Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

O Problema da Dedução do Intruso para um Protocolo Criptográfico Especificado via Reescrita Módulo AC

por

Daniele Nantes Sobrinho

Orientador: Mauricio Ayala Rincón

Brasília
2009

“ Se consegui enxergar mais longe é porque estava
apoiado sobre ombros de gigantes. ”
(Isaac Newton)

Aos meus pais,
Antonio Aparecido Sobrinho e
Selma Pereira Nantes.
Os gigantes da minha vida...

“ Não devemos deixar de explorar.
E no final da exploração,
vamos chegar onde começamos
e conhecer o lugar pela primeira vez. ”
(T.S. Elliot)

Agradecimentos

À Deus, que me manteve no caminho sempre, auxiliando-me e fortalecendo-me em todos os momentos da minha vida.

Aos meus pais, Antonio e Selma e minha avó Aura, por acreditarem em mim desde o meu nascimento, pela força e oração diária, pela presença em minha vida mesmo na distância, pelo amor, proteção, carinho, pela educação que me deram e pela fé que eles tem em mim.

Aos meus irmãos, Gizele e Lucas Rafael, por fazerem parte da minha vida e por encherem meu coração de amor, alegria e orgulho.

Ao João Paulo, pelo amor, carinho, paciência, pela sua presença, pela disposição de muitas vezes aprender para me ensinar, por ter participado de todas as fases deste trabalho e por fazer dos meus dias mais felizes.

Ao professor Mauricio Ayala Rincon, pela oportunidade de trabalhar em conjunto, pela dedicação, paciência, profissionalismo, disposição, incentivo, pela orientação sempre séria tanto nas aulas como nas discussões relacionadas a este trabalho e também por ter me mostrado um mundo inteiro de coisas a aprender.

Ao amigo e pesquisador Sergiu Bursuc pela paciência e disposição em responder todas as minhas perguntas e cuja colaboração foi essencial para conclusão deste trabalho.

Aos amigos Fernanda Gomes, Simone, Ana Paula, Daniel Ventura, Marcelo Bezerra, Gustavo Monge, Juliana Mündel e Ana Cláudia, pela ajuda insubstituível nos estudos, pela profundidade com que marcaram a minha vida, ora sorrindo, ora chorando, partici-

pando da minha vida dentro e fora da universidade.

Aos colegas de estudo Adriana, André Caldas, Andréia, Bruno, Bruninho, Emília, Igor, Jorge, Kaliana, Laura, Mariana, Renato, Sérgio, Tarcísio, Thaynara, Wembesom e Wesley.

Aos professores e funcionários do Departamento de Matemática da UnB, sem os quais seria impossível a realização deste trabalho.

Aos professores do Departamento de Matemática da UFMS, por terem dado início à essa jornada. Especialmente a professora Sonia Di Giacomo.

Ao CNPq, pelo apoio financeiro.

Resumo

O ponto inicial deste trabalho é um caso de estudo de um protocolo de carteira eletrônica modelado por uma teoria equacional de um fragmento da aritmética, que inclui exponenciação. Foi estudado um procedimento de decisão para o *problema da dedução do intruso*, proposto recentemente por Bursuc, Comon-Lundh e Delaune. O intruso tem as mesmas capacidades algébricas de dedução que a teoria equacional que modela o protocolo. Associa-se a essa teoria equacional um sistema de reescrita equivalente, que é convergente módulo associatividade e comutatividade. Formula-se a capacidade de dedução do intruso através de um sistema de regras de inferência. Afim de mostrar que o problema em questão pode ser decidido em tempo limitado polinomialmente, será mostrado que esse sistema de dedução tem uma propriedade de *localidade* e que a deducibilidade em um passo é decidida em tempo limitado polinomialmente

Palavras-chave: Teoria da Reescrita; Teoria Equacional, Protocolo Criptográfico; Carteira Eletrônica; Intruso Passivo; Modelo de Dolev-Yao; Propriedade do Variante Finito; Localidade; Deducibilidade em um passo.

Abstract

The starting point of this work is a case study of an electronic purse protocol modeled by an equational theory of a fragment of arithmetic including exponentiation. A decision procedure for the *intruder deduction problem* was studied, which was proposed recently by Bursuc, Comon-Lundh and Delaune. The intruder algebraic deduction capabilities are the same as the ones of the equational theory that model the protocol. This equational theory is associated with an equivalent term rewriting system which is convergent modulo associativity and commutativity. The intruder deduction capabilities are formalized by a system of inference rules. In order to show that this problem can be decided in polynomial time, it is proved that this deduction system has a *locality* property and that the one-step deducibility property is decidable in polynomial time.

Keywords: Rewriting Theory; Equational Theory; Cryptographic Protocol; Eletronic Purse; Passive Intruder; Dolev-Yao Model; Finite Variante Property; Locality; One-step deducibility.

Sumário

Capítulo 1

Introdução

Contextualização

Protocolos criptográficos são essenciais em aplicações de computação distribuída. Eles são usados, por exemplo, em transações bancárias pela internet, serviços de vídeo sob demanda, comunicação sem fio, ou simples serviços de transferência segura de arquivos, como os comandos ssh e scp de UNIX. Protocolos criptográficos podem ser descritos como programas relativamente simples que são executados em um ambiente não confiável. Estes protocolos usam primitivas criptográficas para implementar encriptação simétrica, assimétrica (chave-pública) e assinaturas.

A verificação de protocolos é notoriamente difícil, e mesmo protocolos simples que parecem sólidos podem ter sérias falhas de segurança. Os métodos mais eficazes para verificar tais protocolos recaem em técnicas matemáticas entre as quais se destacam aquelas baseadas em dedução automática e mais recentemente teoria de reescrita. Tais técnicas especificam ou modelam o processo do cálculo que descreve a execução do protocolo, o que permite a demonstração formal de propriedades como a de segurança, entre outras.

Nos últimos anos muito trabalho tem sido direcionado na verificação lógica de segurança de protocolos. Em geral, o problema de segurança é indecidível. Muitos autores

desenvolveram subclasses para as quais existem algoritmos de decisão, *e.g* [BP05,CLC05, Low99,RS05]. Existem diferentes maneiras de modelar protocolos criptográficos e analisar suas propriedades de segurança, por exemplo, a abordagem de Dolev-Yao [DY81], que consiste em modelar um intruso por um sistema de dedução. Este sistema de dedução especifica como um intruso pode obter uma nova informação a partir de conhecimento prévio, que ele tenha obtido silenciosamente através de espionagem da comunicação entre participantes honestos do protocolo (no caso de um intruso *passivo*), ou através de espionagem e emissão de mensagens fraudulentas (no caso de um intruso *ativo*). Chamamos de *problema da dedução do intruso* a questão de se um intruso passivo pode obter certa informação a partir de um conhecimento que ele observa na rede. O modelo de Dolev-Yao reduz este problema para a questão de se uma informação pode ser deduzida a partir de um certo sistema de dedução.

As técnicas assumem na maior parte do tempo a *hipótese da criptografia perfeita*, que afirma que é impossível obter qualquer informação sobre uma mensagem encriptada sem saber exatamente a chave para decriptar esta mensagem. Mais ainda, a álgebra das mensagens deve ser uma álgebra livre. Infelizmente, existem protocolos que podem ser provados seguros com a hipótese da criptografia perfeita, mas que são na verdade inseguros, uma vez que um intruso pode usar propriedades de primitivas criptográficas em combinação com as regras do protocolo afim de obter conhecimento sobre o segredo. A representação de mensagens como termos em uma álgebra livre, permite encontrar alguns ataques, mas falha para maioria deles, principalmente para aqueles que contam com propriedades algébricas. Ou ainda, para alguns protocolos, o programa local de um agente honesto pode contar com algumas propriedades algébricas e o protocolo não tem nenhuma execução honesta no modelo de criptografia perfeita. Essas propriedades são tipicamente expressas como axiomas equacionais (também conhecidos como propriedades algébricas), como por exemplo, associatividade e comutatividade de certos operadores, propriedades de grupos Abelianos, propriedades de exponenciação modular ou associatividade, comu-

tatividade e nilpotência de ou-exclusivo. Algumas vezes, os protocolos não podem nem ser executados quando estas propriedades não são consideradas.

Protocolos mais precisos têm sido, portanto, necessários. Eles assumem que mensagens são termos módulo uma teoria equacional, ou seja, mensagens são representadas por termos construídos sob um alfabeto de símbolos de funções, constantes, encriptação, decriptação, ou-exclusivo, multiplicação entre outros símbolos. Consideramos aqui uma teoria equacional definida por um conjunto de equações para levar em conta as propriedades algébricas dos operadores. Uma lista de teorias equacionais relevantes é proposta em [CDL06]. Provar segurança para um número limitado de sessões em tais modelos formais deu origem a muitos trabalhos. Vale a pena mencionar [RT01, RT03], no qual os autores provaram que o problema de segurança é co-$\mathcal{NP}$ completo no caso de criptografia perfeita. A extensão de várias teorias equacionais já foi considerada, entre elas destaca-se: ou-exclusivo [CLS03], grupos Abelianos [Shm04], algumas propriedades de exponenciação modular [CKRT03], associatividade-comutatividade (AC) [BClD07b], entre outros. Todos estes trabalhos resolvem restrições de deducibilidade módulo teorias equacionais, uma abordagem que é seguida neste trabalho.

Metodologia e objetivos

Aborda-se um caso de estudo de um protocolo de carteira eletrônica, introduzido por S. Bursuc, H. Comon-Lundh e S. Delaune, em [BCLD07a]. O objetivo é provar se o protocolo é seguro ou se existe uma possibilidade ataque.

Para modelagem deste protocolo é considerada, inicialmente, uma teoria equacional que possui as propriedades de exponenciação $(x^y)^z = x^{y \times z}$ e $x^y \times x^z = x^{y+z}$, que são essenciais para execução do protocolo, bem como as propriedades de grupos Abelianos de $+$ (soma) e $\times$ (produto).

Porém, quando são colocadas juntas as propriedade de grupos Abelianos de $+$ e $\times$, pode-se derivar a distributividade de $\times$ com relação a $+$, neste caso, como foi mostrado

em [BS99], a unificação e portanto, a segurança, torna-se indecidível.

Para contornar este problema, foi introduzida uma teoria equacional poderosa o suficiente para que o protocolo seja executado; então, será mostrado que esta teoria pode ser representada por um sistema de reescrita AC-convergente para o qual a unificação é decidível. Para isto é demonstrado que o sistema de reescrita módulo satisfaz a *propriedade do variante finito*, introduzida em [CLD04].

Será realizado um estudo do procedimento de decisão, introduzido em [BCLD07a]. Um importante passo em direção a este resultado, é o estudo de um procedimento para decidir o *problema da dedução do intruso*, na presença de um intruso possuindo capacidades complexas de dedução, que serão modeladas através de um teoria equacional, extensão do modelo de Dolev-Yao. Adota-se a abordagem introduzida por H. Comon-Lundh e V. Shmatikov em [CLS03], uma generalização do método de localidade introduzido por D. McAllester em [McA90], que afirma que existe um algoritmo limitado em tempo polinomial para decidir a deducibilidade de um termo s (que pode ser o segredo), a partir de um conjunto finito de termos T, se o sistema de dedução tem a propriedade de *localidade*. Para que este resultado possa ser usado, será introduzido um sistema de regras de dedução local para representar as capacidades de dedução do intruso.

Porém, esta abordagem sofre de duas importantes restrições:

- O sistema de dedução deve ser finito.
- A noção de localidade é restrita a subtermos sintáticos.

Essas restrições dão origem a sérios problemas quando são consideradas regras que envolvem associatividade e comutatividade de alguns operadores, que é o caso de estudo tratado aqui. Infelizmente, existe em geral, um número exponencial de subtermos módulo AC de um termo dado. A solução proposta por H. Comon-Lundh e V. Shmatikov em [CLS03], que será utilizada aqui, ajuda a evitar o número exponencial de subtermos. No entanto, um novo problema surge: o conjunto de regras passa a ser infinito. Ainda

assim, será mostrado que se pode obter um algoritmo limitado em tempo polinomial implementando o teste de se um termo s é dedutível em um-passo de um conjunto T.

Finalmente, depois de todos estes resultados estabelecidos, será mostrado que o *problema da dedução do intruso* é decidível em tempo polinomial para a teoria equacional que será introduzida e a capacidade do intruso que será adotada aqui.

Resultados

A abordagem seguida é basicamente a mesma de [BCLD07a], mas alguns aspectos não tratados em detalhe nesse trabalho são precisados aqui:

1. A demonstração de que o sistema de reescrita módulo AC satisfaz a *propriedade do variante finito*, o que garante que o problema de unificação é decidível para a teoria que modela o protocolo.

2. A demonstração de que a relação de deducibilidade em um-passo é limitada polinomialmente, o que é fundamental, junto com a localidade do sistema dedutivo, para garantir que o *problema de dedução do intruso* é decidível em tempo polinomial.

Todas as provas são apresentadas detalhadamente eliminando imprecisões e em alguns casos realizando correções do trabalho original [BCLD07a].

Organização

Capítulo 2: Preliminares. Neste capítulo serão apresentadas as definições e resultados básicos sobre sistemas de reescrita, reescrita módulo equações, propriedade do variante finito e condição de fronteira, que serão usados durante o trabalho. Além de relembrar alguns conceitos, a idéia aqui é também estabelecer as notações usadas. As referências usadas neste capítulo, são [CLD04, BN98, DJ90]

Capítulo 3: O protocolo de carteira eletrônica. Neste capítulo, serão descritos protocolo de carteira eletrônica, a teoria equacional utilizada para sua modelagem bem como o sistema de reescrita associado a ela. Além disso, serão apresentados o sistema

de regras de dedução $\mathcal{I}_{\mathsf{EP}}$ que modela a capacidade do intruso e o problema central deste trabalho, o chamado *problema da dedução do intruso*.

Capítulo 4: O problema da dedução do intruso é PTIME para o sistema de inferência $\mathcal{I}_{\mathsf{EP}}$. Neste capítulo será introduzido um novo sistema de dedução, que é equivalente ao anterior mas que tem a propriedade de localidade. Esta propriedade juntamente com o conceito de deducibilidade em um-passo, que também será introduzido neste capítulo, tem papéis fundamentais para a prova de decidibilidade em tempo polinomial do *problema da dedução do intruso*, que será demonstrado no final deste capítulo.

Capítulo 2

Preliminares

Este capítulo é destinado a definições e alguns resultados elementares para o entendimento dos próximos capítulos. Inicialmente, serão introduzidos conceitos referentes à teoria de reescrita. Em seguida serão apresentados resultados relacionados à propriedade do variante finito. Além de relembrar alguns conceitos a idéia aqui é estabelecer as notações utilizadas. Mais detalhes sobre teoria de reescrita e propriedade do variante finito podem ser encontrados em [BN98, DJ90, CLD04].

2.1 Termos, substituições e unificação

Definição 1 (Assinatura) Uma *assinatura* $\mathcal{F}$ é um conjunto de *símbolos de função*, onde cada $f \in \mathcal{F}$ é associado com um inteiro não-negativo n, a *aridade* de f. Para $n \geq 0$, denote o conjunto de todos os elementos n-ários de $\mathcal{F}$ por $\mathcal{F}^{(n)}$. Os elementos de $\mathcal{F}^{(0)}$ são também chamados de *símbolos constantes*.

Por exemplo, para falar sobre *grupos*, que são equipados com um elemento neutro, uma operação unária de inversão, e uma operação de multiplicação binária, usa-se a seguinte assinatura $\mathcal{F}_G = \{e_\bullet, J_\bullet, \bullet\}$, onde $e_\bullet$ tem aridade 0, $J_\bullet$ é unário e $\bullet$ é binário.

Definição 2 (Termos) Seja $\mathcal{F}$ uma assinatura e $\mathcal{X}$ um conjunto de variáveis tais que $\mathcal{F} \cap \mathcal{X} = \emptyset$. O conjunto $T(\mathcal{F}, \mathcal{X})$ de todos os $\mathcal{F}$-termos sobre $\mathcal{X}$ é definido indutivamente da seguinte forma

- $\mathcal{X} \subseteq T(\mathcal{F}, \mathcal{X})$ (i.e. toda variável é um termo),
- para todo $n \geq 0$, todo $f \in \mathcal{F}^{(n)}$, e todos $t_1, \ldots, t_n \in T(\mathcal{F}, \mathcal{X})$,tem-se que $f(t_1, \ldots, t_n) \in T(\mathcal{F}, \mathcal{X})$.

Definição 3 (Posições) Seja $\mathcal{F}$ uma assinatura, $\mathcal{X}$ um conjunto de variáveis disjunto de $\mathcal{F}$, e $s, t \in T(\mathcal{F}, \mathcal{X})$.

1. O conjunto de *posições* do termo s é o conjunto, denotado por $\mathcal{O}(s)$, de palavras sobre os inteiros positivos, que é definido indutivamente como segue:
   - Se $s = x$, então $\mathcal{O}(s) := \{\varepsilon\}$, onde ε denota a palavra vazia.
   - Se $s = f(s_1, \ldots, s_n)$, então
   $$\mathcal{O}(s) := \{\varepsilon\} \bigcup_{i=1}^{n} \{ip \,|\, p \in \mathcal{O}(s_i)\}$$
   A posição ε é chamada *posição raiz* do termo s, e o símbolo de função ou de variável nesta posição é chamado de *símbolo raiz* de s.
2. O *tamanho* de um termo $|s|$ é a cardinalidade de $\mathcal{O}(s)$.
3. Para $p \in \mathcal{O}(s)$, o *subtermo de s na posição p*, denotado por $s|_p$, é definido por indução no comprimento de p:
   $$s|_\varepsilon := s,$$
   $$f(s_1, \ldots, s_n)|_{iq} := s_i|_q.$$
   Note que, para $p = iq, p \in \mathcal{O}(s)$ implica que s é da forma $s = f(s_1, \ldots, s_n)$, com $i \leq n$.

4. Para $p \in \mathcal{O}(s)$, denote por $s[t]_p$ o termo que é obtido de s pela *substituição do subtermo na posição p por t*, i.e.

$$s[t]_\varepsilon := t,$$

$$f(s_1, \ldots, s_n)[t]|_{iq} := f(s_1, \ldots, s_i[t]|_q, \ldots, s_n).$$

5. Seja $\mathcal{V}(s)$ o conjunto de *variáveis ocorrendo em s*, i.e.

$$\mathcal{V}ar(s) := \{x \in \mathcal{X} \mid \text{ existe } p \in \mathcal{O}(s) \text{ tal que } s|_p = x\}.$$

Quando $t|_p$ é uma variável, $p \in \mathcal{O}(s)$ é chamada de *posição variável*.

Exemplo: Seja $t = f(e, f(x, i(x)))$.

$$\begin{aligned} \mathcal{O}(t) &= \{\varepsilon, 1, 2, 21, 22, 221\} \\ t|_{22} &= i(x) \\ t[e]_2 &= f(e, e) \\ \mathcal{V}ar(t) &= \{x\} \\ |t| &= 6 \end{aligned}$$

Definição 4 (Substituição) Seja $\mathcal{F}$ uma assinatura e V um conjunto infinito enumerável de variáveis. Uma *substituição* é uma função $\sigma : V \to T(\mathcal{F}, V)$, tal que $x\sigma \neq x$ apenas para um número finito de variáveis $x \in \mathcal{X}$. Este conjunto (finito) de variáveis é chamado *domínio* de σ:

$$\mathcal{D}om(\sigma) := \{x \in V \mid \sigma(x) \neq x\}$$

Toda substituição σ pode ser *extendida* a uma aplicação $\widehat{\sigma} : T(\mathcal{F}, V) \to T(\mathcal{F}, V)$ da seguinte forma:

$$\widehat{\sigma}(x) := x, \text{ se } x \in V$$

$$\widehat{\sigma}(f(s)) := f(\widehat{\sigma}(s_1), \ldots, \widehat{\sigma}(s_n)), \text{ se } s = f(s_1, \ldots, s_n)$$

Observação 1 Um termo t é chamado uma *instância* de um termo s se, e somente se, existe uma substituição σ tal que $s\sigma = t$.

Definição 5 (Equação) Seja $\mathcal{F}$ uma assinatura e V um conjunto de variáveis infinito enumerável e disjunto de $\mathcal{F}$. Uma *$\mathcal{F}$-equação* (ou simplesmente equação) é um par $(s,t) \in T(\mathcal{F},V) \times T(\mathcal{F},V)$. O *lado direito*(ld) é dado por s e o *lado esquerdo*(le) por t.

Notação: $s = t$

Definição 6 (Equações regulares) Um conjunto de equações E é dito *regular* se, para toda equação $t_1 = t_2 \in E$, $vars(t_1) = vars(t_2)$.

Definição 7 (Congruência) Seja E um conjunto de equações. Denote por $sig(E)$ o conjunto de todos os símbolos de função ocorrendo em E e por $=_E$ a menor congruência em $T(\mathcal{F},\mathcal{X})$ gerada por E, i.e., a menor relação de equivalência gerada por E que é compatível com substituições e a estrutura dos termos: para toda substituição σ, se $u =_E v$, então para todo termo t e $p \in \mathcal{O}(t)$, tal que $t = t[\sigma(u)]_p$, $t[\sigma(u)]_p =_E t[\sigma(v)]_p$.

Definição 8 (Unificador) Seja E um conjunto de equações. Dois termos s,t são chamados *E-unificáveis* se existe uma substituição σ tal que $s\sigma =_E t\sigma$. Tal substituição é chamada *E-unificador* de s,t.

Definição 9 (Algoritmo de E-unificação) Seja E um conjunto de equações. Existe um *algoritmo de E-unificação* se é possível, para quaisquer dois termos s,t, calcular um conjunto finito $\sigma_1,\sigma_2,\ldots,\sigma_n$ de E-unificadores de s,t, tais que, para todo E-unificador σ de s,t, existe um índice i e uma substituição θ tais que, para toda variável $x \in vars(s) \cup vars(t), x\sigma =_E x\sigma_i\theta$.

Definição 10 (Sistema de reescrita de termos) Um *sistema de reescrita de termos (TRS)* é um conjunto de regras de reescrita. Uma *regra de reescrita* é dada por $l \to r$ onde $l \in T(\mathcal{F},\mathcal{X})$ não é uma variável e $\mathcal{V}ar(l) \supseteq \mathcal{V}ar(r)$.

