = \{E^{sp}_{ob'}\}_{ob' \in Sb^1_{ob} \cup Sb^2_{ob}}$ uma explicação para sp em eco. Se

$$\mathcal{E} = \{E_{ob'}\}_{ob' \in Sb^1_{ob} \cup Sb^2_{ob}}$$

onde $E_{ob'} = \bigcup_{sp \in X} E^{sp}_{ob'}$ para cada $ob' \in Sb^1_{ob} \cup Sb^2_{ob}$ é eco-possível então $\mathcal{E}$ é uma explicação para o problema de segurança f.

Prova: Seja eco' o enriquecimento de eco com E.

(a) Dado que qualquer modelo de eco' é também modelo de eco, $eco' \models_{ob} sp$ para todo $sp \in Sp(f)$ tal que $sp \notin X$.

Seja $sp \in X$. Seja eco'' o enriquecimento de eco com $\mathcal{E}_{sp}$. Pela Definição 4.33 tem-se que $eco'' \models_{ob} sp$ e, dado que qualquer modelo de eco' é também modelo de eco'', $eco' \models_{ob} sp$. Pela Proposição 4.88, $eco' \models_{ob} f$.

(b) Dado que $\mathcal{E}$ é eco-possível, tem-se que eco' é coerente.

(c) Por (a), (b) e Definição 4.33, $\mathcal{E}$ é uma explicação para f. ∎

A terminar esta subsecção seguem-se alguns breves comentários relativos a critérios de preferência entre explicações no âmbito de problemas de segurança.

A construção de explicações para problemas de segurança envolve a construção de explicações para a garantia inicial de constrangimentos de estado e para a garantia de certos constrangimentos de estado a partir de outros constrangimento através de acções compostas. Deste modo, os critérios que foram já mencionados para tais casos deverão naturalmente ser aqui utilizados.

Tal como no caso local, no âmbito de problemas $\mathbf{G}\,q \in O_{ob}$, as explicações por restrição de activação para as várias garantias $gr_A(\mathbf{G}\,q)$, que sejam induzidas por famílias de conjuntos de literais induzidas por fechos em $Fc(\{q\})$, serão sempre menos interessantes que outras que não se encontrem nesta situação, e que sejam consideradas preferíveis face aos critérios mencionados no parágrafo anterior.

4.8.2 Problemas de resposta

Nesta subsecção descreve-se a construção de explicações para problemas de resposta no âmbito de uma comunidade de objectos. A construção de explicações tem por base ideias semelhantes às utilizadas na construção de problemas de resposta no Capítulo 3. São aqui consideradas apenas *explicações em um passo.*

Recorde-se que se assumiram fixados no princípio desta secção $i_1 \ldots i_m \in Enm(ob)$ e $r, q_1, q_2 \in CE_{ob}^{\mathbf{tf}}$. Para o que se segue torna-se conveniente introduzir as seguintes noções sobre fórmulas em $CE_{ob}^{\mathbf{tf}}$.

Definição 4.97 Sejam $m' \geq 1$ e $i'_1, \ldots, i'_{m'}$ elementos distintos de Sb_{ob}^1. Diz-se que a fórmula $p \in CE_{ob}$ é uma *separação conjuntiva sobre* $i'_1, \ldots, i'_{m'}$ sse $p = p_1 \wedge \ldots \wedge p_{m'}$ com $p_j \in (\sigma_{ob}^{i'_j})_F(CE_{i'_j})$ para cada $1 \leq j \leq m'$. ∎

Definição 4.98 Diz-se que a fórmula $p \in CE_{ob}$ é uma *disjunção em separações conjuntivas* sse $p = p_1 \vee \ldots \vee p_n$ e p_j é separacção conjuntiva sobre $m_j \geq 1$ elementos de distintos de Sb_{ob}^1 para cada $1 \leq j \leq n$.

Sendo $q \in CE_{ob}^{\mathbf{tf}}$, denota-se por $DSC(q)$ o conjunto de todas as fórmulas $q' \in CE_{ob}$ que são disjunções em separações conjuntivas e tal que $q' \Leftrightarrow q$ é válida. ∎

O conjunto $DSC(q)$ é sempre não vazio qualquer que seja $q \in CE_{ob}^{\mathbf{tf}}$. Uma forma de obter elementos de $DSC(q)$ consiste em começar por escrever q (ou uma fórmula equivalente a q caso q envolva $\mathbf{t}$ ou $\mathbf{f}$) na forma normal disjuntiva $p_1 \vee \ldots \vee p_n$ e depois rearranjar convenientemente os literais em cada uma das fórmulas p_j, $1 \leq j \leq n$.

Proposição 4.99 Seja $p_1 \vee \ldots \vee p_n \in DSC(q_1 \wedge (\neg q_2))$ sendo, para cada $1 \leq j \leq n$, $p_j = p_{j1} \wedge \ldots \wedge p_{jm_j}$ separação conjuntiva sobre $i_{j1}, \ldots, i_{jm_j} \in Sb_{ob}^1$. Para cada $1 \leq j \leq n$ seja $q_{jk} \in CE_{i_{jk}}$ tal que $p_{jk} = (\sigma_{ob}^{i_{jk}})_F(q_{jk})$ para cada $1 \leq k \leq m_j$. Se

(i) $eco \models_{ob} \mathbf{G}(r \Rightarrow (q_1 \,\mathbf{W}\, q_2))$;

(ii) existe $A \in ACC_{ob}$ e, para cada $1 \leq j \leq n$, existe $1 \leq k_j \leq m_j$ tais que, sendo $b_i = (\sigma_{ob}^i)_{Acc}^{-1}(a_i^A)$ para cada $i \in Sb_{ob}^1$,

- $eco \models_{ob} \mathbf{G}((\nabla a_{i_1}^A \wedge \ldots \wedge \nabla a_{i_m}^A \wedge q_1 \wedge (\neg q_2)) \Rightarrow (\mathbf{X}\, q_2))$,
- $eco \models_{i_{jk_j}} \mathbf{G}(q_{jk_j} \Rightarrow \diamond b_{i_{jk_j}})$ para cada $1 \leq j \leq n$,
- $eco \models_{i_{jk_j}} RJst_{i_{jk_j}}^{b_{i_{jk_j}}}$ para cada $1 \leq j \leq n$,
- $eco \models_{ob} \mathbf{G}(\mathbf{t} \Rightarrow (\nabla a_{i_{jk_j}}^A \Rightarrow \nabla a_{i'}^A))$ para cada $1 \leq j \leq n$ e $i' \in Sb_{ob}^1$,

então $eco \models_{ob} \mathbf{G}(r \Rightarrow (q_1 \,\mathbf{U}\, q_2))$.

Prova: Sejam Λ modelo de eco e $k' \in I\!N_0$ tal que $\Lambda, k' \models_{ob} r$. Pela hipótese (i), $\Lambda, k' \models_{ob} q_1 \,\mathbf{W}\, q_2$ o que significa que: (a) $\Lambda, k' \models_{ob} q_1 \,\mathbf{U}\, q_2$ ou (b) $\Lambda, k' \models_{ob} \mathbf{G}(q_1 \wedge (\neg q_2))$.

No caso (a), tem-se que $\Lambda, k' \models r \Rightarrow_{ob} (q_1 \mathbf{U}\, q_2)$.

No caso (b), tem-se que para cada $k'' \geq k'$ existe $1 \leq j \leq n$ tal que $\Lambda, k'' \models_{ob} p_j$ e portanto $\Lambda, k'' \models_{i_{jk}} q_{jk}$ para cada $1 \leq k \leq m_j$. Consequentemente, existe $1 \leq j' \leq n$ tal que $\Lambda, k' \models_{ob} \mathbf{G}(\mathbf{F}\, p_{j'})$ e portanto $\Lambda, k' \models_{i_{j'k}} \mathbf{G}(\mathbf{F}\, q_{j'k})$ para cada $1 \leq k \leq m_{j'}$. Pela segunda condição da hipótese (ii), $\Lambda, k \models_{i_{j'k_{j'}}} \mathbf{G}(\mathbf{F} \diamond b_{i_{j'k_{j'}}})$ e portanto $\Lambda, 0 \models_{i_{j'k_{j'}}} \mathbf{G}(\mathbf{F} \diamond b_{i_{j'k_{j'}}}))$. Pela terceira condição da hipótese (ii) e pela Definição 2.24, $eco \models_{i_{j'k_{j'}}} (\mathbf{G}(\mathbf{F} \diamond b_{i_{j'k_{j'}}})) \Rightarrow (\mathbf{G}(\mathbf{F}\, \nabla b_{i_{j'k_{j'}}}))$ e portanto também $\Lambda, 0 \models_{i_{j'k_{j'}}} \mathbf{G}(\mathbf{F}\, \nabla b_{i_{j'k_{j'}}})$. Então existe $k'' \geq k'$ tal que $\Lambda, k'' \models \nabla b_{i_{j'k_{j'}}}$. Pela quarta condição da hipótese (ii) e pelo Lema 4.19, $\Lambda, k' \models_{ob} \nabla a^A_{i_1} \wedge \ldots \wedge \nabla a^A_{i_m}$. Como $k'' \geq k'$, $\Lambda, k'' \models q_1 \wedge (\neg q_2)$ e portanto, a primeira condição da hipótese (ii) permite concluir que $\Lambda, k'' + 1 \models_{ob} q_2$, contradizendo assim a possibilidade de se verificar (b).