Definição 11 (Terminalidade) Um $TRS\ \mathcal{R}$ é dito *terminante* se não existem sequências infinitas descendentes do tipo $t_1 \rightarrow_{\mathcal{R}} t_2 \rightarrow_{\mathcal{R}} \ldots$.

Observação 2 Um *redex* (ou expressão redutível) é uma instância de uma lado esquerdo de uma regra. *Contração* de um redex significa substituí-lo pela instância correspondente do lado direito da regra.

Definição 12 (Relação de reescrita gerada por um TRS) Seja $\mathcal{R}$ um TRS. A *relação de reescrita* $\rightarrow_{\mathcal{R}} \subseteq T(\mathcal{F}, V) \times T(\mathcal{F}, V)$ é definida por

$$s \rightarrow_{\mathcal{R}} t \text{ se, e somente se, existe uma posição } p \in \mathcal{O}(s) \text{ tal que}$$

$$s|_p = l\sigma \text{ e } t = s[r\sigma]_p.$$

para uma substituição σ e uma regra $l \rightarrow r \in \mathcal{R}$

Lê-se a expressão $s \rightarrow_{\mathcal{R}} t$ como: s *reescreve* para t por um $TRS\ \mathcal{R}$.

Definição 13 (Reescrita módulo) Considere o conjunto $\mathcal{R}$ de regras de reescrita e o conjunto de equações E. *A relação de reescrita módulo* E, é a relação $\rightarrow_{\mathcal{R}/E}$ definida por:

$$s \rightarrow_{\mathcal{R}/E} t \text{ se, e somente se, existe uma posição } p \in \mathcal{O}(s) \text{ tal que}$$

$$s|_p =_E l\sigma \text{ e } t = s[r\sigma]_p$$

para alguma substituição σ e uma regra $l \rightarrow r \in \mathcal{R}$

Definição 14 (Confluência módulo) Um sistema de reescrita $\mathcal{R}$ é *E-confluente* se, e somente se, para todos os termos s, t tais que $s =_{\mathcal{R} \cup E} t$, existem s, t' tais que $s \overset{*}{\rightarrow}_{\mathcal{R}/E} s'$, $t \overset{*}{\rightarrow}_{\mathcal{R}/E} t'$ e $s' =_E t'$. $\mathcal{R}$ é dito *E-convergente* se, além disso, $\rightarrow_{\mathcal{R}/E}$ é terminante.

Onde por $s =_{\mathcal{R} \cup E} t$ entende-se: $[s]_{=_E} \overset{*}{\leftrightarrow}_{\mathcal{R}/E} [t]_{=_E}$.

Mais ainda, se $\rightarrow_{\mathcal{R}/E}$ é convergente então $s =_{\mathcal{R} \cup E} t \Leftrightarrow ([s]_{=_E} \downarrow_{\mathcal{R}/E}) = ([t]_{=_E} \downarrow_{\mathcal{R}/E})$ acontece.

Definição 15 (Forma normal) Um termo t está na *forma normal* (w.r.t $\mathcal{R}/E$) se não existe um termo s tal que $t \rightarrow_{\mathcal{R}/E} s$. Se $t \stackrel{*}{\rightarrow}_{\mathcal{R}/E} s$ e s está na forma normal então s é a forma normal de t. Quando esta forma normal é única ($\mathcal{R}$ é convergente módulo E), denota-se ($t \downarrow_{\mathcal{R}/E}$).

Definição 16 (Substituição normalizada) Uma substituição σ é dita *normalizada* se para todo $x \in \mathcal{D}om(\sigma), x\sigma$ está na forma normal.

Definição 17 (Substituição normalizada módulo) Para um sistema de reescrita E-convergente $\mathcal{R}$ e uma substituição σ, *escreve-se* $\sigma \downarrow_{\mathcal{R}/E}$ para a substituição cujo domínio é $\mathcal{D}om(\sigma)$ e tal que $x(\sigma \downarrow_{\mathcal{R}/E}) = (x\sigma) \downarrow_{\mathcal{R}/E}$ para todo $x \in \mathcal{D}om(\sigma)$.

2.2 Propriedade do Variante Finito e Condição de Fronteira

Nesta seção, será apresentada a propriedade do variante finito, introduzida em [CLD04]. Ela permite reduzir teorias equacionais para alguma outra teoria (supostamente mais simples).

Assuma uma ordem bem fundada $\geq$ em termos, que é total em termos básicos. Dada uma teoria E e um termo t, escreva $t\downarrow_E$ para o menor termo na classe de equivalência de E. Ele servirá como um representante da classe.

Definição 18 ***(E-variante)***. Dados dois conjuntos de equações E e E'. t' é um *E-variante* de um termo t se existe uma substituição θ tal que $t\theta =_E t'$. Um *conjunto completo de E-variantes módulo E' de t (com relação a $\geq$)* é um conjunto S de E-variantes de t tal que, para toda substituição σ, existe um termo $t' \in S$ e uma substituição θ tal que $(t\sigma\downarrow_E) =_{E'} t'\theta$.

Definição 19 ***(propriedade do variante finito)***. O par $(E,\ E')$ tem a *propriedade do variante finito (com relação a $\geq$)* se para todo termo t, podemos efetivamente computar um conjunto completo de E-variantes módulo E' finito.

Dada uma teoria E, para encontrar uma decomposição $(\mathcal{R},\ E')$ para E e uma ordem $\geq$ tal que o par (E, E') tenha a propriedade do variante finito, as seguintes condições devem ser satisfeitas:

1. $\mathcal{R}$ é um sistema E'-convergente para E e $\rightarrow_{\mathcal{R}/E'} \subseteq \geq$ é uma relação decidível,
2. para todo termo t, existe um conjunto finito de variantes $t_1, \ldots, t_n$, efetivamente calculáveis, tais que, para toda substituição σ, existe um índice i e uma substituição θ tal que $(t\sigma\downarrow_{\mathcal{R}/E'}) =_{E'} t_i\theta$.

Para os próximos resultados, considere um teoria E para a qual existe $\mathcal{R}$ e E' tal que $\mathcal{R}$ é um sistema E'-convergente para E.

Definição 20 ***(Propriedade de Fronteira)***.$(\mathcal{R}, E')$ satisfaz a *propriedade de fronteira* se para todo termo t, existe um inteiro n tal que para toda substituição normalizada σ, a forma normal de $t\sigma$ é obtida por uma derivação cujo comprimento pode ser limitado por n (que independe de σ)*:*

$$\forall t, \exists n, \forall \sigma. t(\sigma\downarrow) \xrightarrow{\leq n}_{\mathcal{R}/E'} (t\sigma)\downarrow$$

O seguinte teorema mostra a relação entre a *propriedade de fronteira* e a *propriedade do variante finito.*

Teorema 1 ([CLD04]) Seja E' uma apresentação regular para a qual existe um algoritmo de E'-unificação. Se, além disso $(\mathcal{R}, E')$ satisfaz a propriedade de fronteira então $(\mathcal{R}, E')$ é uma decomposição de E satisfazendo a propriedade do variante finito.

Reciprocamente, se $(\mathcal{R}, E')$ satisfaz a propriedade do variante finito, então satisfaz a propriedade de fronteira.

Demonstração: A demonstração deste teorema encontra-se em [CLD04]. □

Por causa de equações não-orientáveis (tipicamente AC), é preciso um critério mais refinado para obtenção da propriedade do variante finito. O lema abaixo dá uma condição suficiente para que uma decomposição satisfaça a propriedade de fronteira.

Lema 1 Se $(\mathcal{R}, E')$ é uma decomposição de E que satisfaz:

$$\forall f \in sig(E)\ \exists c_f\, \forall t_1, \ldots, t_n \in T(\mathcal{F}, V). f(t_1\downarrow, \ldots, t_n\downarrow) \stackrel{\leq c_f}{\longrightarrow}_{\mathcal{R}/E'} f(t_1, \ldots, t_n)\downarrow .$$

Então $(\mathcal{R}, E')$ satisfaz a propriedade de fronteira.

Demonstração: Seja t um termo e seja $c_{max} := max(\{c_f \mid f \in sig(E)\})$ tal que para todo $f \in sig(E)$ e para quaisquer $t_1, \ldots, t_n \in \mathcal{T}(\mathcal{F}, \mathcal{X})$ tem-se

$$f(t_1\downarrow, \ldots, t_n\downarrow) \stackrel{\leq c_{max}}{\longrightarrow}_{\mathcal{R}/E'} f(t_1, \ldots, t_n)\downarrow .$$

Note que um tal c_{max} existe desde que $sig(E)$ é finito. Seja θ uma substituição, será provado por indução na estrutura de t que $t(\theta\downarrow)$ pode ser reduzido para sua forma normal, usando no máximo $c_{\max} \times |t|$ passos de redução onde $|t|$ denota o tamanho de um termo t, isto é, a cardinalidade de $\mathcal{O}(t)$. Tem-se os seguintes casos:

1. Se t é uma variável, então $t(\theta\downarrow)$ já está na forma normal.

2. Se $t = f(t_1, \ldots, t_n)$, por hipótese de indução,

$$t_i(\theta\downarrow) \stackrel{\leq c_{max}\times|t_i|}{\longrightarrow}_{\mathcal{R}/E'} (t_i\theta)\downarrow, \quad 1 \leq i \leq n.$$

   Dessa forma,

   - Ou $f \in sig(E)$ e, por hipótese, $f((t_1\theta)\downarrow, \ldots, (t_n\theta)\downarrow) \stackrel{\leq c_{max}}{\longrightarrow}_{\mathcal{R}/E'} f(t_1\theta, \ldots, t_n\theta)\downarrow)$, o que permite concluir o resultado.
   - Ou $f \notin sig(E)$, e neste caso $f((t_1\theta)\downarrow, \ldots, (t_n\theta)\downarrow)$ já está na forma normal, e o resultado segue.

□

Capítulo 3

O Protocolo de Carteira Eletrônica

Neste capítulo será apresentado uma descrição do Protocolo de Carteira Eletrônica, bem como a teoria equacional usada para sua modelagem, ou seja, as propriedades algébricas que permitem que este protocolo seja executado. Esta teoria equacional será descrita com detalhes na Seção 1. Ela consiste do conjunto axiomas equacionais EP, que será dado pela união de três grupos Abelianos e algumas regras para exponenciação. Além disso, será introduzido um sistema $\mathcal{R}$ de regras de reescrita, AC-convergente, associado a esta teoria equacional. Com a finalidade de provar que a unificação módulo EP é decidível, será mostrado que a decomposição $(\mathcal{R}, AC)$ da teoria equacional EP satisfaz a propriedade do variante finito, propriedade que foi introduzida em [CLD04]. Em seguida, serão apresentadas definições, lemas técnicos e outros resultados relacionados a este sistema $\mathcal{R}$, que serão importantes para o próximo capítulo.

Na Seção 2, será apresentado o conjunto de regras de inferência $\mathcal{I}_{\mathsf{EP}}$ que representa a capacidade de dedução do intruso. O sistema de inferência $\mathcal{I}_{\mathsf{EP}}$, será uma extensão do modelo clássico de Dolev-Yao, introduzido em [DY81]. Esta extensão, caracterizada pela adição de algumas regras, é uma forma de considerar o caso onde o intruso pode usar raciocínio equacional módulo o conjunto EP de axiomas equacionais. Ainda nesta seção será apresentado o problema de segurança, o chamado *Problema da Dedução do Intruso.*

3.1 O protocolo de carteira eletrônica

O protocolo envolve três possíveis agentes: a carteira eletrônica EP, um servidor S e uma autoridade de confiança A.

A autoridade A não será considerada aqui, pois ela está envolvida apenas no caso de reivindicação de ambas as partes.

Denote por b e r dois inteiros positivos, que são públicos. A chave pública de EP é $b^s \bmod r$ onde s é sua chave privada.

Primeiro, existe uma fase durante a qual o servidor se autentica. Esta fase também não será considerada aqui, pois não faz uso de propriedades algébricas. Depois dessa fase, S e EP concordam em um **nonce** N_s para essa sessão. Então:

1. a carteira EP gera um **nonce** N, constrói uma mensagem M (que só é usada em caso de conflito, e cujo conteúdo não é relevante aqui) e envia para o servidor S: $\mathsf{hash}(b^N \bmod r, S, N_s, M, X)$, onde X é o valor pago;

2. o servidor S desafia EP enviando um **nonce** N_c;

3. a carteira EP responde com $N - s \times N_c, M, X$ e subtrai X da sua conta;

4. o servidor S checa que a mensagem recebida no passo 1 é consistente com a mensagem recebida no passo 3 e então aumenta sua conta com a quantidade X.

A parte importante e difícil aqui é o último passo: S deve ser capaz de completar essa verificação. Aqui estão as operações executadas por S neste estágio:

$$\begin{aligned} \mathsf{hash}((b^s)^{N_c} \times b^{N-s\times N_c} \mathsf{mod}\ r, S, N_s, M, X) &= \mathsf{hash}(b^{s\times N_c} \times b^N \times b^{-s\times N_c} \mathsf{mod}\ r, S, N_s, M, X) \\ &= \mathsf{hash}(b^N \mathsf{mod}\, r, S, N_s, M, X) \end{aligned}$$

O servidor S eleva $b^s \bmod r$ à potência N_c ($b^s \bmod r$ é público e N_c é conhecido), eleva $b \bmod r$ à potência $N - s \times N_c$ (que é a mensagem enviada no passo 3), e multiplica os dois resultados.

Note que as seguintes propriedades equacionais são usadas:

$$\mathsf{exp}(\mathsf{exp}(b, y), z) = \mathsf{exp}(b, y \times z) \qquad \mathsf{exp}(b, x) \times \mathsf{exp}(b, y) = \mathsf{exp}(b, y + z)$$

bem como as propriedades de grupo Abeliano de $\times$ e $+$.

O problema agora é que quando colocadas juntas as seguintes propriedades de exponenciação:

$$\begin{array}{rrcl} (1) & \mathsf{exp}(\mathsf{exp}(x, y), z) & = & \mathsf{exp}(x, y \times z) \\ (2) & \mathsf{exp}(x, y) \times \mathsf{exp}(x, z) & = & \mathsf{exp}(x, y + z) \end{array}$$

A distributividade da exponenciação sobre a multiplicação pode ser derivada:

$$\begin{array}{rcl} \mathsf{exp}(\mathsf{exp}(x, y_1) \times \mathsf{exp}(x, y_2), z) & =_2 & \mathsf{exp}(\mathsf{exp}(x, y_1 + y_2), z) \\ & =_1 & \mathsf{exp}(x, (y_1 + y_2) \times z) \\ & = & \mathsf{exp}(x, y_1 \times z + y_2 \times z) \\ & =_2 & \mathsf{exp}(x, y_1 \times z) \times \mathsf{exp}(x, y_2 \times z) \\ & =_1 & \mathsf{exp}(\mathsf{exp}(x, y_1), z) \times \mathsf{exp}(\mathsf{exp}(x, y_2), z) \end{array}$$

E neste caso, a teoria equacional (consequentemente a segurança) torna-se indecidível, como foi mostrado por Kapur em [KNW03].

Para contornar este problema será introduzido um símbolo de função unária h, dado por:

$$h(x) = \mathsf{exp}(b, x).$$

Além disso, serão usados dois símbolos de multiplicação distintos $\bullet$ e $\star$, para auxiliar na combinação dos resultados, como foi proposto em [ACD07].

Dessa forma, o teoria equacional EP utilizada na modelagem do protocolo, é composta pelos seguintes axiomas equacionais:

$$\begin{array}{rrcl} \mathsf{AG}(+, J_+, e_+) & h(x) \bullet h(y) & = & h(x+y) \\ \mathsf{AG}(\star, J_\star, e_\star) & \mathsf{exp}(h(x), y) & = & h(x \star y) \\ \mathsf{AG}(\bullet, J_\bullet, e_\bullet) & \mathsf{exp}(\mathsf{exp}(x, y), z) & = & \mathsf{exp}(x, y \star z) \end{array}$$

Onde $\mathsf{AG}(\circ, J_\circ, e_\circ)$ representa os axiomas de grupos Abelianos para o símbolo de função binário $\circ \in \{\bullet, +, \star\}$, dados por:

$$\mathsf{AG}(\circ, J_\circ, e_\circ) : \left\{ \begin{array}{rclrcl} x \circ (y \circ z) & = & (x \circ y) \circ z & x \circ y & = & y \circ x \\ x \circ e_\circ & = & x & x \circ J_\circ(x) & = & e_\circ \end{array} \right.$$

Estes axiomas equacionais são suficientes para a verificação do último passo do protocolo.

O próximo passo é mostrar que a teoria equacional EP pode ser representada por um sistema de reescrita finito $\mathcal{R}$, AC-convergente (i.e, convergente módulo associatividade e comutatividade), que possui propriedades mais fortes.

Para construção desse sistema de reescrita considere a assinatura finita $\mathcal{F}$ dada por:

$$\mathcal{F} = \{+,\ e_+,\ J_+,\ \star,\ e_\star,\ J_\star, \bullet,\ e_\bullet, J_\bullet, h, \mathsf{exp}\} \cup \mathcal{F}_0$$

onde $\mathcal{F}_0$ é um conjunto finito de símbolos de constantes, $\{+, \star, \bullet\}$ são símbolos associativos e comutativos, exp é um símbolo de função binário , h, $J_\star$, J_+, $J_\bullet$ são símbolos de função unários e $\{e_+, e_\star, e_\bullet\}$ são elementos neutros de $\{+, \star, \bullet\}$, respectivamente.

Para cada $\circ \in \{+, \star, \bullet\}$, $\mathcal{R}_{\mathsf{AG}(\circ)}$ é o sistema de reescrita módulo AC para $\circ$:

$$\begin{array}{rcl@{\qquad}rcl} x \circ e_\circ & \to & x & x \circ J_\circ(x) & \to & e_\circ \\ J_\circ(x) \circ J_\circ(y) & \to & J_\circ(x \circ y) & J_\circ(e_\circ) & \to & e_\circ \\ J_\circ(J_\circ(x)) & \to & x & J_\circ(x) \circ x \circ y & \to & y \\ J_\circ(x) \circ J_\circ(y) \circ z & \to & J_\circ(x \circ y) \circ z & J_\circ(x \circ y) \circ x & \to & J_\circ(y) \\ J_\circ(x \circ y) \circ x \circ z & \to & J_\circ(y) \circ z & J_\circ(J_\circ(x) \circ y) & \to & x \circ J_\circ(y) \end{array}$$

Considere também, as seguintes regras de reescrita:

$$\mathcal{R}_0 = \left\{ \begin{array}{rcl@{\qquad}rcl} \mathsf{exp}(h(x), y) & \to & h(x \star y) & J_\bullet(h(x)) & \to & h(J_+(x)) \\ \mathsf{exp}(\mathsf{exp}(x, y), z) & \to & \mathsf{exp}(x, y \star z) & h(e_+) & \to & e_\bullet \\ h(x) \bullet h(y) & \to & h(x + y) & J_\bullet(h(x) \bullet y) & \to & h(J_+(x)) \bullet J_\bullet(y) \\ h(x) \bullet h(y) \bullet z & \to & h(x + y) \bullet z & \mathsf{exp}(e_\bullet, x) & \to & h(e_+ \star x) \end{array} \right.$$

A orientação não usual para inversos, proposta inicialmente por Lankford, que pode ser encontrado em [Geh94], garantirá a propriedade do variante finito para o par (EP, AC).

O sistema de reescrita $\mathcal{R} = \mathcal{R}_{\mathsf{AG}(\star)} \cup \mathcal{R}_{\mathsf{AG}(\bullet)} \cup \mathcal{R}_{\mathsf{AG}(+)} \cup \mathcal{R}_0$ consiste de 38 regras de reescrita e o seguinte resultado foi verificado mecanicamente usando CiME [CM96].

Lema 2 $\mathcal{R}$ é convergente módulo associatividade e comutatividade.

Para a prova da convergência do sistema de reescrita $\mathcal{R}$, foi necessária também a adição das chamadas *regras de extensão*, que podem ser definidas da seguinte forma:

Definição 21 (Regras de Extensão) Considere as seguintes regras

1. $x \circ J_\circ(x) \longrightarrow e_\circ$
2. $J_\circ(x) \circ J_\circ(y) \longrightarrow J_\circ(x \circ y)$
3. $J_\circ(x \circ y) \circ x \longrightarrow J_\circ(y)$
4. $h(x) \bullet h(y) \longrightarrow h(x + y)$

As suas respectivas *regras de extensão*, são:

1' $x \circ J_\circ(x) \circ z \longrightarrow z$

2' $J_\circ(x) \circ J_\circ(y) \circ z \longrightarrow J_\circ(x \circ y) \circ z$

3' $J_\circ(x \circ y) \circ x \circ z \longrightarrow J_\circ(y) \circ z$

4' $h(x) \bullet h(y) \bullet z \longrightarrow h(x + y) \bullet z$

onde a variável z adicionada é chamada *variável de extensão.*

O seguinte lema, inicialmente enunciado em [BCLD07a] e que será provado aqui, mostra que $\mathcal{R}$ não é apenas convergente, mas também:

Lema 3 $(\mathcal{R}, AC)$ é uma decomposição da teoria equacional EP que tem a propriedade do variante finito.

Demonstração: Sejam t_1 e t_2 termos na forma normal (w.r.t $(\mathcal{R}/AC)$) e $\circ \in \{\star, \bullet, +\}$, então $J_\circ(t_1), t_1 \circ t_2, \mathsf{exp}(t_1, t_2)$ e $h(t_1)$, podem ser reduzidos para sua forma normal, usando no máximo 4 passos de redução. Uma prova para esta afirmação encontra-se em [CLD04]. Logo $(\mathcal{R}, AC)$ é uma decomposição de EP que satisfaz:

$$\forall f \in sig(\mathsf{EP})\ \exists c_f\ \forall t_1, \ldots, t_n \in T(\mathcal{F}, V).f(t_1\downarrow, \ldots, t_n\downarrow) \stackrel{\leq c_f}{\rightarrow}_{\mathcal{R}/AC} f(t_1, \ldots, t_n)\downarrow$$

Então, pelo Lema 1, $(\mathcal{R}, AC)$ satisfaz a propriedade de fronteira. Segue do Teorema 1 que esta decomposição de EP tem a propriedade do variante finito. □

O interesse por esta propriedade é o seguinte: devido ao fato da unificação ser decidível para a teoria AC, ela garante que a unificação é também decidível para EP.

A seguir serão definidos alguns conceitos técnicos fundamentais para a prova de resultados posteriores.

Definição 22 Para $\circ \in \{\star, +, \bullet\}$, defina por $\mathsf{inv}_\circ(u)$ o termo $J_\circ(u)\downarrow$.

Por exemplo, o $\mathsf{inv}_\bullet(h(J_+)(a)) = J_\bullet(h(J_+(a)))\downarrow = h(J_+(J_+(a)))\downarrow = h(a)$.

Definição 23 Denote por $top(t)$ o símbolo raíz do termo t. TOP(u) é definido por TOP$(J_\circ(v \circ w)) = \circ$, TOP$(h(w + v)) = \bullet$, TOP$(h(J_+(u + v))) = \bullet$ e TOP$(u) = top(u)$ nos outros casos.

Por exemplo, TOP$(h(a + b)) = \bullet$, TOP$(h(a)) = h$, e TOP$(J_+(a + b)) = +$.

Observação 3 Segue da Definição 23, que para todo termo v, TOP$(h(v)) = \bullet$ ou TOP$(h(v)) = h$. De fato, TOP$(h(v)) = \bullet$, apenas quando TOP$(v) = +$. Nos casos onde TOP$(v) \neq +$, segue que TOP$(h(v)) = $ top$(h(v)) = h$.

Seja $\mathrm{DS}_\circ(t)$ o conjunto dos *subtermos de decomposição* de um termo t.

Definição 24 Seja $\circ \in \{\star, +, \bullet\}$, o conjunto $\mathrm{DS}_\circ(u)$ é definido por*:*

- $\mathrm{DS}_\circ(u \circ v) = \mathrm{DS}_\circ(u) \cup \mathrm{DS}_\circ(v)$,
- $\mathrm{DS}_\circ(J_\circ(u)) = \{J_\circ(v) | v \in \mathrm{DS}_\circ(u)\}$,
- $\mathrm{DS}_\bullet(h(u)) = \{h(v) | v \in \mathrm{DS}_+(u)\}$,
- $\mathrm{DS}_\circ(u) = \{u\}\ se \mathrm{TOP}(u) \neq \circ$.

Em particular, note que $\mathrm{DS}_\bullet(h(J_+(a+b))) = \{h(J_+(a)), h(J_+(b))\}$.

Definição 25 (subtermos) Seja t um termo na forma normal, $Sub(t)$ é o menor conjunto de termos tais que $t \in Sub(t)$ e se $u \in Sub(t)$ então
- *ou* $\circ = \mathrm{TOP}(u) \in \{\star, \bullet, +\}$ *e* $\mathrm{DS}_\circ(u) \subset Sub(t)$
- *ou então* $u = f(u_1, \ldots, u_n)$ *e* $u_1, \ldots, u_n \in Sub(t)$.

Mais ainda, dado um conjunto T de termos na forma normal, o conjunto dos subtermos de T é dado por: $\mathrm{Sub}(T) = \bigcup_{t \in T} \mathrm{Sub}(t)$.

O seguinte lema mostra que para um conjunto finito $t, t_1, t_2, \ldots, t_n (n \geq 1)$ de termos na forma normal operados com um símbolo associativo-comutativo $\circ \in \{\star, \bullet, +\}$ é possível estabelecer um criério para encontrar o termo $\mathsf{inv}_\circ(t)$. Este lema será usado posteriormente como ferramenta para mostrar que o conjunto de regras de inferência que representa as habilidades do intruso tem uma propriedade chamada *localidade*, esta propriedade bem como o conjunto de regras de inferência serão definidos no último capítulo.

Para a prova deste lema, serão utilizadas as *regras de extensão* para aplicação das regras apenas na posição raiz de um termo. Esta redução via reescrita pode ser ilustrada da seguinte forma:

Exemplo. Considere os termos $t_1 = J_+(z), t_2 = h(a+b), t_3 = z + J_\bullet(w)$.

Observe que o termo $t = t_1 + t_2 + t_3 = J_+(z) + h(a+b) + z + J_\bullet(w)$ não está na forma normal, pois a regra $J_+(x) + x \to e_+$ pode ser utilizada.

Para isto, basta comutar e associar (quantas vezes forem necessárias) os subtermos do termo t até que termo $t = (J_+(z)+z)+(h(a+b)+J_\bullet(w))$ seja obtido. Então, a regra pode ser aplicada no subtermo $t|_1 = J_+(z) + z$, cuja posição é 1.

Note que a regra $J_+(x) + x + y \to y$ também poderia ter sido utilizada.

Basta considerar a substituição σ dada por:

$$\sigma = \{x \mapsto z, y \mapsto h(a + b) + J_\bullet(w)\}$$

e a regra seria aplicada na posição raiz do termo $t = (J_+(z) + z) + (h(a + b) + J_\bullet(w))$. Observe ainda que a *variável de extensão* z foi utilizada para "acumular"os subtermos que anteriormente não faziam parte da redução.

Lema 4 Sejam $t, t_1, t_2, \ldots, t_n$ termos em forma normal, $n \geq 1$, $\circ \in \{\star, \bullet, +\}$, $\mathrm{TOP}(t) \notin \{\circ, e_\circ\}$ e assuma que $\mathrm{TOP}((t \circ t_1 \circ \ldots \circ t_n)\downarrow) \neq \circ$ e $(t_1 \circ \ldots \circ t_n)\downarrow \neq e_\circ$. Então, existe um índice i tal que $\mathsf{inv}_\circ(t) \in \mathrm{DS}_\circ(t_i)$.

Demonstração: Pelo Lema 2, o sistema de reescrita $\mathcal{R}$ é AC-convergente. Então pode-se escolher uma estratégia para reduzir $t \circ t_1 \circ \ldots \circ t_n$ para a sua forma normal.

Dado um termo u possíveis redexes $l\sigma(\to r\sigma)$ em u podem ser ordenados de acordo com a seguinte ordem de prioridade:

1. Regras de extensão;
2. As regras restantes;
3. $l = h(x) \bullet h(y) \bullet z$ e $h(x)\sigma \neq t,\ h(y)\sigma \neq t$;
4. $l = h(x) \bullet h(y) \bullet z$ e $h(x)\sigma = t$ (ou $h(y)\sigma = t$);
5. $l = J_\circ(x) \circ J_\circ(y) \circ z$ e $J_\circ(x)\sigma = t$ (ou $J_\circ(y)\sigma = t$, t dado pelo Lema).

Observe que redexes são constraídos respeitando a ordem de prioridade maximal. Isto significa que os dois últimos casos são aplicados somente quando as outras instâncias de lados esquerdos de regras não são um redex em u.

O resultado será provado por indução no tamanho m da maior sequência de redução do termo $t \circ t_1 \ldots \circ t_n$ para sua forma normal.

Para o caso base, basta notar que $m = 0$ não acontece.

De fato, se $m = 0$ então $(t \circ t_1 \circ \ldots \circ t_n) = (t \circ t_1 \circ \ldots \circ t_n)\downarrow$ e, portanto

$$\mathrm{TOP}((t \circ t_1 \circ \ldots \circ t_n)\downarrow) = \circ,$$

pois $t, t_1, \ldots, t_n$ são termos na forma normal, e isto contradiz a hipótese do lema.

Para o passo indutivo serão analisadas as possíveis regras aplicadas no primeiro passo de redução do termo $t \circ t_1 \ldots \circ t_n$, para sua forma normal.

Primeiramente, é preciso observar que a ordem de prioridade estabelecida inicialmente permite a aplicação das regras apenas na posição raiz do termo $t \circ t_1 \ldots \circ t_n$. De fato, sempre que existirem instâncias de regras em posições distintas da raiz, é possível reordenar os termos (associar e comutar) de forma que os termos $t_i's$ que não participam da reescrita fiquem acumulados na variável de extensão. Dessa forma, basta aplicar a regra de extensão adequada na posição raiz do termo obtido, como foi mostrado no exemplo acima.

Serão analisados 7 casos onde $\circ \neq \bullet$ e outros 2 casos adicionais com $\circ = \bullet$.

Caso 1: A regra é $x \circ e_\circ \to x$.

O primeiro passo de redução pode ser representado por:

$$(t \circ t_1 \circ \ldots \circ t_n)|_\varepsilon = (t \circ t_1 \circ \ldots \circ t_n) = (x \circ e_\circ)\sigma$$

para alguma substituição σ.

Como, por hipótese, $t, t_1, \ldots$ e t_n estão na forma normal e $t \neq e_\circ$, existe j tal que $t_j = e_\circ$.

Observe que não existe índice i, para o qual $t_i = e_\circ \circ u$, pois contradiz a hipótese de t_i ser uma forma normal.

Então,

$$x\sigma = t \circ t_1 \circ \ldots t_{j-1} \circ t_{j+1} \circ \ldots \circ t_n.$$

Além disso, n deve ser pelo menos 2, já que $(t_1 \circ t_2 \circ \ldots \circ t_n)\downarrow \neq e_\circ$.

Assim,

$$(t \circ t_1 \circ \ldots \circ t_n) \to (t \circ t_1 \circ \ldots t_{j-1} \circ t_{j+1} \circ \ldots \circ t_n) \overset{\leq m}{\to} (t \circ t_1 \circ \ldots \circ t_n)\downarrow .$$

Observe que os termos $t, t_1, \ldots, t_{j-1}, t_{j+1}, \ldots, t_n$ satisfazem as hipóteses do lema, pois estão na forma normal,

$$\mathrm{TOP}((t \circ t_1 \circ \ldots \circ t_{j-1} \circ t_{j+1} \circ \ldots t_n)\downarrow) = \mathrm{TOP}((t \circ t_1 \circ \ldots \circ t_{j-1} \circ e_\circ \circ t_{j+1} \circ \ldots t_n)\downarrow) \neq \circ$$

e $(t \circ t_1 \circ \ldots \circ t_{j-1} \circ t_{j+1} \circ \ldots t_n)\downarrow = (t \circ t_1 \circ \ldots \circ t_{j-1} \circ e_\circ \circ t_{j+1} \circ \ldots t_n)\downarrow \neq e_\circ$.

Por hipótese de indução, existe um índice i (distinto de j) tal que $\mathsf{inv}_\circ(t) \in \mathrm{DS}_\circ(t_i)$

Caso 2: A regra é $x \circ J_\circ(x) \to e_\circ$.

O primeiro passo de redução pode ser representado por:

$$t \circ t_1 \circ \ldots \circ t_n = (x \circ J_\circ(x))\sigma = (x\sigma) \circ J_\circ(x\sigma),$$

para alguma substituição σ.

Dessa forma, ou $t = J_\circ(x\sigma)$ ou existe um índice i tal que $t_i = J_\circ(x\sigma)$.

- $t = J_\circ(x\sigma)$, então $t_1 \circ \ldots \circ t_n = x\sigma$.

  Como $\mathrm{TOP}(J_\circ(x\sigma)) = \mathrm{TOP}(t) \neq \circ$ segue que $\mathrm{TOP}(x\sigma) = \mathrm{TOP}(t_1 \circ \ldots \circ t_n) \neq \circ$.

  Note que $x\sigma$ é uma forma normal, caso contrário, $t = J_\circ(x\sigma)$ não estaria na forma normal, contradizendo a hipótese do lema. Assim $x\sigma = (t_1 \circ \ldots \circ t_n) = (t_1 \circ \ldots \circ t_n)\downarrow$. Como cada t_i, $1 \leq i \leq n$ está na forma normal, segue que $n = 1$.

  Observe que

  $$\mathsf{inv}_\circ(t) = J_\circ(t)\downarrow = J_\circ(J_\circ(x\sigma)) = x\sigma = t_1$$

  Além disso,

  $$\mathrm{DS}_\circ(t_1) = \{t_1\}, \text{ pois } \mathrm{TOP}(t_1) = \mathrm{TOP}(x\sigma) \neq \circ.$$

  Portanto, $\mathsf{inv}_\circ(t) \in \mathrm{DS}_\circ(t_1)$.

- Agora, suponha que existe um índice i tal que $t_i = J_\circ(x\sigma)$. Então $x\sigma = t \circ u$ e $u = t_1 \circ \ldots \circ t_{i-1} \circ t_{i+1} \circ \ldots \circ t_n$. Logo, $t_i = J_\circ(t \circ u)$.

Observe que

$$\begin{aligned}
\mathrm{DS}_\circ(t_i) &= \mathrm{DS}_\circ(J_\circ(t \circ u)) \\
&= \{J_\circ(v) \,|\, v \in \mathrm{DS}_\circ(t \circ u)\} \\
&= \{J_\circ(v) \,|\, v \in \mathrm{DS}_\circ(t) \cup \mathrm{DS}_\circ(u)\} \\
&= \{J_\circ(v) \,|\, v \in \mathrm{DS}_\circ(t)\} \cup \{J_\circ(v') | v' \in \mathrm{DS}_\circ(u)\} \\
&= \{J_\circ(t)\} \cup \mathrm{DS}_\circ(J_\circ(u)), \text{ pois } \mathrm{TOP}(t) \neq \circ.
\end{aligned}$$

Assim, $J_\circ(t) \in \mathrm{DS}_\circ(t_i)$, para algum i.

Afirmação: $J_\circ(t) = J_\circ(t) \downarrow = \mathsf{inv}_\circ(t)$.

Suponha, por contradição, que $J_\circ(t)$ não está na forma normal, então existem instâncias de lados esquerdos de regras no termo $J_\circ(t)$. Como por hipótese, t é uma forma normal. Apenas as regras

$$J_\circ(J_\circ(y)) \longrightarrow y \qquad\qquad J_\circ(e_\circ) \longrightarrow e_\circ$$

podem ser utilizadas.

A segunda regra não pode ser aplicada pois $t \neq e_\circ$, por hipótese. Agora, se $t = J_\circ(w)$ para algum termo w, então $x\sigma = J_\circ(w) \circ u$.

Assim, $t_i = J_\circ(x\sigma) = J_\circ(J_\circ(w) \circ u)$, contradizendo o fato de t_i ser um termo na forma normal. Logo, $J_\circ(t)$ é uma forma normal.

Logo, $J_\circ(t) = \mathsf{inv}_\circ(t)$.

Portanto, existe um índice i tal que $\mathsf{inv}_\circ(t) \in \mathrm{DS}_\circ(t_i)$.

Caso 3 $J_\circ(x) \circ x \circ y \to y$.

O primeiro passo de redução pode ser representado por:

$$(t \circ t_1 \circ \ldots \circ t_n)|_\varepsilon = t \circ t_1 \circ \ldots \circ t_n = J_\circ(x\sigma) \circ (x\sigma) \circ (y\sigma),$$

para alguma substituição σ.

Dessa forma, ou $t = J_\circ(x\sigma)$ ou existe um índice i tal que $t_i = J_\circ(x\sigma) \circ t_i'$.

- Quando $t = J_\circ(x\sigma)$ existe um índice i tal que $t_i = x\sigma \circ t'_i$ (com t'_i possivelmente vazio), pois a hipótese $\mathrm{TOP}(t) = J_\circ(x\sigma) \neq \circ$ implica em $\mathrm{TOP}(x\sigma) \neq \circ$.

  Observe que

$$\begin{aligned} \mathrm{DS}_\circ(t_i) &= \mathrm{DS}_\circ(x\sigma \circ t'_i) \\ &= \mathrm{DS}_\circ(x\sigma) \cup \mathrm{DS}_\circ(t'_i) \\ &= \{x\sigma\} \cup \mathrm{DS}_\circ(t_i). \end{aligned}$$

  A última igualdade segue de $\mathrm{TOP}(x\sigma) \neq \circ$. Mais ainda, $\mathsf{inv}_\circ(t) = J_\circ(t) \downarrow = (x\sigma)$.

  Logo, existe um índice i tal que $\mathsf{inv}_\circ(t) \in \mathrm{DS}_\circ(t_i)$.

- Agora, quando existe um índice i tal que $t_i = J_\circ(x\sigma) \circ t'_i$, ou $x\sigma = t \circ u$ ou $y\sigma = t \circ t'_1 \circ \ldots \circ t'_k$ e, para cada k, t'_k está na forma normal.

  (i) No primeiro caso,

$$\begin{aligned} \mathrm{DS}_\circ(t_i) &= \mathrm{DS}_\circ(J_\circ(t \circ u) \circ t'_i) \\ &= \mathrm{DS}_\circ(J_\circ(t \circ u)) \cup \mathrm{DS}_\circ(t'_i) \\ &= \{J_\circ(v) \mid v \in \mathrm{DS}_\circ(t) \cup \mathrm{DS}_\circ(u)\} \cup \mathrm{DS}_\circ(t'_i) \\ &= \{J_\circ(t)\} \cup \mathrm{DS}_\circ(u) \cup \mathrm{DS}_\circ(t'_i) \end{aligned}$$

  A última igualdade vem da hipótese $\mathrm{TOP}(t) \neq \circ$. Pela afirmação feita no Caso 2, $\mathsf{inv}_\circ(t) = J_\circ(t)$.

  Portanto, existe um índice i tal que $\mathsf{inv}_\circ(t) \in \mathrm{DS}_\circ(t_i)$.

  (ii) Para o segundo caso, existe j tal que $t_j = x\sigma \circ t'_j$ e $y\sigma = t \circ t'_1 \circ \ldots \circ t'_k$ tal que t'_k é uma forma normal, para cada índice k .

  Considere a aplicação injetora $\pi : \{1, \ldots, k\} \to \{1, \ldots, n\}$ dada por $t_{\pi(j)} = t'_j \circ u_j$.

  Observe que

$$\begin{aligned} e_\circ \neq (t_1 \circ \ldots \circ t_n) \downarrow &= (t_1 \circ \ldots J_\circ(x\sigma) \circ t'_i \circ \ldots \circ x\sigma \circ t'_j \circ \ldots t_n) \downarrow \\ &= (J_\circ(x\sigma) \circ x\sigma \circ t'_1 \circ \ldots \circ t'_k) \downarrow \\ &= (t'_1 \circ \ldots \circ t'_k) \downarrow \end{aligned}$$

Mais ainda

$$\begin{aligned}\mathrm{TOP}((t \circ t'_1 \circ \ldots \circ t'_k)\downarrow) &= \mathrm{TOP}((t \circ (t'_1 \circ \ldots \circ t'_k)\downarrow))\downarrow \\ &= \mathrm{TOP}((t \circ (t_1 \circ \ldots \circ t_k)\downarrow)\downarrow) \\ &= \mathrm{TOP}((t \circ t_1 \circ \ldots \circ t_k)\downarrow) \neq \circ.\end{aligned}$$

Portanto, $t, t'_1, \ldots, t'_k$ satisfazem as hipóteses do lema.

Logo, por hipótese de indução, existe um índice j tal que $\mathsf{inv}_\circ(t) \in \mathrm{DS}_\circ(t'_j)$. Mas, pela construção de π existe um índice i tal que $i = \pi(j)$. Assim,

$$t_i = t_{\pi(j)} = t'_j \circ u_j.$$

Como $\mathrm{DS}_\circ(t_i) = \mathrm{DS}_\circ(t'_j) \cup \mathrm{DS}_\circ(u_j)$, segue que $\mathsf{inv}_\circ(t) \in \mathrm{DS}_\circ(t_i)$.

Caso 4: A regra é $J_\circ(x) \circ J_\circ(y) \to J_\circ(x \circ y)$.

O primeiro passo de redução pode ser representado por:

$$t \circ t_1 \circ \ldots \circ t_n = J_\circ(x\sigma) \circ J_\circ(y\sigma),$$

para alguma substituição σ.

Assim, $t = J_\circ(x\sigma)$ e $t_1 \circ \ldots \circ t_n = J_\circ(y\sigma)$.

Afirmação: $t_1 \circ \ldots \circ t_n = J_\circ(y\sigma)$ só acontece para $n = 1$.

Se $n > 1$, como $J_\circ$ é um símbolo de função unário e $\circ$ é símbolo de função binário, seria preciso reduzir $t_1 \circ \ldots \circ t_n$ primeiramente. Mas isto contradiz o fato que a regra $J_\circ(x) \circ J_\circ(y)$ é aplicada no primeiro passo de redução. Assim, $t = J_\circ(x\sigma)$ e $t_1 = J_\circ(y\sigma)$.

Além disso, o termo $J_\circ(x\sigma \circ y\sigma)$ já está na forma normal. De fato, suponha que uma regra $l \to r$ possa ser aplicada em $J_\circ(x\sigma \circ y\sigma)$. Então existe uma posição $p' \in \mathcal{O}(J_\circ(x\sigma \circ y\sigma))$ e uma substituição γ tal que

$$J_\circ(x\sigma \circ y\sigma)|_{p'} = l\gamma.$$

A posição é $p' = \varepsilon$. As únicas regras que podem ser aplicadas são

$$\begin{aligned}J_\circ(e_\circ) &\to e_\circ \\ J_\circ(J_\circ(x')) &\to x' \\ J_\circ(J_\circ(x') \circ y') &\to x' \circ J_\circ(y')\end{aligned}$$

i) Suponha que a regra $J_\circ(e_\circ) \to e_\circ$ possa ser aplicada.

Dessa forma, $J_\circ(x\sigma \circ y\sigma) = J_\circ(e_\circ)$ o que implica em $x\sigma = y\sigma = e_\circ$ ou $x\sigma = J_\circ(y\sigma)$. Para $x\sigma = e_\circ$, $t = J_\circ(x\sigma) = J_\circ(e_\circ) = e_\circ$, o que é uma contradição. Agora, quando $x\sigma = J_\circ(y\sigma)$ tem-se que $t = J_\circ(x\sigma) = J_\circ(J_\circ(y\sigma))$ o que implica que t não está na forma normal, outra contradição.

ii) Suponha que a regra $J_\circ(J_\circ(x')) \to x'$ possa ser aplicada.