Conclui-se então que $\Lambda \models_{ob} \mathbf{G}(r \Rightarrow (q_1 \mathbf{U}\, q_2))$ e portanto $eco \models_{ob} \mathbf{G}(r \Rightarrow (q_1 \mathbf{U}\, q_2))$. ■

Corolário 4.100 Seja $p_1 \vee \ldots \vee p_n \in DSC(\neg q)$ sendo $p_j = p_{j1} \wedge \ldots \wedge p_{jm_j}$, para cada $1 \leq j \leq n$, separação conjuntiva sobre $i_{j1}, \ldots, i_{jm_j} \in Sb^1_{ob}$. Para cada $1 \leq j \leq n$ seja $q_{jk} \in CE_{i_{jk}}$ tal que $p_{jk} = (\sigma^{i_{jk}}_{ob})_F(q_{jk})$ para cada $1 \leq k \leq m_j$. Se existe $A \in ACC_{ob}$ e, para cada $1 \leq j \leq n$, existe $1 \leq k_j \leq m_j$ tais que, sendo $b_i = (\sigma^i_{ob})^{-1}_{Acc}(a^A_i)$ para cada $i \in Sb^1_{ob}$,

- $eco \models_{ob} \mathbf{G}((\nabla a^A_{i_1} \wedge \ldots \wedge \nabla a^A_{i_m} \wedge (\neg q)) \Rightarrow (\mathbf{X}\, q))$,
- $eco \models_{i_{jk_j}} \mathbf{G}(q_{jk_j} \Rightarrow \diamond b_{i_{jk_j}})$ para cada $1 \leq j \leq n$,
- $eco \models_{i_{jk_j}} RJst^{b_{i_{jk_j}}}_{i_{jk_j}}$ para cada $1 \leq j \leq n$,
- $eco \models_{ob} \mathbf{G}(\mathbf{t} \Rightarrow (\nabla a^A_{i_{jk_j}} \Rightarrow \nabla a^A_{i'}))$ para cada $1 \leq j \leq n$ e $i' \in Sb^1_{ob}$,

então $eco \models_{ob} \mathbf{G}(\mathbf{F}\, q)$.

Prova: Pela Proposição 4.99 fazendo $r = q_1 = \mathbf{t}$ e $q_2 = q$. ■

Definição 4.101 Seja $f = \mathbf{G}(r \Rightarrow (q_1 \mathbf{U}\, q_2)) \in O_{ob}$. Seja $p = p_1 \vee \ldots \vee p_n \in DSC(q_1 \wedge (\neg q_2))$ sendo, para cada $1 \leq j \leq n$, $p_j = p_{j1} \wedge \ldots \wedge p_{jm_j}$ separação conjuntiva sobre $i_{j1}, \ldots, i_{jm_j} \in Sb^1_{ob}$. Para cada $1 \leq j \leq n$ seja $q_{jk} \in CE_{i_{jk}}$ tal que $p_{jk} = (\sigma^{i_{jk}}_{ob})_F(q_{jk})$ para cada $1 \leq k \leq m_j$. Seja $A \in ACC_{ob}$ e, para cada $1 \leq j \leq n$, seja $1 \leq k_j \leq m_j$.

Os *subproblemas para a explicação de f com base em A, p e $p_{1k_1}, \ldots, p_{nk_n}$* são as fórmulas seguintes onde $b_i = (\sigma^i_{ob})^{-1}_{Acc}(a^A_i)$ para cada $i \in Sb^1_{ob}$

- $sp_{seg}(f) = \mathbf{G}(r \Rightarrow (q_1 \mathbf{W}\, q_2))$;
- $sp_{\nabla A}(f) = \mathbf{G}((\nabla a^A_{i_1} \wedge \ldots \wedge \nabla a^A_{i_m} \wedge q_1 \wedge (\neg q_2)) \Rightarrow (\mathbf{X}\, q_2))$;
- $sp_{<\diamond b_{i_{jk_j}}, i_{jk_j}>}(f) = \mathbf{G}(q_{jk_j} \Rightarrow \diamond b_{i_{jk_j}})$ para cada $1 \leq j \leq n$;
- $sp_{<RJst, i_{jk_j}>}(f)$ é o requisito de justiça para $b_{i_{jk_j}}$ para cada $1 \leq j \leq n$;
- $sp_{<Intr, i_{jk_j}, i'>}(f) = \mathbf{G}(\mathbf{t} \Rightarrow (\nabla a^A_{i_{jk_j}} \Rightarrow \nabla a^A_{i'}))$ para cada $1 \leq j \leq n$ e $i' \in Sb^1_{ob}$.

O conjunto dos subproblemas para a explicação de f com base em A, p e $p_{1k_1}, \ldots, p_{nk_n}$, $Sp(A, p, p_{1k_1}, \ldots, p_{nk_n})(f)$, é o conjunto constituído pelas fórmulas anteriores. ∎

Proposição 4.102 Seja $f = \mathbf{G}(r \Rightarrow (q_1 \mathbf{U}\, q_2)) \in O_{ob}$ um problema de resposta em *eco*. Seja $p = p_1 \vee \ldots \vee p_n \in DSC(q_1 \wedge (\neg q_2))$ sendo, para cada $1 \leq j \leq n$, $p_j = p_{j1} \wedge \ldots \wedge p_{jm_j}$ separação conjuntiva sobre $i_{j1}, \ldots, i_{jm_j} \in Sb^1_{ob}$. Para cada $1 \leq j \leq n$ seja $q_{jk} \in CE_{i_{jk}}$ tal que $p_{jk} = (\sigma^{i_{jk}}_{ob})_F(q_{jk})$ para cada $1 \leq k \leq m_j$. Seja $A \in ACC_{ob}$ e, para cada $1 \leq j \leq n$, seja $1 \leq k_j \leq m_j$. Sejam ainda

$$X = \{sp \in Sp(A, p, p_{1k_1}, \ldots, p_{nk_n})(f) \cap F_{ob} : eco \not\models_{ob} sp\} \cup$$
$$\bigcup_{1 \leq j \leq n} \{sp \in Sp(A, p, p_{1k_1}, \ldots, p_{nk_n})(f) \cap F_{i_{jk_j}} : eco \not\models_{ob} (\sigma^{i_{jk_j}}_{ob})_F(sp)\}$$

e

$$X' = X \backslash (\bigcup_{1 \leq j \leq n} (\{sp_{<\diamond b_{i_{jk_j}}, i_{jk_j}>}(f), sp_{<RJst, i_{jk_j}>}(f)\} \cup (\bigcup_{i' \in Sb^1_{ob}} sp_{<Intr, i_{jk_j}, i'>}(f)))).$$

Para cada $sp \in X'$ seja a família $\mathcal{E}_{sp} = \{E^{sp}_{ob'}\}_{ob' \in Sb^1_{ob} \cup Sb^2_{ob}}$ uma explicação para sp em *eco*. Se

$$\mathcal{E} = \{E_{ob'}\}_{ob' \in Sb^1_{ob} \cup Sb^2_{ob}}$$

onde, para cada $ob' \in Sb^1_{ob} \cup Sb^2_{ob}$,

$$E_{ob'} = (\bigcup_{sp \in X'} E^{sp}_{ob'}) \cup \overline{E}_{ob'}$$

com $\overline{E}_{ob'} = X \cap (\{sp_{<\diamond b_{i_{jk_j}}, i_{jk_j}>}(f), sp_{<RJst, i_{jk_j}>}(f)\} \cup (\bigcup_{i' \in Sb^1_{ob}} sp_{<Intr, i_{jk_j}, i'>}(f)))$ se $ob' = i_{jk_j}$ para algum $1 \leq j \leq n$ e $\overline{E}_{ob'} = \emptyset$ se $ob' \notin \bigcup_{1 \leq j \leq n} \{i_{jk_j}\}$, é *eco*-possível então $\mathcal{E}$ é uma explicação para o problema f em *eco* com base em A, p e $p_{1k_1}, \ldots, p_{nk_n}$.