Dessa forma, $J_\circ(x\sigma \circ y\sigma) = J_\circ(J_\circ(x'\gamma))$, para alguma substituição γ, e então $x\sigma \circ y\sigma = J_\circ(x'\sigma)$, mas $\circ$ é símbolo binário e $J_\circ$ é símbolo unário, uma contradição.

iii) Suponha agora, que a regra $J_\circ(J_\circ(x') \circ y') \to x' \circ J_\circ(y')$ possa ser aplicada.

Então, $J_\circ(x\sigma \circ y\sigma) = J_\circ(J_\circ(x'\gamma) \circ y'\gamma)$, para alguma substituição γ. Dessa forma, $x\sigma \circ y\sigma = J_\circ(x'\gamma) \circ y\sigma$ e isto contradiz o fato de $J_\circ(x\sigma)$ e $J_\circ(y\sigma)$ estarem na forma normal.

Falta analisar se é possível aplicar alguma regra em uma posição $p' \neq \varepsilon$.

Como $x\sigma$ e $y\sigma$ são formas normais, resta apenas analisar se é possível aplicar uma regra na posição raíz do termo $(x\sigma \circ y\sigma)$.

As regras são

$$\begin{aligned} x' \circ e_\circ &\to x' \\ x' \circ J_\circ(x') &\to e_\circ \\ J_\circ(x' \circ y') \circ x' &\to J_\circ(y') \\ J_\circ(x') \circ J_\circ(y') &\to J_\circ(x' \circ y') \end{aligned}$$

em todos os casos, ou $J_\circ(x\sigma)$ ou $J_\circ(y\sigma)$ não estão na forma normal.

Assim $J_\circ(x\sigma \circ y\sigma)$ está na forma normal, o que implica que $(t \circ t_1 \circ \ldots \circ t_n)\downarrow = J_\circ(x\sigma \circ y\sigma)$. Portanto, $\mathrm{TOP}((t \circ t_1 \circ \ldots \circ t_n)\downarrow) = \circ$, o que contradiz a hipótese do lema. Logo este caso não pode acontecer.

Caso 5: A regra é $J_\circ(x) \circ J_\circ(y) \circ z \to J_\circ(x \circ y) \circ z$.

O primeiro passo de redução pode ser representado por:

$$t \circ t_1 \circ \ldots \circ t_n = J_\circ(x\sigma) \circ J_\circ(y\sigma) \circ (z\sigma),$$

para alguma substituição σ.

Se $t = J_\circ(x)\sigma$ (ou $t = J_\circ(y)\sigma$), pela ordem de prioridade adotada, nenhuma outra regra pode ser aplicada, então $J_\circ(y\sigma) \circ z\sigma$ está na forma normal, donde segue que $J_\circ(y\sigma)$ e $z\sigma$ também são formas normais.

Assim

$$(t \circ t_1 \ldots \circ t_n)\downarrow = (J_\circ(x\sigma) \circ J_\circ(y\sigma) \circ z\sigma)\downarrow = (J_\circ(x\sigma \circ y\sigma) \circ z\sigma) \text{ e } \mathrm{TOP}((t \circ t_1 \circ \ldots \circ t_n)\downarrow) = \circ,$$

o que contradiz a hipótese do lema. Logo este caso não pode acontecer.

Agora, suponha que $J_\circ(x \circ y)\sigma$ está na forma normal e $z\sigma = t \circ t'_1 \circ \ldots \circ t'_k$, onde $t'_1, \ldots, t'_k$ são formas normais.

Por hipótese, $(J_\circ(x\sigma \circ y\sigma) \circ t'_1 \circ \ldots \circ t'_k)\downarrow = (t_1 \circ \ldots \circ t_n)\downarrow \neq e_\circ$. Da mesma forma, $\mathrm{TOP}((J_\circ(x\sigma \circ y\sigma) \circ z\sigma)\downarrow) = \mathrm{TOP}((t \circ t_1 \circ \ldots \circ t_n)\downarrow) \neq \circ$.

Aplicando a hipótese de indução, $\mathsf{inv}_\circ(t) \in \mathrm{DS}_\circ(J_\circ(x\sigma \circ y\sigma))$ ou existe um índice j tal que $\mathsf{inv}_\circ(t) \in \mathrm{DS}_\circ(t'_j)$.

No primeiro caso,

$$\mathsf{inv}_\circ(t) \in \mathrm{DS}_\circ(J_\circ(x\sigma \circ y\sigma)) = \mathrm{DS}_\circ(J_\circ(x\sigma)) \cup \mathrm{DS}_\circ(J_\circ(y\sigma)).$$

Logo, existem índices i e j tais que $t_i = J_\circ(x\sigma) \circ u$ e $t_j = J_\circ(y\sigma) \circ v$, com u e v possivelmente vazios.

Portanto,$\mathsf{inv}_\circ(t) \in \mathrm{DS}_\circ(t_i) \cup \mathrm{DS}_\circ(t_j)$.

No segundo caso, como no Caso 3, existe um índice $i = \pi(j)$ tal que $t_i = t'_j \circ u$ e

$$\mathsf{inv}_\circ(t) \in \mathrm{DS}_\circ(t_i) = \mathrm{DS}_\circ(t'_j \circ u) = \mathrm{DS}_\circ(t'_j) \cup \mathrm{DS}_\circ(u).$$

Em todos os casos, existe um índice i tal que $\mathsf{inv}_\circ(t) \in \mathrm{DS}_\circ(t_i)$.

Caso 6: A regra é $J_\circ(x \circ y) \circ x \to J_\circ(y)$.

O primeiro passo de redução pode ser representado por:

$$t \circ t_1 \circ \ldots \circ t_n = J_\circ(x \circ y)\sigma \circ x\sigma,$$

para alguma substituição σ.

Observe que $t = J_\circ(x\sigma \circ y\sigma)$ não acontece. De fato, $\mathrm{TOP}(J_\circ(x\sigma \circ y\sigma)) = \circ$ já que $J_\circ(x\sigma \circ y\sigma)$ é uma forma normal. Mas, por hipótese, $\mathrm{TOP}(t) \neq \circ$.

Logo, existe um índice i tal que $t_i = J_\circ(x\sigma \circ y\sigma) \circ v$ e $x\sigma = t \circ u$, com u e v possivelmente vazios.

Assim,

$$\begin{aligned}
\mathrm{DS}_\circ(t_i) &= \mathrm{DS}_\circ(J_\circ(x\sigma \circ y\sigma)) \cup \mathrm{DS}_\circ(v) \\
&= \{J_\circ(v) | v \in \mathrm{DS}_\circ(x\sigma \circ y\sigma)\} \cup \mathrm{DS}_\circ(v) \\
&= \{J_\circ(v) | v \in \mathrm{DS}_\circ(x\sigma) \cup \mathrm{DS}_\circ(y\sigma)\} \cup \mathrm{DS}_\circ(v) \\
&= \mathrm{DS}_\circ(J_\circ(x\sigma)) \cup \mathrm{DS}_\circ(J_\circ(y\sigma)) \cup \mathrm{DS}_\circ(v) \\
&= \mathrm{DS}_\circ(J_\circ(t \circ u)) \cup \mathrm{DS}_\circ(J_\circ(y\sigma)) \cup \mathrm{DS}_\circ(v) \\
&= \mathrm{DS}_\circ(J_\circ(t)) \cup \mathrm{DS}_\circ(J_\circ(u)) \cup \mathrm{DS}_\circ(J_\circ(y\sigma)) \cup \mathrm{DS}_\circ(v) \\
&= J_\circ(t) \cup \mathrm{DS}_\circ(J_\circ(u)) \cup \mathrm{DS}_\circ(J_\circ(y\sigma)) \cup \mathrm{DS}_\circ(v)
\end{aligned}$$

a última igualdade vem de $\mathrm{TOP}(t) \neq \circ$. Pela afirmação feita no Caso 2, $J_\circ(t) = \mathsf{inv}_\circ(t)$.

Logo, existe um índice i tal que $\mathsf{inv}_\circ(t) \in \mathrm{DS}_\circ(t_i)$.

Caso 7: A regra é $J_\circ(x \circ y) \circ x \circ z \to J_\circ(y) \circ z$

O primeiro passo de redução pode ser representado por:

$$t \circ t_1 \circ \ldots \circ t_n = J_\circ(x \circ y)\sigma \circ x\sigma \circ z\sigma$$

para uma substituição σ.

Observe que $t = J_\circ(x\sigma \circ y\sigma)$ não acontece, pois $\mathrm{TOP}(t) \neq \circ$. Então, ou $x\sigma = t \circ u$ ou $z\sigma = t \circ u$ para algum u possivelmente vazio.

Mais ainda, existe um índice i tal que $t_i = J_\circ(x\sigma \circ y\sigma) \circ w$, com w possivelmente vazio.

Suponha, primeiramente, que $x\sigma = t \circ u$. Então $t_i = J_\circ(x\sigma \circ y\sigma) \circ w = J_\circ(t \circ u \circ y\sigma) \circ w$.

Como

$$\mathrm{DS}_\circ(t_i) = J_\circ(t) \cup \mathrm{DS}_\circ(J_\circ(u)) \cup \mathrm{DS}_\circ(J_\circ(y\sigma)) \cup \mathrm{DS}_\circ(w),$$

juntamente com o fato de $\mathsf{inv}_\circ(t) = J_\circ(t)$, segue que $\mathsf{inv}_\circ(t) \in \mathrm{DS}_\circ(t_i)$.

Agora, suponha que $z\sigma = t \circ t'_1 \circ \ldots \circ t'_k$, com t'_k um termo na forma normal, para cada índice k. Então

$$J_\circ(y\sigma) \circ z\sigma = t \circ J_\circ(y\sigma) \circ t'_1 \circ \ldots \circ t'_k.$$

Observe que $J_\circ(y\sigma), t'_1, \ldots, t'_k$ estão na forma normal. Além disso,

$$(J_\circ(y\sigma) \circ t'_1 \circ \ldots \circ t'_k)\downarrow = (t_1 \circ \ldots \circ t_n)\downarrow \neq e_\circ.$$

Mais ainda,

$$\begin{aligned} \mathrm{TOP}(t \circ (J_\circ(y\sigma) \circ t'_1 \circ \ldots \circ t'_k)\downarrow) &= \mathrm{TOP}((t \circ (t_1 \circ \ldots \circ t_n)\downarrow)\downarrow) \\ &= \mathrm{TOP}((t \circ t_1 \circ \ldots \circ t_n)\downarrow) \neq \circ. \end{aligned}$$

Por hipótese de indução, existe um j tal que $\mathsf{inv}_\circ(t) \in \mathrm{DS}_\circ(t'_j)$ ou $\mathsf{inv}_\circ(t) \in \mathrm{DS}_\circ(J_\circ(y\sigma))$.

Para o primeiro caso, analogamente ao Caso 3, existe um índice i tal que $\pi(j) = i$ e $t_{\pi(j)} = t'_j \circ u_j$. Logo, $\mathsf{inv}_\circ(t) \in \mathrm{DS}_\circ(t_i)$.

No segundo caso, como inicialmente $t_i = J_\circ(x\sigma \circ y\sigma) \circ w$ segue que

$$\mathrm{DS}_\circ(t_i) = \mathrm{DS}_\circ(J_\circ(x\sigma)) \cup \mathrm{DS}_\circ(J_\circ(y\sigma)) \cup \mathrm{DS}_\circ(w).$$

Portanto, $\mathsf{inv}_\circ(t) \in \mathrm{DS}_\circ(t_i)$.

Em todos os casos, existe um índice i tal que $\mathsf{inv}_\circ(t) \in \mathrm{DS}_\circ(t_i)$.

Caso 8: A regra é $h(x) \bullet h(y) \to h(x + y)$.

O primeiro passo de redução pode ser representado por:

$$t \bullet t_1 \bullet \ldots \bullet t_n = h(x)\sigma \bullet h(y)\sigma$$

para uma substituição σ.

Suponha que $t = h(x\sigma) = h(u_1)$. Como, por hipótese, $\mathrm{TOP}(t) \neq \bullet$ tem-se que $\mathrm{TOP}(u_1) \neq +$. Logo, $t_1 \bullet \ldots \bullet t_n = h(y\sigma)$ e com isso $n = 1$. Assim, $t_1 = h(y\sigma) = h(u_2)$.

Dessa forma, $h(x\sigma)$ e $h(y\sigma)$ são termos na forma normal.

Observe que $h(u_1 + u_2)\downarrow = (h((u_1 + u_2)\downarrow))\downarrow$.

Se $(u_1 + u_2)\downarrow \neq e_+$ então $h(u_1 + u_2)\downarrow = h((u_1 + u_2)\downarrow)$. Além disso, por hipótese, $\mathrm{TOP}(h(u_1 + u_2)\downarrow) \neq \bullet$ o que implica em $\mathrm{TOP}((u_1 + u_2)\downarrow) \neq +$. Observe ainda que, $u_2 \neq e_+$, caso contrário, t_1 não seria uma forma normal.

Portanto, por hipótese de indução, $\mathsf{inv}_+(u_1) \in \mathrm{DS}_+(u_2)$.

Pela definição de subtermos de decomposição, $\mathrm{DS}_\bullet(h(u_2)) = \{h(v) | v \in \mathrm{DS}_+(u_2)\}$. Assim,

$$\mathsf{inv}_\bullet(t) = \mathsf{inv}_\bullet(h(u_1)) = h(\mathsf{inv}_+(u_1)) \in \mathrm{DS}_\bullet(h(u_2)) = \mathrm{DS}_\bullet(t_1).$$

Agora, se $(u_1 + u_2)\downarrow = e_+$ será preciso analisar as possíveis regras aplicadas no termo $(u_1 + u_2)$. Em todos os casos, ou $u_1 = u_2 = e_+$ (que não acontece pois contradiz a normalidade de t e t_1) ou então $\mathsf{inv}_\bullet(t) \in \mathrm{DS}_\bullet(t_1)$, e o resultado segue.

Caso 9: A regra é $h(x) \bullet h(y) \bullet z \to h(x + y) \bullet z$.

O primeiro passo de redução pode ser representado por:

$$t \bullet t_1 \bullet \ldots \bullet t_n = h(x\sigma) \bullet h(y\sigma) \bullet z\sigma,$$

para alguma substituição σ.

Se $t = h(x\sigma)$ (respectivamente $t = h(y\sigma)$) por hipótese na estratégia, $h(y\sigma) \bullet z\sigma$ está na forma normal, já que nenhuma outra regra pode ser aplicada pela prioridade estabelecida.

Em particular, $z\sigma$ não pode ser escrito como $h(v) \bullet w$ ou $h(v)$ ou $J_\bullet(h(v)) \bullet w$ ou $J_\bullet(h(v))$, caso contrário $h(y\sigma) \bullet z\sigma$ seria escrito como $h(y\sigma) \bullet h(v) \bullet w$ ou $h(y\sigma) \bullet h(v)$ ou $h(y\sigma) \bullet J_\bullet(h(v)) \bullet w$ ou $h(y\sigma) \bullet J_\bullet(h(v))$, contradizendo a sua normalidade.

Dessa forma,

$$(t \bullet t_1 \bullet \ldots \bullet t_n)\downarrow = h(x\sigma \bullet y\sigma)\downarrow \bullet z\sigma.$$

Com isso, $\mathrm{TOP}((t \bullet t_1 \bullet \ldots \bullet t_n)\downarrow) = \bullet$, o que contradiz a hipótese do lema.

Portanto, o caso onde $t = h(x\sigma)$ (respectivamente $t = h(y\sigma)$) não acontece.

Logo, $z\sigma = t \bullet t'_1 \bullet \ldots \bullet t'_k$ onde cada t'_i está na forma normal. Mais ainda, cada t'_i e t devem estar encabeçados por h, pois $\mathrm{TOP}((h(x\sigma + y\sigma) \bullet z\sigma)\downarrow) \neq \bullet$.

Para cada índice i, sejam $t_i = h(u_i)$ e $t = h(u_0)$ então $(t \bullet t_1 \bullet \ldots \bullet t_n)\downarrow = h(v)$ onde $(u_0 + \ldots + u_n)\downarrow = v$.

Se $(u_1 + \ldots u_n)\downarrow = e_+$ então $(t_1 \bullet \ldots \bullet t_n)\downarrow = h(u_0 + \ldots + u_n) = e_\bullet$, o que contradiz a hipótese do lema.

Mais ainda, $\mathrm{TOP}(u_0 + \ldots u_n)\downarrow \neq +$, caso contrário, $\mathrm{TOP}((t_1 \bullet \ldots \bullet t_n)\downarrow) = \bullet$, outra contradição.

Assim, por hipótese de indução, $\mathsf{inv}_+(u_0) \in \mathrm{DS}_+(u_i)$, para algum índice i.

Como

$$\mathsf{inv}_\bullet(t) = \mathsf{inv}_\bullet(h(u_0)) = h(\mathsf{inv}_+(u_0))$$

e, por definição

$$\mathrm{DS}_\bullet(t_i) = \mathrm{DS}_\bullet(h(u_i)) = \left\{h(v') | v' \in \mathrm{DS}_+(u_i))\right\},$$

segue que $\mathsf{inv}_\bullet(t) \in \mathrm{DS}_\bullet(t_i)$.

Em todos os casos,existe um índice i tal que $\mathsf{inv}_\circ(t) \in \mathrm{DS}_\circ(t_i)$. □

O seguinte lema pode ser visto com uma extensão do lema anterior, pois além dos termos $t_1, \ldots, t_n$ considera um conjunto finito de termos $u_1, \ldots, u_m$, com $m \geq 1$, que tem as mesmas propriedades do termo t do lema anterior.

Lema 5 Seja $\circ \in \{\star, \bullet, +\}$, $t_1, \ldots, t_n, u_1, \ldots, u_m$ termos na forma normal tais que para todo i, $\mathrm{TOP}(t_i) = \circ$ e $\mathrm{TOP}(u_i) \notin \{\circ, e_\circ\}$. Seja $u = (t_1 \circ \ldots \circ t_n \circ u_1 \circ \ldots \circ u_m)\downarrow$. Então para todo i, ou $u_i \in \mathrm{DS}_\circ(u)$ ou existe um índice j tal que $\mathsf{inv}_\circ(u_i) \in \mathrm{DS}_\circ(t_j)$, ou ainda existe um índice j tal que $u_j = \mathsf{inv}_\circ(u_i)$.

Demonstração: Seja $t_{n+1} = \mathsf{inv}_\circ(u)$ um termo na forma normal. Como $\mathcal{R}$ é um sistema AC-convergente, existe um inteiro k tal que

$$(t_1 \circ \ldots \circ t_n \circ u_1 \circ \ldots \circ u_m \circ t_{n+1}) \xrightarrow{(k)} (t_1 \circ \ldots \circ t_n \circ u_1 \circ \ldots \circ u_m \circ t_{n+1})\downarrow .$$

Considere a seguinte estratégia de redução:

$$(t_1 \circ \ldots \circ t_n \circ u_1 \circ \ldots \circ u_m \circ t_{n+1}) \xrightarrow{(k-1)} ((t_1 \circ \ldots \circ t_n \circ u_1 \circ \ldots \circ u_m)\downarrow \circ t_{n+1}) \to e_\circ$$

Assim, $\mathrm{TOP}((t_1 \circ \ldots \circ t_n \circ u_1 \circ \ldots \circ u_m \circ t_{n+1})\downarrow) \neq \circ$.

Mais ainda, como $t_{n+1} = \mathsf{inv}_\circ(t_1 \circ \ldots \circ t_n \circ u_1 \circ \ldots \circ u_m)\downarrow$, segue que

$$(t_1 \circ \ldots \circ t_n \circ t_{n+1} \circ u_1 \circ \ldots \circ u_{i-1} \circ u_{i+1} \circ \ldots \circ u_m)\downarrow = u_i \neq e_\circ$$

para cada i, tal que $1 \leq i \leq m$.

Portanto, os termos $t_1, \ldots, t_n, t_{n+1}, u_1, \ldots, u_m$ satisfazem as hipóteses do Lema 4. Consequentemente, para cada i, ou $\mathsf{inv}_\circ(u_i) \in \mathrm{DS}_\circ(t_{n+1})$ ou existe um índice j tal que $\mathsf{inv}_\circ(u_i) \in \mathrm{DS}_\circ(u_j)$ ou $\mathsf{inv}_\circ(u_j) \in \mathrm{DS}_\circ(t_j)$.

Segue do primeiro caso que $u_i \in \mathrm{DS}_\circ(u)$, pois $\mathsf{inv}_\circ(u_i) \in \mathrm{DS}_\circ(\mathsf{inv}_\circ(u))$. Agora, do segundo caso, tem-se $\mathsf{inv}_\circ(u_i) = u_j$, já que $\mathrm{TOP}(u_j) \neq \circ$ implica que $\mathrm{DS}_\circ(u_j) = \{u_j\}$.

□

3.2 Modelo de Dolev-Yao extendido com a teoria equacional EP

Um dos principais problemas em verificação automática de protocolos criptográficos é conhecido como *problema da dedução do intruso*:

Dado um conjunto finito T de mensagens e (provavelmente) um segredo s, o intruso pode deduzir s de T?

Este problema depende da capacidade de dedução do intruso. Existem diferentes formas de analisar as propriedades de segurança de protocolos criptográficos. Entre elas, encontra-se a abordagem clássica de Dolev-Yao [DY81], que consiste em modelar um intruso através de um sistema de regras de dedução.

Para decidir o problema da dedução do intruso para o protocolo criptográfico em questão, será utilizado uma extensão do modelo de Dolev-Yao. Esta extensão utiliza os operadores dados pela assinatura $\mathcal{F}$ e uma teoria equacional EP que pode ser explorada pelo intruso para montar um ataque.

O sistema de dedução que descreve a habilidade do intruso, denotado por $\mathcal{I}_{\mathsf{EP}}$ é dado na Figura 1, onde $\mathcal{F}' = \{J_+, J_\star, J_\bullet, h, \mathsf{exp}\}$ e $\circ \in \{+, \star, \bullet\}$.

$$(\mathsf{A})\ \frac{}{T \vdash u}\ \text{se } u \in T \qquad (\mathsf{F})\ \frac{T \vdash u_1 \qquad T \vdash u_2}{T \vdash f(u_1, u_2)}\ f \in \mathcal{F}'$$

$$(\mathsf{G}_\circ)\ \frac{T \vdash u_1 \qquad \ldots \qquad T \vdash u_n}{T \vdash (u_1 \circ \ldots \circ u_n)} \qquad (\mathsf{Eq})\ \frac{T \vdash u}{T \vdash v}\ u =_{\mathsf{EP}} v$$

Figura 1. Sistema de Inferência $\mathcal{I}_{\mathsf{EP}}$

Este sistema de dedução é composto das seguintes regras: (A) o intruso pode utilizar qualquer termo que conheça previamente, (F) ele pode construir um novo termo utilizando o símbolo de função f e (Eq) o intruso pode deduzir todos os termos congruentes a um termo que ele conheça

inicialmente. Com a distinção do operador binário $\circ$ adiciona-se uma família de regras ($\mathsf{G}_\circ$) que permite ao intruso construir um novo termo a partir de um número arbitrário de termos já conhecidos utilizando o operador associativo $\circ$.

Assumindo esse sistema de dedução para o intruso, o objetivo central deste trabalho (e que será resolvido nos próximos capítulos) é analisar a decidibilidade do *problema da dedução do intruso*, que corresponde ao problema de decisão de segurança na presença de um intruso passivo. Este problema pode ser representado pelo seguinte teorema.

Teorema 2 *O problema da dedução do intruso* é decidível em tempo polinomial para o sistema de inferência $\mathcal{I}_{\mathsf{EP}}$.

Antes de provar este resultado, é preciso observar que o sistema $\mathcal{I}_{\mathsf{EP}}$ não é apropriado para prova automática, pois a regra (Eq) permite raciocínio equacional em qualquer momento da prova. Isto é, em cada passo, o intruso pode calcular todos os termos equivalentes módulo EP a um termo que ele conheça anteriormente, o que resulta num conjunto infinito de termos.

Para resolver este problema, no próximo capítulo, será introduzido um novo sistema de inferência que é equivalente a $\mathcal{I}_{\mathsf{EP}}$, do ponto de vista de dedução, e que satisfaz algumas propriedades mais fortes.

Finalmente, depois que todos os resultados necessários forem estabelecidos, será possível provar o Teorema 2.

Capítulo 4

O problema da dedução do intruso é PTIME para $\mathcal{I}_{\mathsf{EP}}$

Neste capítulo será provado que *o problema da dedução do intruso* é decidível em tempo limitado polinomialmente para o sistema de inferência $\mathcal{I}_{\mathsf{EP}}$.

O ponto de partida para esta prova é o resultado introduzido por David McAllester [McA90]. Ele mostra, através do Lema de Tratabilidade, que existe um algoritmo em tempo polinomial para decidir a deducibilidade de um termo t a partir de um conjunto finito de termos T se o sistema de dedução tem uma propriedade chamada *localidade*, que será introduzida na seção 1 deste capítulo. Ainda nesta seção, será mostrado que o sistema de dedução $\mathcal{I}_{\mathsf{EP}}$ é equivalente a outro sistema de inferência $\mathcal{I}_1 \cup \mathcal{I}_2$, que tem esta propriedade, ou seja, toda prova de $T \vdash t$ pode ser transformada em uma prova cujos nós são subtermos sintáticos de T e t, isto é, pertencem a $F(T \cup \{t\})$.

Ainda neste capítulo, será introduzido o conceito de *deducibilidade em um-passo*. Com isso, será possível a obtenção de um algoritmo polinomial através do teste de um termo t ser um passo dedutível de um conjunto finito de termos T. Com estes conceitos estabelecidos, pode ser provado que *O problema da dedução do intruso* é PTIME para o sistema de inferência $\mathcal{I}_1 \cup \mathcal{I}_2$, que é equivalente ao sistema $\mathcal{I}_{\mathsf{EP}}$.

4.1 Localidade

Nesta seção, será definido um novo sistema de inferência que é equivalente a $\mathcal{I}_{\mathsf{EP}}$ e então será mostrado que este sistema é *local* com relação a um noção de subtermos F.

Definição 26 (Noção de Subtermos) Uma *noção de subtermos* é uma função

$$F : T(\mathcal{F}, \mathcal{X}) \to \mathrm{Sub}(T(\mathcal{F}, \mathcal{X}))$$

que associa à um termo t o conjunto finito dos seus subtermos.

Definição 27 Seja P uma prova de $t \vdash u$.

- Uma *subprova* P' de P é uma sub-árvore de P.
- O *tamanho* de uma prova P, denotado por $|P|$, é o número de nós em P.
- Uma *subfórmula* de P é um nó da árvore P.
- Uma prova P de $T \vdash u$ é *minimal* se para toda prova P' de $T \vdash u$: $|P| \leq |P'|$.
- Uma prova P de $T \vdash u$ é *normal* nenhuma regra de dedução pode ser aplicada.

Definição 28 (F-localidade) Seja F uma noção de subtermos. Uma prova P de $T \vdash u$ é F-local se todas fórmulas intermediárias estão em $F(T \cup \{u\})$. Um sistema de inferência $\mathcal{I}$ é F-local se sempre que existir uma prova de $T \vdash u$ em $\mathcal{I}$ existe uma que é F-local.

Notação: Seja F uma noção de subtermos. Denota-se por $F(T)$ o conjunto $\bigcup_{t \in T} F(t)$.

Este novo sistema de inferência pode ser visto com a união de dois sistemas, denotados respectivamente, por $\mathcal{I}_1$ e $\mathcal{I}_2$.

A partir de agora, a regra (Eq) será omitida e com utilização de uma variação do modelo de dedução que opera em formas normais, após cada passo, o termo obtido é reduzido para sua forma normal.

O sistema $\mathcal{I}_1$ é composto das seguintes 7 regras, onde $\mathcal{F}^- = \{J_+, J_\star, J_\bullet, h\}$ e $\circ \in \{+, \star, \bullet\}$.

$$(\mathsf{R}_f)\ \frac{T \vdash u_1 \quad \ldots \quad T \vdash u_n}{T \vdash f(u_1, \ldots, u_n)\downarrow_{\mathcal{R}/AC}},\ f \in \mathcal{F}^- \qquad (\mathsf{R}_\circ)\ \frac{T \vdash u_1 \quad \ldots \quad T \vdash u_n}{T \vdash (u_1 \circ \ldots \circ u_n)\downarrow_{\mathcal{R}/AC}}$$

E $\mathcal{I}_2$ é o sistema de inferência composto das três seguintes regras:

$$\frac{H \vdash h(t_1) \quad H \vdash t_2 \quad \ldots H \vdash t_n}{H \vdash h(t_1 \star \cdots \star t_n)\downarrow_{\mathcal{R}/AC}}\ (\mathsf{Exp}_1)$$

$$\frac{H \vdash \mathsf{exp}(t_1, t_2) \quad H \vdash t_3 \quad \ldots H \vdash t_n}{H \vdash \mathsf{exp}(t_1, t_2 \star \cdots \star t_n)\downarrow_{\mathcal{R}/AC}}\ (\mathsf{Exp}_2)$$

$$\frac{H \vdash t_1 \quad H \vdash t_2}{H \vdash \mathsf{exp}(t_1, t_2)\downarrow_{\mathcal{R}/AC}}\ (\mathsf{Exp}_3)$$

As regras obtidas por exponenciação serão decompostas, dependendo da primeira premissa da regra de inferência:

- ou a primeira premissa é $u = h(t_1)$ e a regra é Exp_1;
- ou então a primeira premissa é $u = \mathsf{exp}(t_1, t_2)$ e a regra é Exp_2;
- ou ainda aplicação da exponenciação a u, v produz um termo $\mathsf{exp}(u, v)$ já na forma normal, e a regra obtida é Exp_3.

Esta decomposição de uma única regra em três regras de inferência distintas, será mais conveniente para provas futuras.

Na sequência será omitido o índice $\mathcal{R}/AC$ e ao invés de $\rightarrow_{\mathcal{R}/AC}$ será usado apenas $\rightarrow$.

A seguinte proposição mostra que este novo sistema de regras inferência é equivalente ao sistema anterior $\mathcal{I}_{\mathsf{EP}}$, para termos na forma normal.

Proposição 1 Seja T um conjunto de termos e u um termo (na forma normal).

$T \vdash u$ é derivável em $\mathcal{I}_{\mathsf{EP}}$ se, e somente se, $T \vdash u$ é derivável em $\mathcal{I}_1 \cup \mathcal{I}_2$.

Demonstração: Suponha que $T \vdash u$ é derivável em $\mathcal{I}_{\mathsf{EP}}$

Será provado, por indução no tamanho da prova de u, que $T \vdash u$ é derivável em $\mathcal{I}_1 \cup \mathcal{I}_2$.

Base da indução: A prova consiste apenas de um axioma, isto é,

$$\frac{}{T \vdash_{\mathcal{I}_{\mathsf{EP}}} u}\, , u \in T$$

se e, somente se

$$\frac{}{T \vdash_{\mathcal{I}_1 \cup \mathcal{I}_2} u}\, , u \in T$$

novamente por axioma.

Passo indutivo: Será analisada a última regra usada na prova de $T \vdash_{\mathcal{I}_{\mathsf{EP}}} u$.

- *A última regra é* (F) *com* $f \in \mathcal{F}' - \{\mathsf{exp}\}$

A prova de u pode ser representada por:

$$(F)\ \frac{\dfrac{\Pi_1}{T \vdash_{\mathcal{I}_{\mathsf{EP}}} u_1}}{T \vdash_{\mathcal{I}_{\mathsf{EP}}} u = f(u_1)}\ (f \in \mathcal{F} - \{\mathsf{exp}\})$$

Como, por hipótese, u é um termo na forma normal e (f) é a última regra aplicada na prova de $T \vdash_{\mathcal{I}_{\mathsf{EP}}} u = f(u_1)$, segue que $u = f(u_1) = f(u_1) \downarrow$ e assim, u_1 pode ser considerado um termo na forma normal.

Além disso, $T \vdash u_1$ é derivável em $\mathcal{I}_{\mathsf{EP}}$, então, por hipótese de indução, $T \vdash_{\mathcal{I}_1 \cup \mathcal{I}_2} u_1$.

Assim,

$$\frac{\dfrac{\Pi_1'}{T \vdash_{\mathcal{I}_1 \cup \mathcal{I}_2} u_1}}{T \vdash_{\mathcal{I}_1 \cup \mathcal{I}_2} u = f(u_1) \downarrow}\ (\mathsf{R}_f) \in \mathcal{I}_1$$

Logo, $T \vdash u$ é derivável em $\mathcal{I}_1 \cup \mathcal{I}_2$.

- *A última regra é* (F) *com* $f = \mathsf{exp}$.

  A prova de u pode ser representada por:

$$\dfrac{\dfrac{\Pi_1}{T \vdash_{\mathcal{I}_{\mathsf{EP}}} u_1} \quad \dfrac{\Pi_2}{T \vdash_{\mathcal{I}_{\mathsf{EP}}} u_2}}{T \vdash_{\mathcal{I}_{\mathsf{EP}}} u = \mathsf{exp}(u_1, u_2)} \text{ onde } f = \mathsf{exp}$$

  Novamente, como u é um termo na forma normal, $u = \mathsf{exp}(u_1, u_2) = \mathsf{exp}(u_1, u_2)\downarrow$, u_1 e u_2 podem ser considerados termos na forma normal e deriváveis em $\mathcal{I}_{\mathsf{EP}}$, por hipótese de indução, u_1 e u_2 são deriváveis em $\mathcal{I}_1 \cup \mathcal{I}_2$, ou seja, $T \vdash_{\mathcal{I}_1 \cup \mathcal{I}_2} u_i$, com $i = 1, 2$.

  Assim,

$$\dfrac{\dfrac{\Pi_1'}{T \vdash_{\mathcal{I}_1 \cup \mathcal{I}_2} u_1} \quad \dfrac{\Pi_2'}{T \vdash_{\mathcal{I}_1 \cup \mathcal{I}_2} u_2}}{T \vdash_{\mathcal{I}_1 \cup \mathcal{I}_2} u = \mathsf{exp}(u_1, u_2)\downarrow} \mathsf{Exp}_i \text{ com } i = 1, 2, 3$$

  A escolha de i depende de $\mathrm{TOP}(u_1)$.

  Quando $\mathrm{TOP}(u_1) = h$, $\mathrm{TOP}(u_1) = \mathsf{exp}$ e $\mathrm{TOP}(u_1) \notin \{h, \mathsf{exp}\}$ segue que $T \vdash u$ é derivável em $\mathcal{I}_1 \cup \mathcal{I}_2$ pelas regras Exp_1, Exp_2 e Exp_3, respectivamente.

- *A última regra é* $(\mathsf{G}_\circ)$.

  A prova de u pode ser representada por:

$$(\mathsf{G}_\circ)\ \dfrac{\dfrac{\Pi_1}{T \vdash_{\mathcal{I}_{\mathsf{EP}}} u_1} \quad \ldots \quad \dfrac{\Pi_n}{T \vdash_{\mathcal{I}_{\mathsf{EP}}} u_n}}{T \vdash_{\mathcal{I}_{\mathsf{EP}}} (u_1 \circ \ldots \circ u_n)}\ (\circ \in \{+, \star, \bullet\})$$

  Como, por hipótese, u é um termo na forma normal e $(\mathsf{G}_\circ)$ é a última regra aplicada na prova de $T \vdash_{\mathcal{I}_{\mathsf{EP}}} u = (u_1 \circ \ldots \circ u_n)$, segue que $u = (u_1 \circ \ldots \circ u_n) = (u_1 \circ \ldots \circ u_n)\downarrow$ e assim, $u_1, \ldots, u_n$ são termos na forma normal.

  Além disso, $T \vdash u_i$ é derivável em $\mathcal{I}_{\mathsf{EP}}$, para todo $i = 1, \ldots, n$, então, por hipótese de indução, $T \vdash_{\mathcal{I}_1 \cup \mathcal{I}_2} u_i$.

Assim,

$$\dfrac{\dfrac{\Pi'_1}{T \vdash_{\mathcal{I}_1 \cup \mathcal{I}_2} u_1} \quad \ldots \quad \dfrac{\Pi'_n}{T \vdash_{\mathcal{I}_1 \cup \mathcal{I}_2} u_n}}{T \vdash_{\mathcal{I}_1 \cup \mathcal{I}_2} u = (u_1 \circ \ldots \circ u_n)\downarrow}\ (\mathsf{R}_f) \in \mathcal{I}_1$$

Logo, $T \vdash u$ é derivável em $\mathcal{I}_1 \cup \mathcal{I}_2$.

- *A última regra é* (Eq).

A prova de u pode ser representada por:

$$\dfrac{\dfrac{\dfrac{\Pi_1}{T \vdash_{\mathcal{I}_{\mathsf{EP}}} u_1}\ (\mathsf{Eq})}{T \vdash_{\mathcal{I}_{\mathsf{EP}}} u_1\downarrow} \quad \ldots \quad \dfrac{\dfrac{\Pi_n}{T \vdash_{\mathcal{I}_{\mathsf{EP}}} u_n}\ (\mathsf{Eq})}{T \vdash_{\mathcal{I}_{\mathsf{EP}}} u_n\downarrow}\ (\mathsf{Eq})}{\dfrac{T \vdash_{\mathcal{I}_{\mathsf{EP}}} u = f(u_1, \ldots, u_n)}{T \vdash_{\mathcal{I}_{\mathsf{EP}}} u = f(u_1, \ldots, u_n)\downarrow}\ (\mathsf{Eq})}\ (f \in \mathcal{F})$$

Por hipótese de indução, $T \vdash u_i\downarrow$ são deriváveis em $\mathcal{I}_1 \cup \mathcal{I}_2$, i.e, $T \vdash_{\mathcal{I}_1 \cup \mathcal{I}_2} u_i\downarrow$, com $i = 1, \ldots, n$.

Assim,

$$\dfrac{\dfrac{\Pi'_1}{T \vdash_{\mathcal{I}_1 \cup \mathcal{I}_2} u_1\downarrow} \quad \ldots \quad \dfrac{\Pi'_n}{T \vdash_{\mathcal{I}_1 \cup \mathcal{I}_2} u_n\downarrow}}{T \vdash_{\mathcal{I}_1 \cup \mathcal{I}_2} u = f(u_1, \ldots, u_n)\downarrow}\ (\mathsf{R}'_f \in \mathcal{I}_1 \cup \mathcal{I}_2)$$

Logo, $T \vdash u$ é derivável em $\mathcal{I}_1 \cup \mathcal{I}_2$.

Reciprocamente, suponha que $T \vdash u$ é derivável em $\mathcal{I}_1 \cup \mathcal{I}_2$.

Novamente, será mostrado, por indução no tamanho da prova de u, que $T \vdash u$ é derivável em $\mathcal{I}_{\mathsf{EP}}$.

Base da indução. A prova de u consiste de um axioma, como foi provado no caso acima.

Passo indutivo. Será analisada a última regra usada na prova de $T \vdash_{\mathcal{I}_1 \cup \mathcal{I}_2} u$.

- *A última regra é* $\mathsf{R_f} \in \mathcal{I}_1$.

A prova de u pode ser representada por:

$$\dfrac{\dfrac{\Pi_1}{T \vdash_{\mathcal{I}_1 \cup \mathcal{I}_2} u_1}}{T \vdash_{\mathcal{I}_1 \cup \mathcal{I}_2} u = f(u_1)\downarrow}\,(\mathsf{R}_f)$$

Por hipótese de indução, a premissa $T \vdash u_1 = u_1 \downarrow$ é derivável em $\mathcal{I}_{\mathsf{EP}}$. Assim,

$$\dfrac{\dfrac{\dfrac{\Pi_1'}{T \vdash_{\mathcal{I}_{\mathsf{EP}}} u_1}}{T \vdash_{\mathcal{I}_{\mathsf{EP}}} f(u_1)}\, f \in \mathcal{F}^-}{T \vdash_{\mathcal{I}_{\mathsf{EP}}} (f(u_1)\downarrow) = u}\,(\mathsf{Eq})$$

Logo, $T \vdash u$ é derivável em $\mathcal{I}_{\mathsf{EP}}$.

- *A última regra é* $\mathsf{R}_\circ$*, com* $\circ \in \{+, \star, \bullet\}$.

A prova de u pode ser representada por:

$$\dfrac{\dfrac{\Pi_1}{T \vdash_{\mathcal{I}_1 \cup \mathcal{I}_2} u_1} \quad \ldots \quad \dfrac{\Pi_n}{T \vdash_{\mathcal{I}_1 \cup \mathcal{I}_2} u_n}}{T \vdash_{\mathcal{I}_1 \cup \mathcal{I}_2} u = (u_1 \circ \ldots \circ u_n)\downarrow}\,(\mathsf{R}_\circ)$$

Por hipótese de indução, as premissas $T \vdash u_1, \ldots, T \vdash u_n$ estão na forma normal e são deriváveis em $\mathcal{I}_{\mathsf{EP}}$. Assim,

$$\dfrac{\dfrac{\dfrac{\Pi_1'}{T \vdash_{\mathcal{I}_{\mathsf{EP}}} u_1} \quad \ldots \quad \dfrac{\Pi_n'}{T \vdash_{\mathcal{I}_{\mathsf{EP}}} u_n\downarrow}}{T \vdash_{\mathcal{I}_{\mathsf{EP}}} (u_1 \circ \ldots \circ u_n)}\,(\mathsf{G}_\circ)}{T \vdash_{\mathcal{I}_{\mathsf{EP}}} (u_1 \circ \ldots \circ u_n)\downarrow = u}\,(\mathsf{Eq})$$

Logo, $T \vdash u$ é derivável em $\mathcal{I}_{\mathsf{EP}}$.

- *A última regra é* Exp_1

A prova de u pode ser representada por:

$$\dfrac{\dfrac{\Pi_1}{T \vdash_{\mathcal{I}_1 \cup \mathcal{I}_2} h(u_1)} \quad \dfrac{\Pi_2}{T \vdash_{\mathcal{I}_1 \cup \mathcal{I}_2} u_2} \quad \cdots \dfrac{\Pi_n}{T \vdash_{\mathcal{I}_1 \cup \mathcal{I}_2} u_n}}{T \vdash_{\mathcal{I}_1 \cup \mathcal{I}_2} \mathsf{exp}(h(u_1), u_2, \ldots, u_n) \downarrow = h(u_1 \star \ldots \star u_n) \downarrow} \mathsf{Exp}_1$$

Por hipótese de indução, segue que $T \vdash h(u_1), T \vdash u_2, \ldots, T \vdash u_n$ são deriváveis em $\mathcal{I}_{\mathsf{EP}}$.

Assim,

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\Pi'_1}{T \vdash_{\mathcal{I}_{\mathsf{EP}}} h(u_1)} \quad \dfrac{\Pi'_2}{T \vdash_{\mathcal{I}_{\mathsf{EP}}} u_2}}{T \vdash_{\mathcal{I}_{\mathsf{EP}}} \mathsf{exp}(h(u_1), u_2)}\,(\mathsf{exp})}{T \vdash_{\mathcal{I}_{\mathsf{EP}}} \mathsf{exp}(h(u_1), u_2) \downarrow = h(u_1 \star u_2) \downarrow}\,(\mathsf{Eq}) \quad T \vdash_{\mathcal{I}_{\mathsf{EP}}} u_3}{T \vdash_{\mathcal{I}_{\mathsf{EP}}} \mathsf{exp}(h(u_1 \star u_2), u_3)}\,(\mathsf{exp})}{T \vdash_{\mathcal{I}_{\mathsf{EP}}} \mathsf{exp}(h(u_1 \star u_2), u_3) \downarrow = (h(u_1 \star u_2 \star u_3) \downarrow}\,(\mathsf{Eq})}{\dfrac{\dfrac{\vdots}{h(u_1 \star \ldots \star u_{n-1})}\,(\mathsf{Eq}) \quad T \vdash_{\mathcal{I}_{\mathsf{EP}}} u_n}{T \vdash_{\mathcal{I}_{\mathsf{EP}}} \mathsf{exp}(h(u_1 \star \ldots \star u_{n-1}), u_n)}\,(\mathsf{exp})}{T \vdash_{\mathcal{I}_{\mathsf{EP}}} \mathsf{exp}(h(u_1 \star \ldots \star u_{n-1}), u_n) \downarrow = h(u_1 \star \ldots \star u_n) \downarrow = u}\,(\mathsf{Eq})$$

Logo, $T \vdash u$ é derivável em $\mathcal{I}_{\mathsf{EP}}$.