Prova: Seja eco' o enriquecimento de *eco* com $\mathcal{E}$.

(a) Dado que qualquer modelo de eco' também é modelo de *eco*, $eco' \models_{ob} sp$ para todo $sp \in Sp(A, p, p_{1k_1}, \ldots, p_{nk_n})(f)$ tal que $sp \notin X$.

Seja $sp \in X$. Se $sp = sp_{\nabla A}(f)$, e sendo eco'' o enriquecimento de *eco* com $\mathcal{E}_{sp}$, pela Definição 4.36 $eco'' \models_{ob} sp$ e, dado que qualquer modelo de eco' é modelo de eco'', $eco' \models_{ob} sp$. Se $sp = sp_{seg}(f)$, e sendo eco'' o enriquecimento de *eco* com $\mathcal{E}_{sp}$, pela Definição 4.33, $eco'' \models_{ob} sp$ e novamente $eco' \models_{ob} sp$. Finalmente, se sp pertence ao conjunto $\bigcup_{1 \leq j \leq n} (\{sp_{<\diamond b_{i_{jk_j}}, i_{jk_j}>}(f), sp_{<RJst, i_{jk_j}>}(f)\} \cup (\bigcup_{i' \in Sb^1_{ob}} sp_{<Intr, i_{jk_j}, i'>}(f)))$ então, trivialmente, $eco' \models_{ob} sp$.

Conclui-se assim, pela Proposição 4.99, que $eco' \models_{ob} f$.

(b) Dado que $\mathcal{E}$ é *eco*-possível, tem-se que eco' é coerente.

(c) Por (a), (b) e Definição 4.33, $\mathcal{E}$ é uma explicação para f. ∎

No contexto da proposição anterior, naturalmente que, para cada $1 \leq j \leq n$, se tem que $eco \models < Intr, i_{jk_j}, i_{jk_j} >$ e portanto estas fórmulas nunca pertencem a X. Elas têm vindo a ser incluídas nos enunciados das proposições e definições anteriores apenas para simplificar a exposição.

Exemplo 4.103 Considere-se novamente a especificação de comunidade de objectos *eco* referida no Exemplo 4.25. A fórmula

$$f = \mathbf{G}(\mathbf{F}(x^3 \wedge y^4)) \in O_{\{3,4\}}$$

é um problema de resposta em *eco*. Sendo $p_1 = \neg x^3$ e $p_2 = \neg y^4$ tem-se que a fórmula $p = p_1 \vee p_2 \in DSC(\neg(x^3 \wedge y^4))$.

Pretende-se encontrar explicações para f com base em $A = \{c^3, a^4\}$, p e p_{11}, p_{21}. Como é óbvio, neste caso, $p_{11} = p_1$, $p_{21} = p_2$ e $k_1 = k_2 = 1$. Seguindo a notação usada na Definição 4.101 tem-se que $i_{11} = 3$ e $i_{21} = 4$. Deste modo, $a^A_{i_{11}} = c^3$ e $a^A_{i_{21}} = a^4$ e, consequentemente, $b_{i_{11}} = c$ e $b_{i_{21}} = a$.

1. O subproblema $sp_{seg}(f)$ é trivialmente satisfeito.

2. Tem-se que $sp_{\nabla A}(f) = \mathbf{G}((\nabla c^3 \wedge \nabla a^4 \wedge (\neg(x^3 \wedge y^4))) \Rightarrow (\mathbf{X}(x^3 \wedge y^4)))$ e $eco \models_{\{3,4\}} sp_{\nabla A}(f)$.

3. Tem-se que $sp_{<\diamond c,3>}(f) = \mathbf{G}((\neg x) \Rightarrow \diamond c)$ e $eco \not\models_{\{3,4\}} (\sigma^3_{\{3,4\}})_F(sp_{<\diamond c,3>}(f))$.

4. Tem-se que $sp_{<\diamond a,4>}(f) = \mathbf{G}((\neg y) \Rightarrow \diamond a)$ e $eco \not\models_{\{3,4\}} (\sigma^4_{\{3,4\}})_F(sp_{<\diamond a,4>}(f))$.

5. Tem-se que $eco \not\models_{\{3,4\}} (\sigma^3_{\{3,4\}})_F(sp_{<RJst,3>}(f))$.

6. Tem-se que $eco \not\models_{\{3,4\}} (\sigma^4_{\{3,4\}})_F(sp_{<RJst,4>}(f))$.

7. Tem-se que $sp_{<Intr,3,4>}(f) = \mathbf{G}(\mathbf{t} \Rightarrow (\nabla c^3 \Rightarrow \nabla a^4))$ e $eco \not\models_{\{3,4\}} sp_{<Intr,3,4>}(f)$.

8. Tem-se que $sp_{<Intr,4,3>}(f) = \mathbf{G}(\mathbf{t} \Rightarrow (\nabla a^4 \Rightarrow \nabla c^3))$ e $eco \models_{\{3,4\}} sp_{<Intr,4,3>}(f)$.

9. A família

$$\begin{aligned}
&\mathcal{E} = \{E_{ob'}\}_{ob' \in \{3,4,\{3,4\}\}} \text{ onde}\\
&\quad E_3 = \{\mathbf{G}((\neg x) \Rightarrow \diamond c), (\mathbf{G}(\mathbf{F}\diamond c) \Rightarrow (\mathbf{G}(\mathbf{F}\nabla c)\}\\
&\quad E_4 = \{\mathbf{G}((\neg y) \Rightarrow \diamond a), (\mathbf{G}(\mathbf{F}\diamond a)) \Rightarrow (\mathbf{G}(\mathbf{F}\nabla a))\}\\
&\quad E_{\{3,4\}} = \{\mathbf{G}(\mathbf{t} \Rightarrow (\nabla c^3 \Rightarrow \nabla a^4))\}
\end{aligned}$$

é explicação para o problema de resposta. ∎

Exemplo 4.104 Considere-se uma vez mais a especificação de comunidade de objectos *eco* referida no Exemplo 4.25. A fórmula

$$f = \mathbf{G}(\mathbf{F}(u^2 \wedge u^4)) \in O_{\{2,4\}}$$

é um problema de resposta em *eco*. Sendo $p_1 = \neg u^2$ e $p_2 = \neg u^4$ tem-se que a fórmula $p = p_1 \vee p_2 \in DSC(\neg(u^2 \wedge u^4))$.

Pretende-se encontrar explicações para f com base em $A = \{d^2, c^4\}$, p e p_{11}, p_{21}. Novamente, $p_{11} = p_1$, $p_{21} = p_2$ e $k_1 = k_2 = 1$. Seguindo a notação usada na Definição 4.101 tem-se que $i_{11} = 2$ e $i_{21} = 4$. Deste modo, $a^A_{i_{11}} = d^2$ e $a^A_{i_{21}} = c^4$ e, consequentemente, $b_{i_{11}} = d$ e $b_{i_{21}} = c$.

1. O subproblema $sp_{seg}(f)$ é trivialmente satisfeito.

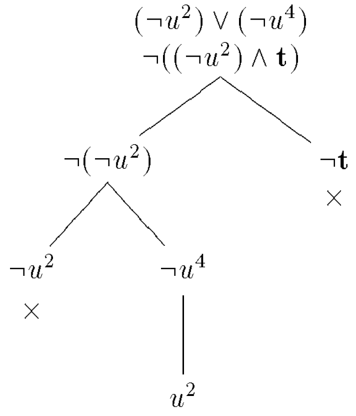

Figura 4.4: Tableau de decisão para $\{(\neg u^2) \vee (\neg u^4), \neg((\neg u^2) \wedge \mathbf{t})\}$

2. Tem-se que $sp_{\nabla A}(f) = \mathbf{G}((\nabla d^2 \wedge \nabla c^4 \wedge (\neg(u^2 \wedge u^4))) \Rightarrow (\mathbf{X}(u^2 \wedge u^4)))$ e $eco \not\models_{\{2,4\}} sp_{\nabla A}(f)$. Na Figura 4.4 encontra-se representado um tableau t o qual é tableau de decisão em $T_{\{2,4\}}(G^{(\neg u^2)\vee(\neg u^4)\overset{A}{-}u^2\wedge u^4}_{<eco,\{2,4\}>})$.