- *A última regra é* Exp_2.

A prova de u pode ser representada por:

$$\dfrac{\dfrac{\Pi_1}{T \vdash_{\mathcal{I}_1 \cup \mathcal{I}_2} \mathsf{exp}(u_1, u_2)} \quad \dfrac{\Pi_2}{T \vdash_{\mathcal{I}_1 \cup \mathcal{I}_2} u_3} \quad \cdots \dfrac{\Pi_{n-1}}{T \vdash_{\mathcal{I}_1 \cup \mathcal{I}_2} u_n}}{T \vdash_{\mathcal{I}_1 \cup \mathcal{I}_2} \mathsf{exp}(u_1, u_2 \star \ldots \star u_n) \downarrow} \mathsf{Exp}_2$$

Por hipótese de indução, $\mathsf{exp}(u_1, u_2), u_3 \ldots, u_n$ são deriváveis em $\mathcal{I}_{\mathsf{EP}}$.

Assim,

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\Pi_1'}{T \vdash_{\mathcal{I}_{\mathsf{EP}}} \mathsf{exp}(u_1,u_2)} \quad \dfrac{\Pi_2'}{T \vdash_{\mathcal{I}_{\mathsf{EP}}} u_3}}{T \vdash_{\mathcal{I}_{\mathsf{EP}}} \mathsf{exp}(\mathsf{exp}(u_1,u_2),u_3)}\,(\mathsf{exp})}{T \vdash_{\mathcal{I}_{\mathsf{EP}}} \mathsf{exp}(\mathsf{exp}(u_1,u_2),u_3) \downarrow= \mathsf{exp}(u_1, u_2 \star u_3)}\,(\mathsf{Eq}) \quad T \vdash_{\mathcal{I}_{\mathsf{EP}}} u_4}{T \vdash_{\mathcal{I}_{\mathsf{EP}}} \mathsf{exp}(\mathsf{exp}(u_1,u_2 \star u_3),u_4)}\,(\mathsf{exp})}{T \vdash_{\mathcal{I}_{\mathsf{EP}}} \mathsf{exp}(\mathsf{exp}(u_1,u_2 \star u_3),u_4) \downarrow= \mathsf{exp}(\mathsf{exp}(u_1,u_2 \star u_3 \star u_4)}\,(\mathsf{Eq})$$

$$\dfrac{\dfrac{\dfrac{\vdots}{\mathsf{exp}(u_1, u_2 \star u_3 \star \ldots \star u_{n-1})}\,(\mathsf{Eq}) \quad T \vdash_{\mathcal{I}_{\mathsf{EP}}} u_n}{T \vdash_{\mathcal{I}_{\mathsf{EP}}} \mathsf{exp}(\mathsf{exp}(u_1, u_2 \star u_3 \star \ldots \star u_{n-1}), u_n)}\,(\mathsf{exp})}{T \vdash_{\mathcal{I}_{\mathsf{EP}}} \mathsf{exp}(u_1, u_2 \star u_3 \star \ldots \star u_{n-1} \star u_n) \downarrow= u}\,(\mathsf{Eq})$$

Logo, $T \vdash u$ é derivável em $\mathcal{I}_{\mathsf{EP}}$.

- *A última regra é* Exp_3.

A prova de u pode ser representada por:

$$\dfrac{\dfrac{\Pi_1}{T \vdash_{\mathcal{I}_1 \cup \mathcal{I}_2} u_1} \quad \dfrac{\Pi_2}{T \vdash_{\mathcal{I}_1 \cup \mathcal{I}_2} u_2}}{T \vdash_{\mathcal{I}_1 \cup \mathcal{I}_2} \mathsf{exp}(u_1,u_2) = \mathsf{exp}(u_1,u_2) \downarrow= u}\,\mathsf{Exp}_3$$

com $\mathrm{TOP}(u_i) \notin \{\mathsf{exp}, h\}$.

Por hipótese de indução, $T \vdash u_1$ e $T \vdash u_2$ são deriváveis em $\mathcal{I}_{\mathsf{EP}}$.

Assim,

$$\dfrac{\dfrac{\Pi_1'}{T \vdash_{\mathcal{I}_{\mathsf{EP}}} u_1} \quad \dfrac{\Pi_2'}{T \vdash_{\mathcal{I}_{\mathsf{EP}}} u_2}}{T \vdash_{\mathcal{I}_{\mathsf{EP}}} \mathsf{exp}(u_1,u_2) = \mathsf{exp}(u_1,u_2) \downarrow= u}\,(\mathsf{exp})$$

Logo, $T \vdash u$ é derivável em $\mathcal{I}_{\mathsf{EP}}$.

□

Definição 29 (regra de decomposição) A aplicação de uma regra em $\mathcal{I}_2$ é uma *decomposição* se é uma instância da regra Exp_1 e o termo resultante é da forma $h(u)$ com $\mathrm{TOP}(u) \neq \star$. Uma *regra de decomposição* para $\mathcal{I}_1$ é uma regra R_f, tal que uma das seguintes situações ocorre:
- $f \in \{\star, \bullet, +\}$ e a conclusão $t = (f(t_1, \ldots, t_n)) \downarrow$ é tal que $\mathrm{TOP}(t) \neq f$
- $f = J_\circ$ e a regra é aplicada para um termo da forma $J_\circ(t)$.

Regras que não são regras de decomposição são *composições.*

Lema 6 Se t é obtido por decomposição usando $\mathsf{R}_f \in \mathcal{I}_1$, uma das seguintes situações ocorre:
- $t \in \{e_+, e_\star, e_\bullet\}$
- a premissa é $f(t)$ $\;(f \in \{J_+, J_\star, J_\bullet\})$
- $f \in \{\star, +, \bullet\}$ e existe uma premissa u tal que $t \in \mathrm{DS}_f(u)$.

Demonstração: Pela Definição 29, uma regra de decomposição para $\mathcal{I}_1$ é uma regra R_f quando $f \in \{J_\circ, \circ\}$ e $\circ \in \{\star, +, \bullet\}$.

Se $f = J_\circ$, a regra é aplicada a um termo da forma $f(t)$, o que implica que a premissa é $f(t)$, concluindo o segundo caso do lema.

Seja $f = \circ \in \{\star, +, \bullet\}$ e considere $t_1, \ldots, t_n$ termos na forma normal, $n \geq 2$, como as premissas da regra, a conclusão é $t = (t_1 \circ \ldots \circ t_n) \downarrow$ tal que $\mathrm{TOP}(t) \neq \circ$.

Se $t = e_\circ$, segue o primeiro caso da conclusão do lema.

Suponha que $t \neq e_\circ$. Então, $(\mathsf{inv}_\circ(t) \circ t_1 \circ \ldots \circ t_n) \downarrow = e_\circ$.

De fato, $(\mathsf{inv}_\circ(t) \circ t_1 \circ \ldots \circ t_n)$ reduz para sua forma normal $(\mathsf{inv}_\circ(t) \circ t_1 \circ \ldots \circ t_n) \downarrow$ após um número finito m de passos de redução, pois pelo Lema 2, $\mathcal{R}$ é convergente módulo AC.

Considere a seguinte estratégia para normalizar $(\mathsf{inv}_\circ(t) \circ t_1 \circ \ldots \circ t_n)$:

$$(\mathsf{inv}_\circ(t) \circ t_1 \circ \ldots \circ t_n) \overset{\leq m}{\to} \mathsf{inv}_\circ(t) \circ (t_1 \circ \ldots \circ t_n)\downarrow = \mathsf{inv}_\circ(t) \circ t \to e_\circ$$

Então

$$(\mathsf{inv}_\circ(t) \circ t_1 \circ \ldots \circ t_n)\downarrow = e_\circ.$$

Portanto, aplicando o Lema 4, segue que existe um índice i, tal que $\mathsf{inv}_\circ(\mathsf{inv}_\circ(t)) \in \mathrm{DS}_\circ(t_i)$, ou ainda, $t \in \mathrm{DS}_f(t_i)$, concluindo então o terceiro caso do Lema. □

Lema 7 *Se t é obtido por uma regra de decomposição de $\mathcal{I}_2$, então as premissas podem ser escritas $h(t_1), t_2, \ldots, t_n, t = h(u)$ e existe um índice i tal que $t_i = e_\star$ ou $u \in \mathrm{DS}_\star(t_i)$.*

Demonstração: Se t é obtido por uma regra de decomposição de $\mathcal{I}_2$ então, por definição, esta regra é uma instância de Exp_1. Com isso, as premissas são $h(t_1), t_2, \ldots, t_n$ e o termo resultante é $t = h(u)$ com $u = (t_1 \star \ldots \star t_n)\downarrow$ e $\mathrm{TOP}(u) \neq \star$.

Agora, como $\mathrm{TOP}(u) \neq \star$, novamente pela definição de regra de decomposição, a regra $\mathsf{R}_\star$ com premissas $t_1, \ldots, t_n$ e conclusão u é uma decomposição. Pelo lema anterior, $u = e_\star$ ou então existe um índice i, tal que $u \in \mathrm{DS}_\star(t_i)$. □

Agora, para provar que o sistema de inferência $\mathcal{I}_1 \cup \mathcal{I}_2$ tem a propriedade de localidade será necessária a seguinte noção de subtermos F:

$$
\begin{aligned}
F(T) \;=\; & \mathrm{Sub}(T) \\
& \cup \{h(t) \,|\, t \in \mathrm{Sub}(T), \mathrm{TOP}(t) = +\} \\
& \cup \{h(\mathsf{inv}_+(t) \,|\, t \in \mathrm{Sub}(T), \mathrm{TOP}(t) = +\} \\
& \cup \{\mathsf{inv}_\circ(t) \,|\, t \in \mathrm{Sub}(T), \mathrm{TOP}(t) = \circ, \quad \circ \in \{\star, +, \bullet\}\} \\
& \cup \{h(t) \,|\, \exists\, t \in \mathrm{Sub}(T) \text{ tal que } \mathrm{TOP}(u) = \circ, t \in \mathrm{DS}_\circ(u), \quad \circ \in \{\star, +\}\} \\
& \cup \{\mathsf{inv}_\circ(t) \,|\, \exists\, u \in \mathrm{Sub}(T) \text{ tal que } \mathrm{TOP}(u) = \circ, \quad t \in \mathrm{DS}_\circ(u), \quad \circ \in \{\star, +, \bullet\}\} \\
& \cup \{h(\mathsf{inv}_\circ(t)) \,|\, \exists\, u \in \mathrm{Sub}(T)(T) \text{ tal que } \mathrm{TOP}(u) = \circ, \quad t \in \mathrm{DS}_\circ(u), \quad \circ \in \{\star, +\}\}
\end{aligned}
$$

Lema 8 (Linearidade de F) O tamanho de $F(T)$ (o número de subtermos distintos) é linear no tamanho de T.

Demonstração: Observe que todos os termos em $F(T)$ estão sempre no conjunto

$$\mathrm{Sub}(T) \cup h(\mathrm{Sub}(T)) \cup \mathsf{inv}_\circ(\mathrm{Sub}(T)) \cup h(\mathsf{inv}_\circ(\mathrm{Sub}(T))),$$

para $\circ \in \{\star, +, \bullet\}$.

Portanto, o tamanho de $F(T)$ é limitado por 8 vezes o tamanho de T. □

Lema 9 (Idempotência de F) Para qualquer conjunto T de termos na forma normal, $F(F(T)) = F(T)$.

Demonstração: Pela definição de subtermos, $F(T) \subset \mathrm{Sub}(F(T))$.

Por outro lado, $\mathrm{Sub}(F(T)) \subset F(F(T))$, pela definição de F. Assim, $F(T) \subset F(F(T))$.

Afim de provar que $F(F(T)) \subset F(T)$, tome $t \in F(F(T))$. Para mostrar que $t \in F(T)$ os seguintes casos serão analisados:

Caso 1:

Observe primeiramente que:

$$\begin{aligned}
\mathrm{Sub}(F(T)) \quad &= \mathrm{Sub}(\mathrm{Sub}(T)) \\
&\cup \mathrm{Sub}(\{h(u) \,|\, u \in \mathrm{Sub}(T), \mathrm{TOP}(u) = +\}) \\
&\cup \mathrm{Sub}(\{h(\mathsf{inv}_+(u) \,|\, u \in \mathrm{Sub}(T), \mathrm{TOP}(u) = +\}) \\
&\cup \mathrm{Sub}(\{\mathsf{inv}_\circ(u) \,|\, u \in \mathrm{Sub}(T), \mathrm{TOP}(u) = \circ, \quad \circ \in \{\star, +, \bullet\}\}) \\
&\cup \mathrm{Sub}(\{h(u) \,|\, \exists\, v \in \mathrm{Sub}(T) \text{ tal que } \mathrm{TOP}(v) = \circ, u \in \mathrm{DS}_\circ(v), \quad \circ \in \{\star, +\}\}) \\
&\cup \mathrm{Sub}(\{\mathsf{inv}_\circ(u) \,|\, \exists\, v \in \mathrm{Sub}(T) \text{ tal que } \mathrm{TOP}(v) = \circ, \quad u \in \mathrm{DS}_\circ(v), \quad \circ \in \{\star, +, \bullet\}\}) \\
&\cup \mathrm{Sub}(\{h(\mathsf{inv}_\circ(u) \,|\, \exists\, v \in \mathrm{Sub}(T) \text{ tal que } \mathrm{TOP}(v) = \circ, \quad u \in \mathrm{DS}_\circ(v), \quad \circ \in \{\star, +\}\})
\end{aligned}$$

Caso 1.1: $t \in \mathrm{Sub}(\mathrm{Sub}(T))$

Novamente, pela definição de subtermos, $\mathrm{Sub}(T) \subseteq \mathrm{Sub}(\mathrm{Sub}(T))$. Por outro lado,

$$\mathrm{Sub}(\mathrm{Sub}(T)) = \bigcup_{t' \in \mathrm{Sub}(T)} \mathrm{Sub}(t')$$

.

Para cada $t' \in \mathrm{Sub}(T)$ tem-se que $\mathrm{Sub}(t') \subseteq \mathrm{Sub}(T)$. Então $\mathrm{Sub}(\mathrm{Sub}(T)) \subseteq \mathrm{Sub}(T)$ e assim, $\mathrm{Sub}(\mathrm{Sub}(T)) = \mathrm{Sub}(T)$.

Logo, $t \in \mathrm{Sub}(T)$ e então, $t \in F(T)$.

Caso 1.2: $t \in \mathrm{Sub}(\{h(u) \,|\, u \in \mathrm{Sub}(T), \mathrm{TOP}(u) = +\})$

Neste caso, $t \in \mathrm{Sub}(h(u))$. Como $\mathrm{TOP}(h(u)) = \bullet$, segue pela definição de subtermos, que $\mathrm{DS}_\bullet(h(u)) \subseteq \mathrm{Sub}(h(u))$.

Mas $\mathrm{DS}_\bullet(h(u)) = \{h(v') \,|\, v' \in \mathrm{DS}_+(u)\}$. Por hipótese, $u \in \mathrm{Sub}(T)$ e $\mathrm{TOP}(u) = +$, então existem duas possibilidades para u:

1. $u = u_1 + \ldots + u_n$, com $n \geq 1$ e $u_1, \ldots, u_n$ termos na forma normal.

   Por definição, $\mathrm{DS}_+(u) = \mathrm{DS}_+(u_1 + \ldots + u_n) = \mathrm{DS}_+(u_1) \cup \ldots \cup \mathrm{DS}_+(u_n)$. Observe que apenas o caso onde $\mathrm{TOP}(u_i) \neq +$, para todo i, será analisado, já que quando $\mathrm{TOP}(u_i) = +$ basta que os subtermos de decomposição de u_i sejam calculados até que todos os subtermos mais internos u_{i_j} sejam tais que $\mathrm{TOP}(u_{i_j}) \neq +$

   Por definição, como $\mathrm{TOP}(u_i) \neq +$ segue que $\mathrm{DS}_+(u_i) = \{u_i\}$ e portanto, $\mathrm{DS}_+(u) = \{u_1, \ldots, u_n\}$.

   Logo $\mathrm{DS}_\bullet(h(u)) = \{h(u_1), \ldots, h(u_n)\}$. Assim,

   $$\mathrm{Sub}(h(u)) = \{h(u), h(u_1), \ldots, h(u_n)\} \cup \bigcup_{i=1}^{n} \mathrm{Sub}(u_i)$$

   Se $t = h(u)$ então $t \in F(T)$, pois $u \in \mathrm{Sub}(T)$ e $\mathrm{TOP}(u) = +$.

   Se $t = h(u_i)$, para algum i, então

   $$t \in \{h(v) \,|\, \exists u \in \mathrm{Sub}(T), \mathrm{TOP}(u) = + \text{ e } v \in \mathrm{DS}_+(u)\},$$

   pois $u_i \in \mathrm{DS}_+(u)$. Logo, $t \in F(T)$.

   Se $t \in \mathrm{Sub}(T)(u_i)$ então $t \in \mathrm{Sub}(T) \subseteq F(T)$, pois $u_i \in \mathrm{Sub}(u) \subseteq \mathrm{Sub}(T)$.

2. $u = J_+(u_1 + \ldots + u_n)$, com $n \geq 1$ e $u_1, \ldots, u_n$ termos na forma normal.

   Pela definição de subtermos de decomposição,

   $$\mathrm{DS}_+(u) = \mathrm{DS}_+(J_+(u_1 + \ldots + u_n)) = \{J_+(v) | v \in \mathrm{DS}_+(u_1 + \ldots + u_n)\}$$

onde $\mathrm{DS}_+(u_1 + \ldots + u_n) = \mathrm{DS}_+(u_1) \cup \ldots \cup \mathrm{DS}_+(u_n)$. Novamente, apenas o caso $\mathrm{TOP}(u_i) \neq +$ será analisado.

Dessa forma,

$$\mathrm{DS}_+(u) = \mathrm{DS}_+(J_+(u_1 + \ldots + u_n)) = \{J_+(u_1), J_+(u_2), \ldots, J_+(u_n)\},$$

donde segue que

$$\mathrm{DS}_\bullet(h(u)) = \{h(J_+(u_1)), \ldots, h(J_+(u_n))\}.$$

Assim,

$$\mathrm{Sub}(h(u)) = \{h(u), h(J_+(u_1)), \ldots, h(J_+(u_n))\} \cup \bigcup_{i=1}^{n} \mathrm{Sub}(J_+(u_i))$$

Se $t = h(u)$ então $t \in F(T)$, pois $u \in \mathrm{Sub}(T)$ e $\mathrm{TOP}(u) = +$.

Se $t = h(J_+(u_i))$, para algum i, então

$$t \in \{h(\mathsf{inv}_+(v) \mid \exists u \in \mathrm{Sub}(T), \mathrm{TOP}(u) = +) \text{ e } v \in \mathrm{DS}_+(u)\},$$

pois $J_+(u_i) \in \mathrm{DS}_+(u)$. Logo, $t \in F(T)$.

Se $t \in \mathrm{Sub}(J_+(u_i))$, para algum i, então $t \in \mathrm{Sub}(T)$, já que

$$J_+(u_i) \in \mathrm{DS}_+(u) \subseteq \mathrm{Sub}(u) \subseteq \mathrm{Sub}(T).$$

Logo, $t \in F(T)$.

Caso 1.3: $t \in \mathrm{Sub}(\{h(\mathsf{inv}_+(u)) \mid u \in \mathrm{Sub}(T), \mathrm{TOP}(u) = +\})$

Neste caso, $t \in \mathrm{Sub}(h(\mathsf{inv}_+(u))$. Como $\mathrm{TOP}(h(\mathsf{inv}_+(u))) = \bullet$, segue pela definição de subtermos que $\mathrm{DS}_\bullet(h(\mathsf{inv}_+(u)) \subseteq \mathrm{Sub}(h(\mathsf{inv}_+(u))$.

Mas $\mathrm{DS}_\bullet(h(\mathsf{inv}_+(u)) = \{h(v') \mid v' \in \mathrm{DS}_+(J_+(u))\}$.

Por hipótese, $u \in \mathrm{Sub}(T)$ e $\mathrm{TOP}(u) = +$, como no Caso 1.2, temos duas possíveis formas para u:

1. $u = u_1 + \ldots + u_n$, com $n \geq 1$ e $u_1, \ldots, u_n$ termos na forma normal.

   Como no Caso 1.2, segue que $\mathrm{DS}_+(J_+(u)) = \{J_+(u_1), \ldots, J_+(u_n)\}$. Mais ainda, $\mathrm{DS}_+(h(\mathsf{inv}_+(u))) = \mathrm{DS}_+(h(J_+(u)\ \downarrow)) = \mathrm{DS}_+(h(J_+(u)))$, pois u é um termo na forma normal.

   Dessa forma,

$$\mathrm{DS}_\bullet(h(\mathsf{inv}_+(u))) = \{h(J_+(u_1)), \ldots, h(J_+(u_n))\}$$

   donde segue que

$$\begin{aligned}\mathrm{Sub}(h(\mathrm{inv}_+(u))) = \ & \{h(\mathsf{inv}_+(u)), h(J_+(u_1)), \ldots, h(J_+(u_n)), J_+(u_1), \ldots, J_+(u_n)\} \cup \\ & \textstyle\bigcup_{i=1}^{n} \mathrm{Sub}(u_i)\end{aligned}$$

   Se $t = h(\mathsf{inv}_+(u))$ então $t \in F(T)$, pois $u \in \mathrm{Sub}(T)$ e $\mathrm{TOP}(u) = +$.

   Se $h(\mathsf{inv}_+(u_i))$, para algum i, então

$$t \in \{h(\mathsf{inv}_+(v)) \,|\, \exists u \in \mathrm{Sub}(T), \mathrm{TOP}(u) = + \text{ e } v \in \mathrm{DS}_+(u)\} \subseteq F(T),$$

   pois $u_i \in \mathrm{DS}_+(u)$. Logo, $t \in F(T)$

   Agora, se $t = J_+(u_i)$, para algum i, então

$$t \in \{\mathsf{inv}_+(u_i) \,|\, \exists u \in \mathrm{Sub}(T) \text{ tal que } \mathrm{TOP}(u) = +, v \in \mathrm{DS}_+ u\},$$

   pois $u_i \in \mathrm{DS}_+(u)$. Logo, $t \in F(T)$.