A família de conjuntos de restrições de activação

$$\begin{aligned} \mathcal{E}' &= \{E'_{ob'}\}_{ob' \in \{2,4\,\{2,4\}\}} \text{ onde} \\ E'_2 &= \{\mathbf{G}(\diamond d \Rightarrow (\neg u))\} \\ E'_4 &= E'_{\{2,4\}} = \emptyset \end{aligned}$$

é induzida pela família de conjuntos de literais induzida pelo fecho $\{\neg u^2\}$ de t e é uma explicação para a garantia de $u^2 \wedge u^4$ a partir de $(\neg u^2) \vee (\neg u^4)$ por A.

3. Tem-se que $sp_{<\diamond d,2>}(f) = \mathbf{G}((\neg u) \Rightarrow \diamond d)$ e $eco \not\models_{\{2,4\}} (\sigma^2_{\{2,4\}})_F(sp_{<\diamond d,2>}(f))$.

4. Tem-se que $sp_{<\diamond c,4>}(f) = \mathbf{G}((\neg u) \Rightarrow \diamond c)$ e $eco \not\models_{\{2,4\}} (\sigma^4_{\{2,4\}})_F(sp_{<\diamond c,4>}(f))$.

5. Tem-se que $eco \not\models_{\{2,4\}} \sigma^2_{\{2,4\}\,F}(sp_{<RJst,2>}(f))$.

6. Tem-se que $eco \not\models_{\{2,4\}} \sigma^4_{\{2,4\}\,F}(sp_{<RJst,4>}(f))$.

7. Tem-se que $sp_{<Intr,2,4>}(f) = \mathbf{G}(\mathbf{t} \Rightarrow (\nabla d^2 \Rightarrow \nabla c^4))$ e $eco \not\models_{\{2,4\}} sp_{<Intr,2,4>}(f)$.

8. Tem-se que $sp_{<Intr,4,2>}(f) = \mathbf{G}(\mathbf{t} \Rightarrow (\nabla c^4 \Rightarrow \nabla d^2))$ e $eco \not\models_{\{2,4\}} sp_{<Intr,4,2>}(f)$.

9. A família

$$\begin{aligned} \mathcal{E} &= \{E_{ob'}\}_{ob' \in \{2,4,\{2,4\}\}} \text{ onde} \\ E_2 &= \{\mathbf{G}(\diamond d \Rightarrow (\neg u)), \mathbf{G}((\neg u) \Rightarrow \diamond d), (\mathbf{G}(\mathbf{F}\,\diamond d) \Rightarrow (\mathbf{G}(\mathbf{F}\,\nabla d)\} \\ E_4 &= \{\mathbf{G}((\neg u) \Rightarrow \diamond c), (\mathbf{G}(\mathbf{F}\,\diamond c)) \Rightarrow (\mathbf{G}(\mathbf{F}\,\nabla c))\} \\ E_{\{2,4\}} &= \{\mathbf{G}(\mathbf{t} \Rightarrow (\nabla d^2 \Rightarrow \nabla c^4)), \mathbf{G}(\mathbf{t} \Rightarrow (\nabla c^4 \Rightarrow \nabla d^2))\} \end{aligned}$$

é explicação para o problema de resposta. ∎

4.8.3 Problemas de garantia

Nesta subsecção descreve-se a construção de explicações para problemas de garantia no âmbito de uma comunidade de objectos.

Recorde-se que se assumiram fixados no princípio desta secção $i_1 \dots i_m \in Enm(ob)$ e $r, q_1, q_2 \in CE^{\mathbf{tf}}_{ob}$.

Proposição 4.105 Seja $p_1 \vee \dots \vee p_n \in DSC(q_1 \wedge (\neg q_2))$ sendo, para cada $1 \leq j \leq n$, $p_j = p_{j1} \wedge \dots \wedge p_{jm_j}$ separação conjuntiva sobre $i_{j1}, \dots, i_{jm_j} \in Sb^1_{ob}$. Para cada $1 \leq j \leq n$ seja $q_{jk} \in CE_{i_{jk}}$ tal que $p_{jk} = (\sigma^{i_{jk}}_{ob})_F(q_{jk})$ para cada $1 \leq k \leq m_j$. Se

(i) $eco \models_{ob} r \Rightarrow (q_1 \mathbf{W}\, q_2)$;

(ii) existe $A \in ACC_{ob}$ e, para cada $1 \leq j \leq n$, existe $1 \leq k_j \leq m_j$ tais que, sendo $b_i = (\sigma^i_{ob})^{-1}_{Acc}(a^A_i)$ para cada $i \in Sb^1_{ob}$,

- $eco \models_{ob} \mathbf{G}((\nabla a^A_{i_1} \wedge \dots \wedge \nabla a^A_{i_m} \wedge q_1 \wedge (\neg q_2)) \Rightarrow (\mathbf{X}\, q_2))$,
- $eco \models_{i_{jk_j}} \mathbf{G}(q_{jk_j} \Rightarrow \diamond b_{i_{jk_j}})$ para cada $1 \leq j \leq n$,
- $eco \models_{i_{jk_j}} RJst^{b_{i_{jk_j}}}_{i_{jk_j}}$ para cada $1 \leq j \leq n$,
- $eco \models_{ob} \mathbf{G}(\mathbf{t} \Rightarrow (\nabla a^A_{i_{jk_j}} \Rightarrow \nabla a^A_{i'}))$ para cada $1 \leq j \leq n$ e $i' \in Sb^1_{ob}$,

então $eco \models_{ob} r \Rightarrow (q_1 \mathbf{U}\, q_2)$.

Prova: Sejam Λ modelo de eco e tal que $\Lambda, 0 \models_{ob} r$. A prova é semelhante à apresentada para a Proposição 4.99 ∎

Definição 4.106 Seja $f = r \Rightarrow (q_1 \mathbf{U}\, q_2) \in O_{ob}$. Seja $p = p_1 \vee \dots \vee p_n \in DSC(q_1 \wedge (\neg q_2))$ sendo, para cada $1 \leq j \leq n$, $p_j = p_{j1} \wedge \dots \wedge p_{jm_j}$ separação conjuntiva sobre $i_{j1}, \dots, i_{jm_j} \in Sb^1_{ob}$. Para cada $1 \leq j \leq n$ seja $q_{jk} \in CE_{i_{jk}}$ tal que $p_{jk} = (\sigma^{i_{jk}}_{ob})_F(q_{jk})$ para cada $1 \leq k \leq m_j$. Seja $A \in ACC_{ob}$ e, para cada $1 \leq j \leq n$, seja $1 \leq k_j \leq m_j$.

Os *subproblemas para a explicação de f com base em A, p e $p_{1k_1}, \dots, p_{nk_n}$* são as fórmulas seguintes onde $b_i = (\sigma^i_{ob})^{-1}_{Acc}(a^A_i)$ para cada $i \in Sb^1_{ob}$

- $sp_{seg}(f) = r \Rightarrow (q_1 \mathbf{W}\, q_2)$;
- $sp_{\nabla A}(f) = \mathbf{G}((\nabla a^A_{i_1} \wedge \dots \wedge \nabla a^A_{i_m} \wedge q_1 \wedge (\neg q_2)) \Rightarrow (\mathbf{X}\, q_2))$;
- $sp_{<\diamond b_{i_{jk_j}}, i_{jk_j}>}(f) = \mathbf{G}(q_{jk_j} \Rightarrow \diamond b_{i_{jk_j}})$ para cada $1 \leq j \leq n$;
- $sp_{<RJst, i_{jk_j}>}(f)$ é o requisito de justiça para $b_{i_{jk_j}}$ para cada $1 \leq j \leq n$;
- $sp_{<Intr, i_{jk_j}, i'>}(f) = \mathbf{G}(\mathbf{t} \Rightarrow (\nabla a^A_{i_{jk_j}} \Rightarrow \nabla a^A_{i'}))$ para cada $1 \leq j \leq n$ e $i' \in Sb^1_{ob}$.

O conjunto dos subproblemas para a explicação de f com base em A, p e $p_{1k_1}, \dots, p_{nk_n}$, $Sp(A, p, p_{1k_1}, \dots, p_{nk_n})(f)$, é o conjunto constituído por todas as fórmulas anteriores. ∎

Proposição 4.107 Seja $f = r \Rightarrow (q_1 \mathbf{U}\, q_2) \in O_{ob}$ um problema de garantia em *eco*. Seja $p = p_1 \vee \ldots \vee p_n \in DSC(q_1 \wedge (\neg q_2))$ sendo, para cada $1 \leq j \leq n$, $p_j = p_{j1} \wedge \ldots \wedge p_{jm_j}$ separação conjuntiva sobre $i_{j1}, \ldots, i_{jm_j} \in Sb^1_{ob}$. Para cada $1 \leq j \leq n$ seja $q_{jk} \in CE_{i_{jk}}$ tal que $p_{jk} = (\sigma^{i_{jk}}_{ob})_F(q_{jk})$ para cada $1 \leq k \leq m_j$. Seja $A \in ACC_{ob}$ e, para cada $1 \leq j \leq n$, seja $1 \leq k_j \leq m_j$. Sejam ainda

$$X = \{sp \in Sp(A, p, p_{1k_1}, \ldots, p_{nk_n})(f) \cap F_{ob} : eco \not\models_{ob} sp\} \cup$$
$$\bigcup_{1\leq j\leq n}\{sp \in Sp(A, p, p_{1k_1}, \ldots, p_{nk_n})(f) \cap F_{i_{jk_j}} : eco \not\models_{ob} (\sigma^{i_{jk_j}}_{ob})_F(sp)\}$$

e

$$X' = X \backslash (\bigcup_{1\leq j\leq n}(\{sp_{<\diamond b_{i_{jk_j}}, i_{jk_j}>}(f), sp_{<RJst, i_{jk_j}>}(f)\} \cup (\bigcup_{i\in Sb^1_{ob}} sp_{<Intr, i_{jk_j}, i>}(f)))).$$

Para cada $sp \in X'$ seja a família $\mathcal{E}_{sp} = \{E^{sp}_{ob'}\}_{ob' \in Sb^1_{ob} \cup Sb^2_{ob}}$ uma explicação para *sp* em *eco*. Se

$$\mathcal{E} = \{E_{ob'}\}_{ob' \in Sb^1_{ob} \cup Sb^2_{ob}}$$

onde, para cada $ob' \in Sb^1_{ob} \cup Sb^2_{ob}$,

$$E_{ob'} = (\bigcup_{sp\in X'} E^{sp}_{ob'}) \cup \overline{E}_{ob'}$$

com $\overline{E}_{ob'} = X \cap (\{sp_{<\diamond b_{i_{jk_j}}, i_{jk_j}>}(f), sp_{<RJst, i_{jk_j}>}(f)\} \cup (\bigcup_{i\in Sb^1_{ob}} sp_{<Intr, i_{jk_j}, i>}(f)))$ se $ob' = i_{jk_j}$ para algum $1 \leq j \leq n$ e $\overline{E}_{ob'} = \emptyset$ se $ob' \notin \bigcup_{1\leq j\leq n}\{i_{jk_j}\}$, é *eco*-possível então $\mathcal{E}$ é uma explicação para o problema f em *eco* com base em A, p e $p_{1k_1}, \ldots, p_{nk_n}$.

Prova: A prova é semelhante à apresentada para a Proposição 4.102. ∎

Exemplo 4.108 Considere-se de novo a especificação de comunidade de objectos *eco* referida no Exemplo 4.25. A fórmula

$$f = y^4 \Rightarrow (y^1 \mathbf{U}\, (z^1 \wedge y^4)) \in O_{\{1,4\}}$$

é um problema de garantia em *eco*. Seguindo a notação usada na Definição 4.106 tem-se que neste caso $r = y^4$, $q_1 = y^1$ e $q_2 = z^1 \wedge y^4$. Sendo $p_1 = y^1 \wedge (\neg z^1)$ e $p_2 = y^1 \wedge (\neg y^4)$ tem-se que a fórmula $p = p_1 \vee p_2 \in DSC(q_1 \wedge (\neg q_2))$.

Pretende-se encontrar explicações para f com base em $A = \{c^1, a^4\}$, p e p_{11}, p_{22}. Neste caso, $p_{11} = p_1$, $p_{22} = \neg y^4$ e $k_1 = 1$ e $k_2 = 2$. Seguindo a notação usada na Definição 4.101 tem-se que $i_{11} = 1$ e $i_{22} = 4$. Deste modo, $a^A_{i_{11}} = c^1$ e $a^A_{i_{22}} = a^4$ e, consequentemente, $b_{i_{11}} = c$ e $b_{i_{22}} = a$.

1. Tem-se que $sp_{seg}(f) = y^4 \Rightarrow (y^1 \mathbf{W}\, (z^1 \wedge y^4))$ e $eco \not\models_{\{1,4\}} sp_{seg}(f)$.
Seja $f' = sp_{seg}(f)$.

1.1 Tem-se que $sp_{CI}(f') = y^4 \Rightarrow (y^1 \vee (z^1 \wedge y^4))$ e $eco \not\models_{\{1,4\}} sp_{CI}(f')$.

1.1.1 O tableau t representado na Figura 4.5 é tableau de decisão em $T_{\{1,4\}}(G^{\stackrel{ci}{-}\, sp_{CI}(f')}_{<eco,\{1,4\}>})$.

A família de conjuntos de constrangimentos de estado

$$\begin{array}{ccc} & \neg z^1 & \\ & y^4 & \\ & \neg u^4 & \\ & \neg(y^4 \Rightarrow (y^1 \vee (z^1 \wedge y^4))) & \\ & | & \\ & y^4 & \\ & \neg(y^1 \vee (z^1 \wedge y^4)) & \\ & | & \\ & \neg y^1 & \\ & \neg(z^1 \wedge y^4) & \\ \swarrow & & \searrow \\ \neg z^1 & & \neg y^4 \\ & & \times \end{array}$$

Figura 4.5: Tableau de decisão para $\{\neg z^1, y^4, \neg u^4, \neg(y^4 \Rightarrow (y^1 \vee (z^1 \wedge y^4)))\}$

$$\begin{aligned} \mathcal{E}^1 &= \{E^1_{ob'}\}_{ob' \in \{1,4\,\{1,4\}\}} \text{ onde} \\ E^1_1 &= \{y\} \\ E^1_4 &= E^1_{\{1,4\}} = \emptyset \end{aligned}$$

é induzida pela família de literais induzida pelo fecho $\{\neg y^1\}$ de t e é uma explicação para $sp_{CI}(f')$.

1.2 Tem-se que $sp_{seg}(f') = \mathbf{G}((q_1 \wedge (\neg q_2)) \Rightarrow (\mathbf{X}(q_1 \vee q_2)))$ e $eco \not\models_{\{1,4\}} sp_{seg}(f')$.

1.2.1 As únicas acções compostas que não garantem $q_1 \vee q_2$ a partir de $q_1 \wedge (\neg q_2)$ são $\{b^1, \perp^4\}$, $\{b^1, a^4\}$ e $\{b^1, c^4\}$. Procedendo como anteriormente encontra-se a família de conjuntos de restrições de activação

$$\begin{aligned} \mathcal{E}^2 &= \{E^2_{ob'}\}_{ob' \in \{1,4\,\{1,4\}\}} \text{ onde} \\ E^2_1 &= \{\mathbf{G}(\diamond b \Rightarrow (\neg y))\} \\ E^2_4 &= E^2_{\{1,4\}} = \emptyset \end{aligned}$$

como explicação para $sp_{seg}(f')$.

1.3. A família de conjuntos

$$\begin{aligned} \mathcal{E}^3 &= \{E^3_{ob'}\}_{ob' \in \{1,4\,\{1,4\}\}} \text{ onde} \\ E^3_1 &= \{y,\, \mathbf{G}(\diamond b \Rightarrow (\neg y))\} \\ E^3_4 &= E^3_{\{1,4\}} = \emptyset \end{aligned}$$

é uma explicação para $sp_{seg}(f)$.

2. Tem-se que $sp_{\nabla A}(f) = \mathbf{G}((\nabla c^1 \wedge \nabla a^4 \wedge q_1 \wedge (\neg q_2)) \Rightarrow (\mathbf{X}\, q_2))$ e $eco \models_{\{1,4\}} sp_{\nabla A}(f)$.

3. Tem-se que $sp_{<\diamond c,1>}(f) = \mathbf{G}((y \wedge (\neg z)) \Rightarrow \diamond c)$ e $eco \not\models_{\{1,4\}} (\sigma^1_{\{1,4\}})_F(sp_{<\diamond c,1>}(f))$.

4. Tem-se que $sp_{<\diamond a,4>}(f) = \mathbf{G}((\neg y) \Rightarrow \diamond a)$ e $eco \not\models_{\{1,4\}} (\sigma^4_{\{1,4\}})_F(sp_{<\diamond a,4>}(f))$.