   Finalmente, quando $t \in \mathrm{Sub}(u_i)$ então $t \in F(T)$, pois

$$u_i \in \mathrm{Sub}(u) \subseteq \mathrm{Sub}(T) \subseteq F(T).$$

2. $u = J_+(u_1 + \ldots + u_n)$, com $n \geq 1$ e $u_1, \ldots, u_n$ termos na forma normal.

   Observe que

$$\begin{aligned} \mathrm{DS}_\bullet(h(\mathsf{inv}_+(u))) &= \mathrm{DS}_\bullet(h(J_+(u))\downarrow) \\ &= \mathrm{DS}_\bullet(h(J_+(J_+(u_1 + \ldots + u_n))\downarrow)) \\ &= \mathrm{DS}_\bullet(h(u_1 + \ldots + u_n)). \end{aligned}$$

   Como nos caso anteriores, suponha que $\mathrm{TOP}(u_i) \neq +$, para todo i. Então

$$\begin{aligned} \mathrm{DS}_+(\mathsf{inv}_+(u)) &= \mathrm{DS}_+((J_+(u))\downarrow) \\ &= \mathrm{DS}_+(u_1 + \ldots + u_n) \\ &= \{u_1, \ldots, u_n\} \end{aligned}$$

   donde segue que

$$\mathrm{DS}_\bullet(h(\mathsf{inv}_+(u))) = \{h(v) \,|\, v \in \mathrm{DS}_+((\mathsf{inv}_+(u)))\} = \{h(u_1), \ldots, h(u_n)\}$$

   Logo,

$$\mathrm{Sub}(h(\mathsf{inv}_+(u))) = \{h(\mathsf{inv}_+(u)), h(u_1), \ldots, h(u_n)\} \cup \bigcup_{i=1}^{n} \mathrm{Sub}(u_i).$$

   Analogamente ao Caso 1.2, pode-se concluir que $t \in F(T)$.

Caso 1.4: $t \in \mathrm{Sub}(\{\mathsf{inv}_\circ(u) \,|\, u \in \mathrm{Sub}(T), \mathrm{TOP}(u) = \circ, \circ \in \{\star, +, \bullet\}\})$.

Neste caso, $t \in \mathrm{Sub}(\mathsf{inv}_\circ(u))$. Como $\mathrm{TOP}(\mathsf{inv}_\circ(u)) = \circ$, pela definição de subtermos, segue que $\mathrm{DS}_\circ(\mathsf{inv}_\circ(u)) \subset \mathrm{Sub}(\mathsf{inv}_\circ(u))$.

Por outro lado, como $\mathrm{TOP}(u) = \circ$, $\circ \in \{\star, +, \bullet\}$, u pode ter uma das seguintes formas:

1. $u = u_1 \circ \ldots \circ u_n$, com $n \geq 1$ e $u_1, \ldots, u_n$ termos na forma normal.

   Suponha que $\mathrm{TOP}(u_i) \neq \circ$, então $\mathrm{DS}_\circ(u) = \{u_1, \ldots, u_n\}$ donde segue que

$$\mathrm{DS}_\circ(\mathsf{inv}_\circ(u)) = \{\mathsf{inv}_\circ(u_1), \ldots, \mathsf{inv}_\circ(u_n)\}.$$

Portanto,

$$\mathrm{Sub}(\mathsf{inv}_\circ(u)) = \{\mathsf{inv}_\circ(u), \mathsf{inv}_\circ(u_1), \ldots, \mathsf{inv}_\circ(u_n)\} \cup \bigcup_{i=1}^{n} \mathrm{Sub}(u_i).$$

Se $t = \mathsf{inv}_\circ(u)$ então $t \in F(T)$, pois $u \in \mathrm{Sub}(T)$ e $\mathrm{TOP}(u) = \circ$.

Agora, se $t = \mathsf{inv}_\circ(u_i)$, para algum i, então

$$t \in \{\mathsf{inv}_\circ(v) \,|\, \exists u \in \mathrm{Sub}(T) \text{ tal que } \mathrm{TOP}(u) = \circ, v \in \mathrm{DS}_\circ(u), \circ \in \{\star, +, \bullet\}\},$$

pois $u_i \in \mathrm{DS}_\circ(u)$. Assim, $t \in F(T)$.

Finalmente, se $t \in \mathrm{Sub}(u_i)$, para algum i, então $t \in \mathrm{Sub}(T)$, pois

$$u_i \in \mathrm{DS}_\circ(u) \subseteq \mathrm{Sub}(u) \subseteq \mathrm{Sub}(T),$$

donde segue que $\mathrm{Sub}(u_i) \subseteq \mathrm{Sub}(T)$. Assim, $t \in F(T)$.

2. $u = J_\circ(u_1 \circ \ldots \circ u_n)$, com $n \geq 1$ e $u_1, \ldots, u_n$ termos na forma normal e tais que $\mathrm{TOP}(u_1 \circ \ldots \circ u_n) = \circ$.

   Suponha $\mathrm{TOP}(u_i) \neq \circ$, então

$$\mathrm{DS}_\circ(u) = \mathrm{DS}_\circ(J_\circ(u_1 \circ \ldots \circ u_n)) = \{J_\circ(u_1), \ldots, J_\circ(u_n)\},$$

   donde segue que

$$\begin{aligned} \mathrm{DS}_\circ(\mathsf{inv}_\circ(u)) &= \mathrm{DS}_\circ(J_\circ(u)\downarrow) \\ &= \mathrm{DS}_\circ(J_\circ(J_\circ(u_1 \circ \ldots \circ u_n))\downarrow) \\ &= \mathrm{DS}_\circ(u_1 \circ \ldots \circ u_n) \\ &= \{u_1, \ldots, u_n\}. \end{aligned}$$

   Portanto,

$$\mathrm{Sub}(\mathsf{inv}_\circ(u)) = \{\mathsf{inv}_\circ(u)\} \cup \bigcup_{i=1}^{n} \mathrm{Sub}(u_i)$$

Se $t = \mathsf{inv}_\circ(u)$, segue que $t \in F(T)$, pois $u \in \mathrm{Sub}(T)$, $\mathrm{TOP}(u) = \circ$ e $\circ \in \{\star, +\}$.

Agora, se $t \in \mathrm{Sub}(u_i)$ para algum i, segue que $t \in \mathrm{Sub}(T)$, o que implica que $t \in F(T)$ pois

$$u_i \in \mathrm{Sub}(u) \subseteq \mathrm{Sub}(T) \subseteq F(T).$$

3. Quando $u \in \mathrm{Sub}(T)$ tal que $\mathrm{TOP}(u) = \bullet$, u pode ter a forma $u = h(u')$, tal que $u' \in \mathrm{Sub}(T)$ e $\mathrm{TOP}(u') = +$.

   Observe que

$$\mathrm{DS}_\bullet(\mathsf{inv}_\bullet(u)) = \mathrm{DS}_\bullet(\mathsf{inv}_\bullet(h(u'))) = \mathrm{DS}_\bullet(h(\mathsf{inv}_+(u'))).$$

   Assim, se $t \in \mathrm{Sub}(\mathsf{inv}_\bullet(u)) = \mathrm{Sub}(h(\mathsf{inv}_\bullet\mathsf{inv}_+(u')))$ então, pelo Caso 1.3, pode-se concluir que $t \in F(T)$.

Caso 1.5: $t \in \mathrm{Sub}(\{h(u) \mid \exists\, v \in \mathrm{Sub}(T)$ tal que $\mathrm{TOP}(v) = \circ, u \in \mathrm{DS}_\circ(v), \quad \circ \in \{\star, +\}\})$

Neste caso, $t \in \mathrm{Sub}(h(u))$.

Observe que, pela definição de subtermos, $\mathrm{TOP}(v) = \circ$ implica em $\mathrm{DS}_\circ(v) \in \mathrm{Sub}(v)$. Além disso, $u \in \mathrm{Sub}(T)$ pois $\mathrm{Sub}(v) \in \mathrm{Sub}(T)$.

Inicialmente, suponha que $\mathrm{TOP}(u) = +$.

Pelo Caso 1.2, $t \in F(T)$ sempre que $t \in \mathrm{Sub}(h(u))$.

Agora, para $\mathrm{TOP}(u) \neq +$ tem-se que $\mathrm{TOP}(h(u)) = h$ e assim,

$$\mathrm{Sub}(h(u)) = \{h(u)\} \cup \mathrm{Sub}(u).$$

Quando $t = h(u)$ segue que $t \in F(T)$ pois, por hipótese, existe $v \in \mathrm{Sub}(T)$ tal que $u \in \mathrm{DS}_\circ(v)$.

Caso 1.6: $t \in \mathrm{Sub}(\{\mathsf{inv}_\circ(u) \mid \exists\, v \in \mathrm{Sub}(T)$ tal que $\mathrm{TOP}(v) = \circ, u \in \mathrm{DS}_\circ(v), \circ \in \{\star, +, \bullet\}\})$

Neste caso, $t \in \mathrm{Sub}(\mathsf{inv}_\circ(u))$. Além disso, como no caso anterior, $u \in \mathrm{Sub}(T)$.

Quando $\mathrm{TOP}(u) = \circ$, pelo Caso 1.4 segue que $t \in F(T)$.

Suponha que $\mathrm{TOP}(u) \neq \circ$. Então $\mathrm{TOP}(\mathsf{inv}_\circ(u)) \neq \circ$ e assim,

$$\mathrm{Sub}(\mathsf{inv}_\circ(u)) = \{\mathsf{inv}_\circ(u) \cup \mathrm{Sub}(u)\}\,.$$

Se $t = \mathsf{inv}_\circ(u)$ então $t \in F(T)$ pois, por hipótese, existe $v \in \mathrm{Sub}(T)$ tal que $u \in \mathrm{DS}_\circ(v)$.

Agora, se $t \in \mathrm{Sub}(u)$, como no caso anterior, $t \in F(T)$.

Caso 1.7: $t \in \mathrm{Sub}(\{h(\mathsf{inv}_\circ(u)) \,|\, \exists\, v \in \mathrm{Sub}(T)$ tal que $\mathrm{TOP}(v) = \circ, u \in \mathrm{DS}_\circ(v), \circ \in \{\star, +, \}\})$

Neste caso $t \in \mathrm{Sub}(h(\mathsf{inv}_\circ(u)))$. Como no caso anterior, $u \in \mathrm{Sub}(T)$.

Quando $\circ = +$ e $\mathrm{TOP}(u) = +$, segue pelo Caso 1.3 que $t \in F(T)$.

Suponha que $\circ = \star$ e $\mathrm{TOP}(u) = \star$. Então,

$$\mathrm{Sub}(h(\mathsf{inv}_\star(u))) = \{h(\mathsf{inv}_\star(u))\} \cup \mathrm{Sub}(\mathsf{inv}_\star(u)).$$

Se $t = h(\mathsf{inv}_\star(u))$ então $t \in F(T)$ pois, por hipótese, existe $v \in \mathrm{Sub}(T)$, tal que $u \in \mathrm{DS}_\star(v)$.

Por outro lado, se $t \in \mathrm{Sub}(\mathsf{inv}_\star(u))$ então, pelo Caso 1.4, $t \in F(T)$.

Suponha, agora, que $\circ \in \{\star, +\}$ e $\mathrm{TOP}(u) \neq \circ$.

Então,

$$\mathrm{Sub}(h(\mathsf{inv}_\circ(u))) = \{h(\mathsf{inv}_\circ(u), \mathsf{inv}_\circ(u))\} \cup \mathrm{Sub}(u).$$

Analogamente aos casos anteriores, pode-se concluir que $t \in F(T)$.

Caso 2: $t \in \{h(u) \,|\, u \in \mathrm{Sub}(F(T)),\ \ \mathrm{TOP}(u) = +\}\,.$

Neste caso, $t = h(u)$. Além disso, como $u \in \mathrm{Sub}(F(T))$, segue do Caso 1 que $u \in F(T)$.

Como $\mathrm{TOP}(u) = +$, $u \in \mathrm{Sub}(T)$ ou $u = \mathsf{inv}_+(v)$ com $v \in \mathrm{Sub}(T)$ e $\mathrm{TOP}(v) = +$.

No primeiro caso, segue facilmente que $t \in F(T)$, já que $t = h(u)$ com $u \in \mathrm{Sub}(T)$ e $\mathrm{TOP}(u) = +$.

No último caso, $t = h(u) = h(\mathsf{inv}_+(v))$ com $v \in \mathrm{Sub}(T)$ e $\mathrm{TOP}(v) = +$, donde segue que $t \in F(T)$.

Logo, $t \in F(T)$

Caso 3: $t \in \{h(\mathsf{inv}_+(u) | u \in \mathrm{Sub}(F(T)),\ \ \mathrm{TOP}(u) = +\}$

Neste caso, $t = h(\mathsf{inv}_+(u))$.

Novamente, como $u \in F(T)$ e $\mathrm{TOP}(u) = +$, segue que $u \in \mathrm{Sub}(T)$ ou $u = \mathsf{inv}_+(v)$ com $v \in \mathrm{Sub}(T)$ e $\mathrm{TOP}(v) = +$.

Do primeiro caso, segue que $t = h(\mathsf{inv}_+(u)) \in F(T)$, pois $u \in \mathrm{Sub}(T)$ e $\mathrm{TOP}(u) = +$.

Do último caso, $t = h(\mathsf{inv}_+(u)) = h(\mathsf{inv}_+(\mathsf{inv}_+(v))) = h(v)$ e então $t \in F(T)$, pois $v \in \mathrm{Sub}(T)$ e $\mathrm{TOP}(v) = +$.

Logo, $t \in F(T)$

Caso 4: $t \in \{\mathsf{inv}_\circ(u) \,|\, u \in \mathrm{Sub}(F(T)),\ \mathrm{TOP}(u) = \circ, \circ \in \{\star, +, \bullet\}\}$

Neste caso, $t = \mathsf{inv}_\circ(u)$. Novamente, como $u \in F(T)$ e $\mathrm{TOP}(u) = \circ, \circ \in \{\star, +\}$, segue que $u \in \mathrm{Sub}(T)$ ou $u = \mathsf{inv}_\circ(v)$ com $v \in \mathrm{Sub}(T)$, $\mathrm{TOP}(v) = \circ$ ou ainda, $u = h(v)$ com $v \in \mathrm{Sub}$ e $\mathrm{TOP}(v) = +$ (para $\circ = \bullet$).

Do primeiro caso, segue que $t \in F(T)$.

Do segundo caso, segue que $t = \mathsf{inv}_\circ(u) = \mathsf{inv}_\circ(\mathsf{inv}_\circ(v)) = v \in \mathrm{Sub}(T)$.

Finalmente, do último caso segue que $t = \mathsf{inv}_\bullet(u) = \mathsf{inv}_\bullet(h(v)) = h(\mathsf{inv}_+(v)) \in F(T)$.

Logo, $t \in F(T)$.

Caso 5: $t \in \{h(u) \,|\, \exists v \in \mathrm{Sub}(F(T))$ tal que $\mathrm{TOP}(v) = \circ, u \in \mathrm{DS}_\circ(v), \circ \in \{\star, +\}\}$.

Neste caso, $t = h(u)$. Novamente, como $v \in F(T)$ e $\mathrm{TOP}(v) = \circ$, segue que $v \in \mathrm{Sub}(T)$ ou $v = \mathsf{inv}_\circ(w)$, com $w \in \mathrm{Sub}(T), \mathrm{TOP}(w) = \circ$.

No primeiro caso, segue diretamente que $t \in F(T)$.

Para o último caso, inicialmente, observe que $\mathsf{inv}_\circ(v) = w \in \mathrm{Sub}(T)$ e também que $\mathrm{TOP}(\mathsf{inv}_\circ(v)) = \circ, \circ \in \{\star, +\}$. Além disso, como $u \in \mathrm{DS}_\circ(v)$ então $\mathsf{inv}_\circ(u) \in \mathrm{DS}_\circ(\mathsf{inv}_\circ(v))$.

Então,

$$t = h(u) = h(\mathsf{inv}_\circ(\mathsf{inv}_\circ(u))) \in F(T).$$

Isto é, $t \in F(T)$.

Caso 6: $t \in \{\mathsf{inv}_\circ(u) \,|\, \exists v \in \mathrm{Sub}(F(T))$ tal que $\mathrm{TOP}(v) = \circ, u \in \mathrm{DS}_\circ(v), \circ \in \{\star, +, \bullet\}\}$.

Neste caso, $t = \mathsf{inv}_\circ(u)$. Novamente, como $v \in F(T)$ e $\mathrm{TOP}(v) = \circ$, segue que $v \in \mathrm{Sub}(T)$ ou $v = \mathsf{inv}_\circ(w)$ com $w \in \mathrm{Sub}(T)$ e $\mathrm{TOP}(w) = \circ$.

No primeiro caso, segue diretamente que $t \in F(T)$.

Para o segundo caso, observe que $u \in \mathrm{DS}_\circ(v)$ implica em $\mathsf{inv}_\circ(u) \in \mathrm{DS}_\circ(\mathsf{inv}_\circ(v))$.

Por sua vez, $\mathsf{inv}_\circ(v) = w \in \mathrm{Sub}(T)$. Além disso, como $\mathrm{TOP}(\mathsf{inv}_\circ(v)) = \circ$ segue que $\mathrm{DS}_\circ(\mathsf{inv}_\circ(v)) \subseteq \mathrm{Sub}(\mathsf{inv}_\circ(v)) \subseteq \mathrm{Sub}(T)$. Assim, $t = \mathsf{inv}_\circ(u) \in \mathrm{Sub}(T)$.

Logo, $t \in F(T)$.

Caso 7: $t \in \{h(\mathsf{inv}_\circ(u)) \,|\, \exists v \in \mathrm{Sub}(F(T))$ tal que $\mathrm{TOP}(v) = \circ, u \in \mathrm{DS}_\circ(v), \circ \in \{\star, +\}\}$.

Neste caso, $t = h(\mathsf{inv}_\circ(u))$. Novamente, como $v \in F(T)$ e $\mathrm{TOP}(v) = \circ$ segue que $v \in \mathrm{Sub}(T)$ ou $v = \mathsf{inv}_\circ(w) \in \mathrm{Sub}(T)$ com $\mathrm{TOP}(w) = \circ$.

Do primeiro caso, segue diretamente que $t \in F(T)$.

Para o último caso, como $u \in \mathrm{DS}_\circ(v)$ então $\mathsf{inv}_\circ(u) \in \mathrm{DS}_\circ(\mathsf{inv}_\circ(v))$. Além disso, $\mathsf{inv}_\circ(v) = w \in \mathrm{Sub}(T)$ e $\mathrm{TOP}(\mathsf{inv}_\circ(v)) = \circ \in \{+, \star\}$.

Assim $t = h(\mathsf{inv}_\circ(u)) \in F(T)$. □

Afim de provar que o sistema de inferência $\mathcal{I}_1 \cup \mathcal{I}_2$ tem a propriedade de localidade, serão consideradas provas normais de t que são minimais no tamanho e então, por indução no número de regras segue a demonstração deste fato. Dessa forma, o problema se transforma em uma série de casos, recaindo principalmente nos lemas 4 e 5 e lemas técnicos que cuidadosamente investigam casos em que existe uma decomposição.