5. Tem-se que $eco \not\models_{\{1,4\}} (\sigma^1_{\{1,4\}})_F(sp_{<RJst,1>}(f))$.

6. Tem-se que $eco \not\models_{\{1,4\}} (\sigma^4_{\{1,4\}})_F(sp_{<RJst,4>}(f))$.

7. Tem-se que $sp_{<Intr,1,4>}(f) = \mathbf{G}(\mathbf{t} \Rightarrow (\nabla c^1 \Rightarrow \nabla a^4))$ e $eco \not\models_{\{1,4\}} sp_{<Intr,1,4>}(f)$.

8. Tem-se que $sp_{<Intr,2,4>}(f) = \mathbf{G}(\mathbf{t} \Rightarrow (\nabla a^4 \Rightarrow \nabla c^1))$ e $eco \not\models_{\{1,4\}} sp_{<Intr,4,1>}(f)$.

9. A família

$$\begin{aligned} \mathcal{E} &= \{E_{ob'}\}_{ob' \in \{1,4,\{1,4\}\}} \text{ onde} \\ E_1 &= \{y, \mathbf{G}(\diamond b \Rightarrow (\neg y)), \\ &\qquad \mathbf{G}((y \wedge (\neg z)) \Rightarrow \diamond c), (\mathbf{G}(\mathbf{F} \diamond c) \Rightarrow (\mathbf{G}(\mathbf{F} \nabla c)\} \\ E_4 &= \{\mathbf{G}((\neg y) \Rightarrow \diamond a), (\mathbf{G}(\mathbf{F} \diamond a)) \Rightarrow (\mathbf{G}(\mathbf{F} \nabla a))\} \\ E_{\{1,4\}} &= \{\mathbf{G}(\mathbf{t} \Rightarrow (\nabla c^1 \Rightarrow \nabla a^4)), \mathbf{G}(\mathbf{t} \Rightarrow (\nabla a^4 \Rightarrow \nabla c^1))\} \end{aligned}$$

é explicação para o problema de garantia. ∎

4.8.4 Problemas de persistência

Nesta subsecção descreve-se a construção de explicações para problemas de persistência no âmbito de uma comunidade de objectos. Tal como anteriormente, as explicações para um problema de persistência são encontradas à custa de explicações para um problema de segurança e para um problema de resposta.

Recorde-se que se assumiram fixados no princípio desta secção $i_1 \ldots i_m \in Enm(ob)$ e $r, q \in CE^{\mathbf{tf}}_{ob}$.

Proposição 4.109 Se

(i) $eco \models \mathbf{G}(q \Rightarrow (\mathbf{X}\, q))$,

(ii) $eco \models \mathbf{G}(r \Rightarrow (\mathbf{F}\, q))$,

então $eco \models \mathbf{G}(r \Rightarrow (\mathbf{F}(\mathbf{G}\, q)))$

Prova: A prova é análoga à apresentada para a Proposição 3.105. ∎

Definição 4.110 Seja $f = \mathbf{G}(r \Rightarrow (\mathbf{F}(\mathbf{G}\, q))) \in O_{ob}$. Os *subproblemas para a explicação de* f são as fórmulas

- $sp_{seg}(f) = \mathbf{G}(q \Rightarrow (\mathbf{X}\, q))$;
- $sp_{resp}(f) = \mathbf{G}(r \Rightarrow (\mathbf{F}\, q))$.

O conjunto dos subproblemas para a explicação de f é o conjunto constituído pelas fórmulas anteriores e denota-se por $Sp(f)$. ∎

Proposição 4.111 Seja $f = \mathbf{G}(r \Rightarrow \mathbf{F}(\mathbf{G}(q))) \in O_{ob}$ um problema de persistência em *eco*. Seja

$$X = \{sp \in Sp(f) : eco \not\models_{ob} sp\}$$

e para cada $sp \in X$ seja $\mathcal{E}_{sp} = \{E^{sp}_{ob'}\}_{ob' \in Sb^1_{ob} \cup Sb^2_{ob}}$ uma explicação para sp em *eco*. Se

$$\mathcal{E} = \{E_{ob'}\}_{ob' \in Sb^1_{ob} \cup Sb^2_{ob}}$$

onde $E_{ob'} = \bigcup_{sp \in X} E^{sp}_{ob'}$ para cada $ob' \in Sb^1_{ob} \cup Sb^2_{ob}$, é *eco*-possível então $\mathcal{E}$ é uma explicação para o problema de persistência f.

Prova: A prova é semelhante à apresentada para a Proposição 4.96, recorrendo aqui à Definição 4.110 e Proposição 4.109. ∎

Exemplo 4.112 Considere-se novamente a especificação de comunidade de objectos *eco* referida no Exemplo 4.25. A fórmula

$$f = \mathbf{F}(\mathbf{G}(x^3 \wedge y^4)) \in O_{\{3,4\}}$$

é um problema de persistência em *eco*.

1. Tem-se que $sp_{seg}(f) = \mathbf{G}((x^3 \wedge y^4) \Rightarrow (\mathbf{X}(x^3 \wedge y^4)))$ e $eco \not\models_{\{2,4\}} sp_{seg}(f)$. Procedendo como anteriormente é possível construir a família de conjuntos de restrições de activação

$$\begin{aligned} &\mathcal{E}' = \{E'_{ob'}\}_{ob' \in \{3,4\,\{3,4\}\}} \text{ onde} \\ &\quad E'_4 = \{\mathbf{G}(\diamond c \Rightarrow (\neg y))\} \\ &\quad E'_3 = E'_{\{3,4\}} = \emptyset \end{aligned}$$

que constitui uma explicação para $sp_{seg}(f)$.

2. Tem-se que $sp_{resp}(f) = \mathbf{G}(\mathbf{F}(x^3 \wedge y^4))$ e $eco \not\models_{\{3,4\}} sp_{resp}(f)$. No Exemplo 4.103 foi encontrada uma explicação para $sp_{resp}(f)$.

3. A família

$$\begin{aligned} &\mathcal{E} = \{E_{ob'}\}_{ob' \in \{3,4,\{3,4\}\}} \text{ onde} \\ &\quad E_3 = \{\mathbf{G}((\neg x) \Rightarrow \diamond c), (\mathbf{G}(\mathbf{F}\diamond c) \Rightarrow (\mathbf{G}(\mathbf{F}\,\triangledown c)\} \\ &\quad E_4 = \{\mathbf{G}(\diamond c \Rightarrow (\neg y)), \mathbf{G}((\neg y) \Rightarrow \diamond a), (\mathbf{G}(\mathbf{F}\diamond a)) \Rightarrow (\mathbf{G}(\mathbf{F}\,\triangledown a))\} \\ &\quad E_{\{3,4\}} = \{\mathbf{G}(\mathbf{t} \Rightarrow (\triangledown c^3 \Rightarrow \triangledown a^4))\} \end{aligned}$$

é explicação para o problema de persistência. ∎

4.9 Conclusões

Neste capítulo foi analisado, numa perspectiva abdutiva, o problema da verificação, no âmbito de uma especificação de comunidades de objectos.

As propriedades (as observações) que se pretendem assegurar neste caso estão relacionadas com o comportamento conjunto de vários objectos (ditos primários) resultante do comportamento especificado individualmente para cada um e das interacções especificadas. Tal como anteriormente, elas foram classificadas em propriedades de segurança, resposta, garantia e persistência e foram expressas à custa de fórmulas na linguagem de objectos apropriados (ditos compostos).

Tal como anteriormente, foram consideradas como fórmulas abdutíveis os constrangimentos de estado, as restrições de activação e os requisitos de justiça na linguagem dos vários objectos primários envolvidos, mas, neste caso, foram também consideradas abdutíveis as fórmulas de interacção na linguagem de certos objectos compostos. Cada explicação é uma família de conjuntos de fórmulas abdutíveis na qual cada conjunto contém as fórmulas relativas a um particular objecto.

As técnicas de geração de explicações são semelhantes às apresentadas para o caso local. As diferenças existentes estão relacionadas, por um lado, com a existência de fórmulas de interacção: os conjuntos de constrangimentos de estado para os quais se constroem os tableaux que contribuem para a geração de explicações têm uma componente relacionada com as fórmulas de interacção especificadas; por outro lado, tanto as novas condições iniciais, como os constrangimentos de estado envolvidos nas novas restrições de activação e fórmulas de interacção construídas, têm de ser conjunções de literais e não disjunções de conjunções de literais como no caso local.

Foram referidos vários critérios de preferência entre as explicações geradas pelas técnicas propostas.

Ao longo deste capítulo foram apresentados diversos exemplos ilustrativos das técnicas descritas.

Capítulo 5

Conclusões

Tradicionalmente, o problema da verificação de especificações centradas em objectos consiste em propor métodos que permitam confirmar que o comportamento do objecto/comunidade de objectos prescrito por uma dada especificação satisfaz certas propriedades. Nesta dissertação a questão da verificação no âmbito da especificação de objectos/comunidade de objectos foi analisada de um ponto de vista que não tem vindo a ser explorado. Este ponto de vista consiste em propor métodos que, nos casos em que o comportamento especificado não verifica as propriedades pretendidas, possam contribuir para auxiliar a tarefa de especificação, sugerindo possíveis enriquecimentos coerentes da especificação dada. O problema da verificação visto sob esta perspectiva foi encarado como uma tarefa a ser tratada num enquadramento abdutivo: as situações em que a especificação em causa não verifica uma determinada propriedade são vistas como *problemas de abdução* para os quais se pretendem encontrar *explicações*.

A especificação de objectos/comunidades de objectos é baseada na lógica temporal linear, na linha do trabalho apresentado em [60, 61]. Nesta dissertação, o trabalho foi desenvolvido no contexto proposicional. Em primeiro lugar trabalhou-se a nível local, isto é, no contexto de um objecto. A este nível a tarefa consiste em assegurar que, isoladamente, o comportamento do objecto determinado pela especificação satisfaz certas propriedades. Em segundo lugar trabalhou-se a nível global, isto é, no âmbito de comunidades objectos vistas como conjuntos de objectos concorrentes que comunicam entre si. A este nível a tarefa consiste em assegurar que o comportamento conjunto de vários de objectos, determinado pelas suas especificações individuais e pelas interacções especificadas, satisfaz certas propriedades.

A natureza do problema a tratar sugeriu naturalmente que o trabalho deveria ser desenvolvido no contexto da abordagem lógica ao raciocínio abdutivo. No âmbito do enquadramento abdutivo do problema, as propriedades que se desejam ver verificadas pelo comportamento dos objectos desempenham o papel de observações. As fórmulas com as quais se pode enriquecer uma especificação são vistas, neste enquadramento, como as fórmulas abdutíveis. No caso local, as observações consideradas são (seguindo as designações apresentadas em [41, 42] no contexto da especificação do comportamento de sistemas reactivos) classificadas em observações de segurança, observações de resposta, observações de garantia e observações de persistência e correspondem a requisitos sobre a evolução do valor dos atributos. As fórmulas abdutíveis são constrangimentos de estado, restrições de activação e requisitos de justiça. As explicações para os problemas de abdução são conjuntos de fórmulas abdutíveis com os quais se enriquece a especificação dada de modo a que a especificação resultante seja coerente e verifique a observação em causa. As explicações consideradas representam assim novos requisitos sobre condições iniciais e sobre a evolução do objecto.

As técnicas propostas para geração de explicações têm por base as técnicas de verificação de propriedades de segurança [43] e de propriedades de resposta [41] e animação [39] de sistemas reactivos concorrentes e as técnicas baseadas em tableaux para raciocínio abdutivo em lógica proposicional [45]. Estas técnicas não garantem que todos os conjuntos de fórmulas abdutíveis construídos conduzem a novas especificações coerentes. Após a fase de construção tem de se seguir uma fase de teste à coerência a qual se viu poder ser conduzida recorrendo a tableaux temporais. Como, em geral, podem ser geradas várias explicações para cada problema de abdução, foi também analisada a questão de seleccionar as explicações segundo certos critérios de preferência e impedir, em alguns casos, a construção de algumas explicações.

Para tratar a questão a nível global foi feita uma extensão das técnicas acimas descritas.

O enquadramento abdutivo do problema em questão é análogo ao proposto para o nível local. As observações, classificadas de modo semelhante, são requisitos sobre o comportamento conjunto de vários objectos e as explicações podem incluir novas interacções entre os objectos envolvidos.

Foram propostas técnicas abdutivas para geração de explicações semelhantes às descritas para o caso local. Fez-se também referência a critérios de preferência entre as explicações geradas.

Em [45] são apresentadas, em paralelo com as técnicas baseadas em tableaux para raciocínio abdutivo em lógica proposicional, técnicas semelhantes com base no cálculo de sequentes de Gentzen. Em alternativa à utilização de tableaux para construção de explicações para problemas de abdução em especificações de objectos/comunidades de objectos da forma que foi descrita neste trabalho poder-se-ia também utilizar, de um modo semelhante, o cálculo de sequentes de Gentzen.

Apontam-se seguidamente algumas direcções para futuro desenvolvimento do trabalho apresentado ao longo desta dissertação.

Nas secções dedicadas à geração de explicações para a garantia de um constrangimento de estado a partir de outro constrangimento de estado através de uma acção e para a garantia inicial de um constrangimento de estado mostrou-se que a técnica de geração proposta possui um certo tipo de completude face a uma certa classe de explicações. Para cada explicação dessa classe existe sempre uma explicação entre as que são geradas que é mais liberal do que ela.

Uma questão que pode ser analisada consiste em procurar outras classes de explicações para as quais as técnicas de geração aqui propostas possuem este tipo de completude.

Uma outra questão poderá passar pela definição de outros critérios interessantes que determinem classes de explicações face às quais as técnicas descritas sejam completas (no sentido a que se fez referência).

As fórmulas que foram consideradas como abdutíveis foram constrangimentos de estado, restrições de activação, requisitos de justiça e fórmulas de interacção. Não foi assim contemplada a hipótese de alterar o modo como a ocorrência das acções afecta os valores dos atributos. Explorar esta hipótese constituí um possível desenvolvimento ao trabalho apresentado.

Outro tópico a explorar é que se relaciona com o desenvolvimento de outros critérios de preferência entre explicações quer no contexto de uma especificação de objecto quer no contexto de uma especificação de comunidades de objectos.

A abordagem à especificação de objectos/comunidades de objectos adoptada nesta dissertação é baseada na lógica temporal proposicional. Um desenvolvimento importante consiste em fazer uma extensão das soluções propostas para o caso da lógica temporal de primeira ordem.

Uma questão também relevante é o desenvolvimento das técnicas propostas considerando a existência de classes de objectos e a possibilidade de herança entre classes de objectos.

Referências

[1] D. Allemang, M. Tanner, T. Bylander e J. Josepheson. Computational complexity of hypothesis assembly. Em *Proceedings of the IJCAI*, págs 1112–1117, 1987.

[2] B. Alpern e F. Schneider. Defining liveness. *Info. Proc. Letters*, 21(4):445–495, 1985.

[3] P. Andrews. *An Introduction to Mathematical Logic and Type Theory*. Academic Press, 1986.

[4] J. Bell e M. Machover. *A Course in Mathematical Logic*. North-Holland, 1977.

[5] M. Ben-Ari. *Mathematical Logic for Computer Science*. Prentice Hall, 1993.

[6] K. Clark. Negation as failure. Em Gallaire e Minker (eds), *Logic and Data Bases*, págs 293–322. Plenum, New York, 1978.

[7] L. Console, D. Dupré e P. Torasso. A theory of diagnosis for incomplete causal models. Em *Proceedings of the IJCAI*, págs 1311–1317, 1989.

[8] L. Console, D. Dupré e P. Torasso. On the relationship between abduction and deduction. *Journal of Logic and Computation*, 1(5):661–690, 1991.

[9] P. Cox e T. Pietrzykowski. Causes for events: their computation and applications. Em *Proceedings of 8th International Conference on automated Deduction, CADE'86*, págs 608–621, 1986.

[10] P. Cox e T. Pietrzykowski. General diagnosis by abductive inference. Em *Proceedings of the IEEE Symp. on Logic Programming*, págs 183–189, 1987.

[11] O.-J. Dahl, B. Myhrhaugh e K. Nygaard. *SIMULA 67: Common Base Language*. Norwegian Computing Center, 1967.

[12] J. deKleer. An assumption-based tms. *Artificial Intelligence*, 32:127–162, 1986.

[13] E. Emerson. Temporal and modal logic. Em J. van Leeuwen (ed), *Handbook of Theoretical Computer Science B: Formal Models and Semantics*, págs 995–1072. Elsevier, 1990.

[14] K. Eshghi. Abductive planning with event calculus. Em *Proceedings of the 5th ICLP*, 1988.

[15] K. Eshghi. A tractable class of abduction problems. Em *Proceedings of the IJCAI 93*, págs 3–8, 1993.

[16] K. Eshghi e R. Kowalski. Abduction compared with negation by failure. Em *Proceedings of the 6th ICLP*, págs 234–254, 1989.

[17] J. Fiadeiro e T. Maibaum. Temporal reasoning over deontic specifications. *Journal of Logic and Computation*, 3(1):357–395, 1991.

[18] J. Fiadeiro e T. Maibaum. Temporal theories as modularization units for concurrent system specification. *Formal Aspects of Computing*, 4(3):239–272, 1992.

[19] J. Fiadeiro, C. Sernadas, T. Maibaum e G. Saake. Proof-theoretic semantics of object-oriented specification constructs. Em R. Meersman, W. Kent e S. Khosla (eds), *Object Oriented Databases: Analysis, Design and Construction (DS-4)*, págs 243–284. Elsevier Science Publishers B. V. (North-Holland), 1991.

[20] J. Fiadeiro, C. Sernadas, T. Maibaum e A. Sernadas. Describing and structuring objects for conceptual schema development. Em P. Loucopolos e R. Zicari (eds), *Conceptual Modeling, Databases and CASE: An Integrated View of Information Systems Development*, págs 117–138. John Wiley, 1992.

[21] M. Fitting. *First-Order Logic and Automated Theorem Proving*. Spriger-Verlag, 1990.

[22] N. Francez. *Fairness*. Springer-Verlag, 1986.

[23] A. Goldberg e D. Robson. *Smalltalk 80: the language and its implementation*. Addisson-Wesley, 1983.

[24] P. Gouveia. Tableaux para raciocínio local sobre objectos. Tese de Mestrado, Instituto Superior Técnico, 1993.

[25] P. Gouveia e C. Sernadas. Reasoning aspects in information systems and databases. Em A. Olivé (ed), *The Deductive Approach to Information Systems and Databases 93*, págs 201–224. Universitat Politècnica de Catalunya, 1993.

[26] P. Gouveia e C. Sernadas. Abduction in temporal object specification using tableaux. Em P. Baumgartner, R. Hahnle, e J. Possega (eds), *4th Workshop on Theorem Proving with Analytic Tableaux and Related Methods - Poster Session and Short Papers*, págs 43–48. University of Koblenz, 1995.

[27] P. Gouveia e C. Sernadas. Introducing explanations in temporal object specification. Em R. Wieringa e R. Feenstra (eds), *IS-CORE'94 - Selected Papers*, págs 53–68. World Scientific Publishers, 1995.

[28] P. Gouveia, C. Sernadas, J. Gomes e M.-J. Apolinário. Tableau for reasoning about objects. Em *Theorem proving with analytic tableaux and related methods*, págs 113–125. Max Plank Institut fur Informatik, 1993.

[29] K. Inoue. An abductive procedure for the cms/atms. Em *LNAI 515*, págs 34–53. Springer Verlag, 1991.

[30] A. Kakas, R. Kowalski e F. Toni. Abductive logic programming. *Journal of Logic and Computation*, 2(6):719–770, 1992.

[31] A. Kakas e P. Mancarella. Knowledge assimilation and abduction. Em *Poc. European Conference on Artificial Intelligence*, págs 54–70. Springer Verlag, 1990.

[32] Y. Kesten, Z. Manna, H. McGuire e A. Pnueli. A decision algorithm for full propositional temporal logic. Em *LNCS 697*, págs 97–109. Springer Verlag, 1993.

[33] K. Konolige. Abduction versus closure in causal theories. *Artificial Intelligence*, 53:255–272, 1992.

[34] L. Lamport. Proving the correctness of multiprocess programs. *IEEE Transactions on Software Engineering*, 3(2):125–143, 1977.

[35] L. Lamport. Basic concepts. Em *Distributed systems: methods and tools for specification, LNCS 190*, págs 19–30. Springer Verlag, 1985.

[36] H. Levesque. A knowledge-level account of abduction. Em *Proceedings of the IJCAI*, págs 1061–1067, 1989.

[37] R. Li e A. Sernadas. Reasoning about objects using tableau method. *Journal of Logic and Computation*, 1(5):575–611, 1991.

[38] O. Lichtenstien, A. Pnueli e L. Zuck. The glory of the past. Em *Proc. Conf. on Logics of Programs, LNCS 193*, págs 196–218. Springer Verlag, 1985.

[39] Z. Manna e A. Pnueli. Adequate proof principles for invariance and liveness properties of concurrent programs. *Science of Computer Programming*, 4:257–289, 1984.

[40] Z. Manna e A. Pnueli. The anchored version of temporal framework. Em J. de Bakker, W.-P. de Roever, e G. Rozenberg (eds), *Linear Time, Branching Time and Partial Order in Logics and Models for Concurrency, LNCS 354*, págs 201–284. Springer Verlag, 1989.

[41] Z. Manna e A. Pnueli. Completing the temporal picture. *Theoretical Computer Science*, 83:97–130, 1991.

[42] Z. Manna e A. Pnueli. *The Temporal Logic of Reactive and Concurrent Systems: Specification.* Springer Verlag, 1992.

[43] Z. Manna e A. Pnueli. *The Temporal Logic of Reactive and Concurrent Systems: Safety.* Springer Verlag, 1995.

[44] P. Marquis. Extending abduction from propositional to first-order logic. Em P. Jorrand e J. Keleman (eds), *Fundamentals of Artificial Intelligence Research, LNAI 535*, págs 140–155. Sringer-Verlag, 1991.

[45] M. Mayer e F. Pirri. First order abduction via tableau and sequent calculi. Em *Bulletin of the IGPL 1 (1)*, págs 99–117. 1993.

[46] M. Mayer e F. Pirri. Propositional abduction in modal logic. Em *Proceedings of the 3rd Workshop on Theorem Proving with Analytic Tableaux and Related Methods*, 1994.

[47] M. Mayer e F. Pirri. Propositional abduction in modal logic. *J. IGPL 3*, 6:907–919, 1995.

[48] G. Paul. Approaches to abductive reasoning: an overview. *Artificial Intelligence Review*, 7:109–152, 1993.

[49] C. Peirce. Abduction and induction. Em Buchler (ed), *Philosophical Writings of Peirce*, págs 150–156. Dover, 1955.

[50] A. Pnueli. The temporal logic of programs. Em *Proceedings of the 18th IEEE Symposium on Foundations of Computer Science*, págs 46–57. 1977.

[51] D. Poole. A logical framework for default reasoning. *Artificial Intelligence*, 36:27–47, 1988.

[52] H. Pople. On the mechanization of abductive logic. Em *Proceedings IJCAI 73*, págs 147–151, 1973.

[53] J. Ramos. Lógica de certificação *gnome*. Tese de Mestrado, Instituto Superior Técnico, 1994.

[54] J. Reggia, D. Nau e P. Wang. A formal model of diagnostic inference. *Information Sciences*, 27:227–256, 1985.

[55] R. Reiter. A logic for default reasoning. *Artificial Intelligence*, 13:81–132, 1980.

[56] B. Ross. Running programs backwards: the logical inversion of imperative computation. *Formal Aspects of Computing*, 9:331–348, 1997.

[57] A. Sernadas e H.-D. Ehrich. What is an object, after all? Em R. Meersman, W. Kent, e S. Khosla (eds), *Object Oriented Databases: Analysis, Design and Construction*, págs 39–69. North-Holland, 1991.

[58] A. Sernadas, J. Fiadeiro, C. Sernadas e H.-D. Ehrich. Abstract object types: a temporal perspective. Em B. Banieqbal, H. Barringer, e A. Pnueli (eds), *Temporal Logic in Specification*, págs 324–350. Springer-Verlag, 1989.

[59] A. Sernadas, J. Fiadeiro, C. Sernadas e H.-D. Ehrich. The basic building blocks of information systems. Em E. Falkenberg e P. Lindgreen (eds), *Information Systems Concepts: An In-depth Analysis*, págs 225–246. North-Holland, 1989.

[60] A. Sernadas, C. Sernadas e J. Costa. Object specification logic. *Journal of Logic and Computation*, 5(5):603–630, 1995.

[61] A. Sernadas, C. Sernadas e J. Ramos. A temporal logic approach to object certification. *Data & Knowledge Engineering*, 19:267–294, 1996.

[62] M. Shanahan. Prediction is deduction but explanation is abduction. Em *Proceedings of the IJCAI*, págs 1055–1060, 1989.

[63] A. Sistla. On the caracterization of safety and liveness properties in temporal logic. Em *Proc. 4th ACM Symp. Princ. of Dist. Comp.*, págs 39–48, 1985.

[64] M. Stickel. Rationale and methods for abductive reasoning in natural language interpetation. Em *Proceedings International Scientific Symposium on Natural Language and Logic*, págs 233–252. Springer Verlag, 1989.

[65] P. Wegner. Concepts and paradigms of object-oriented programming. *OOPS Messenger*, 1(1):7–87, 1990.

[66] P. Wolper. The tableau method for temporal logic: an overview. *Logique et Anal.*, 28, 1985.