A prova será normalizada de acordo com as regras dadas na Figura 2. Essas regras são (fortemente) terminantes (mas não confluentes).

$$\dfrac{\dfrac{h(t_1) \quad t_2 \ldots t_n}{h(t_1 \star \ldots \star t_n)\downarrow}\,\mathsf{Exp}_1 \qquad u_1 \ldots u_m}{h(t_1 \star t_2 \ldots \star u_2 \star \ldots \star u_m)\downarrow}\,\mathsf{Exp}_1 \quad \Rightarrow \quad \dfrac{h(t_1) \quad t_2 \ldots t_n u_2 \ldots u_m}{h(t_1 \star t_2 \ldots \star u_2 \star \ldots \star u_m)\downarrow}\,\mathsf{Exp}_1$$

$$\dfrac{\dfrac{\mathsf{exp}(t_1, t_2) \quad t_3 \ldots t_n}{\mathsf{exp}(t_1, t_2 \star \ldots \star t_n)\downarrow}\,\mathsf{Exp}_2 \qquad u_3 \ldots u_m}{\mathsf{exp}(t_1, t_2 \star \ldots \star t_n \star u_3 \ldots \star u_m)\downarrow}\,\mathsf{Exp}_2 \quad \Rightarrow \quad \dfrac{\mathsf{exp}(t_1, t_2) \quad t_3 \ldots t_n u_3 \ldots u_m}{\mathsf{exp}(t_1, t_2 \ldots \star t_n \star u_3 \star \ldots \star u_m)\downarrow}\,\mathsf{Exp}_2$$

$$\dfrac{h(t_1) t_2 \ldots \quad \dfrac{u_1 \ldots u_m}{(u_1 \star \ldots \star u_m)\downarrow}\,\mathsf{R}_\star \quad \ldots t_n}{h(t_1 \star t_2 \star \ldots \star u_1 \star \ldots \star u_m \star \ldots t_n)\downarrow}\,\mathsf{Exp}_1 \quad \Rightarrow \quad \dfrac{h(t_1) t_2 \ldots u_1 \ldots u_m \ldots t_n}{h(t_1 \star t_2 \star \ldots \star u_1 \star \ldots \star u_m \star \ldots t_n)\downarrow}\,\mathsf{Exp}_1$$

$$\dfrac{\mathsf{exp}(t_1, t_2) \ldots \quad \dfrac{u_1 \ldots u_m}{(u_1 \star \ldots \star u_m)\downarrow}\,\mathsf{R}_\star \quad \ldots t_n}{\mathsf{exp}(t_1, t_2 \star \ldots \star u_1 \star \ldots \star u_m \star \ldots t_n)\downarrow}\,\mathsf{Exp}_2 \quad \Rightarrow \quad \dfrac{\mathsf{exp}(t_1, t_2) \ldots u_1 \ldots u_m \ldots t_n}{\mathsf{exp}(t_1, t_2 \star \ldots \star u_1 \star \ldots \star u_m \star \ldots \star t_n)\downarrow}\,\mathsf{Exp}_2$$

$$\dfrac{\dfrac{t_1 \quad t_2}{\mathsf{exp}(t_1, t_2)}\,\mathsf{Exp}_3 \qquad t_3 \ldots t_n}{\mathsf{exp}(t_1, t_2 \star \ldots \star t_n)\downarrow}\,\mathsf{Exp}_2 \quad \Rightarrow \quad \dfrac{t_1 \qquad \dfrac{t_2 \ldots t_n}{(t_2 \star \ldots \star t_n)\downarrow}\,\mathsf{R}_\star}{\mathsf{exp}(t_1, t_2 \star \ldots \star t_n)\downarrow}\,\mathsf{Exp}_3$$

$$\dfrac{t_1 \ldots \quad \dfrac{u_1 \ldots u_m}{(u_1 \circ \ldots \circ u_m)\downarrow}\,\mathsf{R}_\circ \quad \ldots t_n}{t_1 \circ \ldots \circ u_1 \circ \ldots \circ u_m \circ \ldots \circ t_n)\downarrow}\,\mathsf{R}_\circ \quad \Rightarrow \quad \dfrac{t_1 \ldots u_1 \ldots u_m \ldots t_n}{t_1 \circ \ldots \circ u_1 \circ \ldots \circ u_m \circ \ldots \circ t_n)\downarrow}\,\mathsf{R}_\circ$$

$$\dfrac{\dfrac{u_1 \ldots u_m}{(u_1 + \ldots + u_m)\downarrow}\,\mathsf{R}_+}{h((u_1 + \ldots + u_m)\downarrow)}\,\mathsf{R}_h \quad \Rightarrow \quad \dfrac{\dfrac{u_1}{h(u_1)}\,\mathsf{R}_h \qquad \dfrac{\ldots u_m}{h(u_m)}\,\mathsf{R}_h}{h((u_1 + \ldots + u_m)\downarrow)}\,\mathsf{R}_\bullet$$

$$\dfrac{\dfrac{u_1 \ldots u_m}{(u_1 \circ \ldots \circ u_m)\downarrow}\,\mathsf{R}_\circ}{J_\circ((u_1 \circ \ldots \circ u_m)\downarrow)}\,\mathsf{R}_{J_\circ} \quad \Rightarrow \quad \dfrac{\dfrac{u_1}{J_\circ(u_1)\downarrow}\,\mathsf{R}_{J_\circ} \qquad \dfrac{\ldots u_m}{J_\circ(u_m)\downarrow}\,\mathsf{R}_{J_\circ}}{J_\circ((u_1 \circ \ldots \circ u_m)\downarrow))}\,\mathsf{R}_\circ$$

$$\dfrac{\dfrac{u}{h(u)}\,\mathsf{R}_h \qquad v_1 \ldots v_n}{h(u \star v_1 \star \ldots \star v_n)\downarrow}\,\mathsf{Exp}_1 \quad \Rightarrow \quad \dfrac{u \quad v_1 \ldots v_n}{(u \star v_1 \star \ldots \star v_n)\downarrow}\,\mathsf{R}_\star}{h((u \star v_1 \star \ldots \star v_n)\downarrow)}\,\mathsf{R}_h$$

Figura 2. Regras de normalização de provas

A seguinte proposição pode ser estabelecida:

Proposição 2 *O sistema de inferência $\mathcal{I}_1 \cup \mathcal{I}_2$ é F-local.*

Demonstração: Considere uma prova minimal (em termos do tamanho) de t a partir do conjunto de hipóteses H. Será provado por indução no tamanho da prova que, se a última regra é uma composição então todos os termos da prova estão em $F(H) \cup F(t)$ e, se a última regra é uma decomposição então todos os termos da prova estão em $F(H)$.

No caso base, a prova consiste de um axioma apenas, e o resultado segue.

A partir de agora, a análise dos casos depende da última regra usada na prova.

Caso 1. A útima regra é R_h.

Como R_h é uma regra de composição, é preciso provar que todos os termos da prova de t estão em $F(H) \cup F(t)$.

A prova de t pode ser representada por:

$$\dfrac{\dfrac{\Pi}{H \vdash u}}{H \vdash t = h(u)\downarrow}\,(\mathsf{R}_h)$$

onde Π representa a prova $H \vdash u$.

Se $TOP(t) = \bullet$ então $TOP(u) = +$ e por normalização de prova u não pode ser obtido por R_+. Dessa forma, u deve ser obtido por uma decomposição ou então por uma composição da forma R_{J_+}.

No primeiro caso, $u \in F(H)$, por hipótese de indução. Agora, quando u é obtido pela composição R_{J_+}, a prova pode ser representada por:

$$\dfrac{\dfrac{\dfrac{\Pi_1}{H \vdash u'}}{H \vdash u = J_+(u')\downarrow}\,(\mathsf{R}_{J_+})}{H \vdash t = h(u)\downarrow}\,(\mathsf{R}_h)$$

Por hipótese de indução, os termos da prova de u estão em $F(H) \cup F(u)$.

Note que $u = J_+(u') \downarrow = \mathsf{inv}_+(u')$, pois por minimalidade $u' \neq e_+$ e pelo fato da regra R_{J_+} ser uma composição, u' não pode ser encabeçado por J_+. Mais ainda, $TOP(u') = +$ uma vez que $TOP(u) = +$, por hipótese.

Novamente, por normalização de prova, u' não pode ser obtido por R_+ e, por minimalidade u' não pode ser obtido por R_{J_+}. Dessa forma, u' só pode ser obtido por uma decomposição ou por um axioma. Assim, por hipótese de indução, segue que $u' \in F(H)$. Além disso, como u' não pode ser encabeçado por J_+, temos que $u' \in Sub(H)$.

Portanto, em ambos os casos $u \in F(H)$. Além disso, como $TOP(u) = +$, segue que $u \in Sub(H) \cup \{\mathsf{inv}_+(v) | v \in Sub(H), TOP(v) = +\}$.

Logo $t = h(u) \in F(H)$.

Agora, suponha que $TOP(u) \neq \bullet$. Então $TOP(u) \neq +$, por normalização de prova u pode ser obtido por composições distintas de R_+, ou por decomposições.

Em ambos os casos, por hipótese de indução, $u \in F(H) \cup F(u)$.

Pela definição de F tem-se que $Sub(t) \subset F(t)$. Como $t = h(u)$ segue, pela definição de subtermos, que $u \in \mathrm{Sub}(t)$. Assim $Sub(u) \subseteq \mathrm{Sub}(t)$, ou ainda, $F(u) \subset F(t)$.

Portanto, $t \in F(H) \cup F(t)$.

Caso 2. A útima regra é uma composição $\mathsf{R}_\circ$ com $\circ \in \{+, \star, \bullet\}$.

A prova de t pode ser representada por:

$$\dfrac{\dfrac{\Pi_1}{H \vdash u_1}\,(\mathsf{R}_{f_1}) \quad \cdots \quad \dfrac{\Pi_n}{H \vdash u_n}\,(\mathsf{R}_{f_n})}{H \vdash t = (u_1 \circ u_2 \circ \ldots \circ u_n)\downarrow}\,(\mathsf{R}_\circ)$$

onde Π_i representa a prova $H \vdash u_i$, para cada i, $1 \leq i \leq n$.

Como $\mathsf{R}_\circ$ é composição, é preciso mostrar que todos os termos da prova de t estão em $F(H) \cup F(t)$.

Considere o conjunto S dos índices i tais que $TOP(u_i) = \circ$ (os casos onde $u_i = e_\circ$ podem ser eliminados pois correspondem a provas não minimais).

Pelo Lema 5, para todo $i \notin S$, ou $u_i \in DS_\circ(t)$ ou existe um índice $j \in S$ tal que $\mathsf{inv}_\circ(u_i) \in DS_\circ(u_j)$, ou então existe um índice $j \notin S$ tal que $u_j = \mathsf{inv}_\circ(u_i)$.

Desde já, observe que o último caso não acontece, pois corresponde a uma prova não minimal.

Quando $u_i \in DS_\circ(t)$, segue pela definição de subtermos que $DS_\circ(t) \subset Sub(t)$ pois $TOP(t) = \circ$ (a regra $\mathsf{R}_\circ$ é composição). Assim, $u_i \in F(t)$.

Agora, quando $\mathsf{inv}_\circ(u_i) \in DS_\circ(u_j)$ para algum índice $j \in S$, considere as seguintes situações:

i) Suponha $\circ \in \{\star, +\}$. Como $u_j \in S$, $TOP(u_j) = \circ$ e então, por normalização de prova u_j deve ser obtido por uma decomposição distinta de $\mathsf{R}_\circ$ ou por uma composição do tipo $\mathsf{R}_{J_\circ}$.

   Para u_j obtido por decomposição, segue por hipótese de indução que todos os termos da prova de u_j estão em $F(H)$. Em particular, $u_j \in F(H)$.

   Por outro lado, quando u_j é obtido pela composição $\mathsf{R}_{J_\circ}$, $u_j = J_\circ(u'_j)$ para algum termo u'_j tal que $\mathrm{TOP}(u'_j) = \circ$. Isto é,

$$\frac{H \vdash u'_j}{H \vdash u_j = J_\circ(u'_j) \downarrow = \mathsf{inv}_\circ(u'_j)}\ \mathsf{R}_{J_\circ}$$

   Por hipótese de indução, todos os termos da prova de u_j estão em $F(H) \cup F(u_j)$.

   Observe, primeiramente, que u'_j não pode ser encabeçado por $J_\circ$, caso contrário a regra $\mathsf{R}_{J_\circ}$ não seria uma composição.

   Por normalização de prova u'_j não pode ser obtido por $\mathsf{R}_\circ$ e, por minimalidade não pode ser obtido por $\mathsf{R}_{J_\circ}$. Assim u'_j é obtido por decomposição e por hipótese de indução todos os termos da sua prova estão em $F(H)$. Em particular, $u'_j \in F(H)$.

   Além disso, $TOP(u'_j) = \circ$ então $u'_j \in \mathrm{Sub}(H)$.

   Mas $u_j = \mathsf{inv}_\circ(u'_j)$ e, pela definição de F segue que $u_j \in F(H)$.

ii) Suponha, agora, que $\mathsf{inv}_\bullet(u_i) \in DS_\bullet(u_j)$ para u_j tal que $j \in S$. Dessa forma $TOP(u_j) = \bullet$ e, por normalização de prova u_j não pode ser obtido por $\mathsf{R}_\bullet$. Então, u_j

é obtido por decomposição, ou u_j é obtido por R_h ou ainda por uma composição do tipo $\mathsf{R}_{J_\bullet}$.

Do primeiro caso, segue por hipótese de indução que todos os termos da prova de u_j estão em $F(H)$. Assim, $u_j \in F(H)$.

Agora, se u_j é obtido por R_h então, pelo Caso 1, segue que $u_j \in F(H)$.

Finalmente, se u_j é obtido por um composição do tipo $\mathsf{R}_{J_\bullet}$, então $u_j = J_\bullet(u'_j)\downarrow$ para algum termo u'_j tal que $\mathrm{TOP}(u'_j) = \bullet$.

Por hipótese de indução, todos os termos da prova de u_j estão em $F(H) \cup F(u_j)$.

Além disso, por normalização de prova e por minimalidade, u'_j é obtido por decomposição ou por uma composição do tipo R_h.

Quando u'_j é obtido por decomposição, por hipótese de indução, $u'_j \in F(H)$. Dessa forma, $u'_j \in \mathrm{Sub}(H)$ ou $u'_j = h(t')$ ou então $u'_j = h(\mathsf{inv}_+(t'))$, com $t' \in \mathrm{Sub}(H)$ e $\mathrm{TOP}(t') = +$.

Se $u'_j \in \mathrm{Sub}(H)$ então $u_j = J_\bullet(u'_j)\downarrow = \mathsf{inv}_\bullet(u'_j) \in F(H)$.

Se $u'_j = h(t')$ então $u_j = J_\bullet(u'_j)\downarrow = h(\mathsf{inv}_+(u'_j)) \in F(H)$.

Se $u'_j = h(\mathsf{inv}_+(t'))$ então $u_j = h(t') \in F(H)$.

Agora, quando u'_j é obtido por R_h, então $u'_j = h(u)$ para algum termo u tal que $\mathrm{TOP}(u) = +$ e, pelo Caso 1, segue que $u'_j, u \in F(H)$. Assim, $u_j = J_\bullet(u'_j)\downarrow = h(\mathsf{inv}_+(u)) \in F(H)$.

Logo, $u_j \in F(H)$ donde segue que todos os termos da prova de u_j estão em $F(H)$.

Em todos os casos $u_j \in F(H)$ e $\mathsf{inv}_\circ(u_i) \in DS_\circ(u_j) \subset Sub(u_j)$.

Pelo Lema 9, segue que $Sub(u_j) \subset F(H)$. Além disso, de $\mathsf{inv}_\circ(u_i) \in Sub(u_j)$ pode-se concluir que $Sub(\mathsf{inv}_\circ(u_i)) \subset Sub(u_j)$ e daí, $u_i \in F(H)$.

Assim, para todo índice i, $TOP(u_i) \neq \circ$ e $u_i \in F(H) \cup F(t)$ ou $TOP(u_i) = \circ$ e $u_i \in F(H)$. Por hipótese de indução, todos os termos da prova de u_i estão em $F(H) \cup F(u_i)$.

Como $u_i \in F(H)$, segue pelo Lema 9 que $F(u_i) \subset F(H)$. Portanto, todos os termos da prova de u_i estão em $F(H)$.

Logo, todos os termos da prova de t estão em $F(H) \cup F(t)$.

Caso 3. A útima regra é $\mathsf{R}_{J_\circ}$.

A prova de t pode ser representada por:

$$\dfrac{\dfrac{\Pi}{H \vdash u}\,(\mathsf{R}_f)}{H \vdash t = J_\circ(u)\downarrow}\,(\mathsf{R}_{J_\circ})$$

Por normalização de prova, u não pode ser obtido por uma regra $\mathsf{R}_\circ$ e por minimalidade não pode ser obtido por $\mathsf{R}_{J_\circ}$.

Se $\mathrm{TOP}(u) \in \{\circ, J_\circ\}$ então u deve ser obtido por uma decomposição ou por uma composição do tipo R_h, quando $\circ = \bullet$.

Quando u é obtido por decomposição, por hipótese de indução, todos os termos da prova de u estão em $F(H)$. Em particular, $u \in F(H)$.

Agora, quando u é obtido por R_h, então $u = h(v)$ para algum v tal que $\mathrm{TOP}(v) = +$. Pelo Caso 1, $u \in F(H)$.

Se $\mathrm{TOP}(u) \notin \{\circ, J_\circ\}$ então t é obtido por uma composição $\mathsf{R}_{J_\circ}$ e $t = J_\circ(u)\downarrow = J_\circ(u)$. Novamente, por hipótese de indução, todos os termos da prova de t estão em $F(H) \cup F(t)$.

Portanto, considerando-se todos os casos, segue que todos os termos da prova de t estão em $F(H) \cup F(t)$.

Caso 4. A útima regra é uma decomposição $\mathsf{R}_\circ$ com $\circ \in \{+, \star, \bullet\}$

A prova de t pode ser representada por por:

$$\dfrac{\dfrac{\Pi_1}{H \vdash t_1}\,(\mathsf{R}_{f_1}) \quad \cdots \quad \dfrac{\Pi_n}{H \vdash t_n}\,(\mathsf{R}_{f_n})}{H \vdash t = (t_1 \circ t_2 \circ \ldots \circ t_n)\downarrow}\,(\mathsf{R}_\circ)$$

Os casos onde $t_i = e_\circ$, para algum i, serão descartados por minimalidade.

Como a regra $\mathsf{R}_\circ$ é uma decomposição, pelo Lema 6, existe uma premissa t_i tal que $t \in \mathrm{DS}_\circ(t_i)$.

Se $t_1, \ldots, t_n \in F(H)$ então, por hipótese de indução, todos os termos da prova de t estão em $F(H)$.

Agora, se existir um índice j tal que $t_j \notin F(H)$, por hipótese de indução, t_j deve ser obtido por uma composição.

Por contradição, suponha que $\mathrm{TOP}(t_j) = \circ$. Por normalização de prova ou t_j deve ser obtido por $\mathsf{R}_{J_\circ}$ ou $\circ = \bullet$ e t_j deve ser obtido por R_h.

No primeiro caso, $t_j = J_\circ(u_j)\downarrow$ para algum u_j tal que $\mathrm{TOP}(u_j) = \circ$. Novamente, por normalização de prova, u_j não pode ser obtido por $\mathsf{R}_\circ$. Isto implica que u_j é obtido por decomposição então, por hipótese de indução, todos os termos da prova de u_j estão em $F(H)$. Em particular, $u_j \in F(H)$. Assim,

$$t_j = \mathsf{inv}_\circ(u_j), \quad \text{com } u_j \in F(H),\ \mathrm{TOP}(u_j) = \circ,\ \circ \in \{\star, +\}\,.$$

Como $u_j \in F(H)$ tem-se que $u_j \in \mathrm{Sub}(H) \cup x\, \{\mathsf{inv}_\circ(u) | u \in \mathrm{Sub}(H), \mathrm{TOP}(u) = \circ \in \{\star, +\}\}$.

Observe que o segundo caso não acontece, uma vez que $u_j = \mathsf{inv}_\circ(u)$ contradiz o fato de t_j ser obtido por composição. Portanto $u_j \in \mathrm{Sub}(H)$, donde segue que $t_j \in F(H)$, o que é uma contradição.

Para $\circ = \bullet$ e t_j obtido por R_h, tem-se que $t_j = h(u_j)$ com $\mathrm{TOP}(u_j) = +$. Novamente, pelo Caso 1, $t_j \in F(H)$, o que é uma contradição.

Dessa forma, $\mathrm{TOP}(t_j) \notin \{\circ, e_\circ\}$ e por minimalidade, $t_j \neq e_\circ$ e $t_j \neq t$. Então,

$$\mathrm{TOP}(t_1 \circ \ldots \circ t_j \circ \ldots \circ t_n)\downarrow = \mathrm{TOP}(t) \neq \circ \text{ e } (t_1 \circ \ldots \circ t_{j-1} \circ t_{j+1} \circ \ldots \circ t_n)\downarrow \neq e_\circ.$$

Pela Lema 4, existe um índice $k \neq j$ tal que $\mathsf{inv}_\circ(t_j) \in \mathrm{DS}_\circ(t_k)$.

Observe que $\mathrm{TOP}(t_k) = \circ$, caso contrário $t_k = \mathsf{inv}_\circ(t_j)$, o que contradiz a minimalidade da prova de t. Repetindo o raciocínio feito para t_j segue que t_k foi obtido por decomposição e, por hipótese de indução, $t_k \in F(H)$.

Além disso, como $\mathrm{DS}_\circ(t_k) \subseteq \mathrm{Sub}(t_k) \subseteq F(H)$ então $\mathsf{inv}_\circ(t_j) \in F(H)$, o que implica $t_j \in F(H)$, uma contradição.

Logo, todos os t_i's estão em $F(H)$.

Caso 5. A última regra é uma decomposição Exp_1

$$\frac{h(t_1)t_2 \ldots t_n}{h(t_1 \star \ldots \star t_n)\downarrow}\ (\mathsf{Exp}_1)$$

Seja $u = t_1 \star \ldots \star t_n \downarrow$. Pela definição de regra de decomposição $\mathrm{TOP}(u) \neq \star$.

Por normalização de prova, $h(t_1)$ só pode ser obtido por uma composição $\mathsf{R}_\bullet$ ou por uma decomposição distinta de $\mathsf{Exp1}$. No último caso, $h(t_1) \in F(H)$. Em particular quando a regra é $\mathsf{R}_\bullet$, $\mathrm{TOP}(t_1) = +$.

Similarmente, nenhum dos t_i's ($i \geq 2$) pode ser obtido por $\mathsf{R}_\star$.

Seja u_i dado por:

$$u_i = \begin{cases} t_i, \text{ se } t_i \text{ não é obtido por } \mathsf{R}_{J_\star} \\ \mathsf{inv}_\star(t_i), \text{ caso contrário.} \end{cases}$$

Suponha que $u_i \notin F(H)$ para algum i. Por hipótese de indução, u_i é obtido por composição. Por normalização de prova, u_i não pode ser obtido por $\mathsf{R}_\star$.

Além disso, por minimalidade não pode ser obtido por $\mathsf{R}_{J_\star}$. De fato, se u_i é obtido por $\mathsf{R}_{J_\star}$ e $u_i = t_i$ então t_i seria obtido por $\mathsf{R}_{J_\star}$, o que contradiz a construção de u_i.

Por outro lado, seja $u_i = \mathsf{inv}_\star(t_i)$ e suponha que u_i foi obtido por $\mathsf{R}_{J_\star}$. Isto é

$$\frac{\dfrac{\Pi}{H \vdash t_i}\ (\mathsf{R}_{J_\star})}{H \vdash u_i = \mathsf{inv}_\star(t_i)}\ (\mathsf{R}_{J_\star})$$

E a prova de u_i conteria duas aplicações consecutivas da regra $\mathsf{R}_{J_\star}$, o que contradiz a minimalidade da prova de t.

Assim u_i é obtido por uma composição distinta de $\mathsf{R}_\star$ e de $\mathsf{R}_{J_\star}$. Isto implica que $\mathrm{TOP}(u_i) \neq \star$ e por isso $\mathrm{TOP}(t_i) \neq \star$. Mas então, pelo Lema 5, ou $t_i \in \mathrm{DS}_\star(u)$ ou existe j tal que $\mathsf{inv}_\star(t_i) \in \mathrm{DS}_\star(t_j)$ ou então $\mathsf{inv}_\star(t_j) = t_i$. Desde já, observe que o último caso não acontece, pois contradiz a minimalidade da prova de t.

Além disso, da hipótese $\mathrm{TOP}(u) \neq \star$ segue que $\mathrm{DS}_\star(u) = \{u\}$ e então $t_i = u$ o que também contradiz a minimalidade da prova de t.

Logo, para todo i, $\mathsf{inv}_\star(t_i) \in \mathrm{DS}_\star(t_j)$ e então, $\mathrm{TOP}(t_j) = \star$. Consequentemente, o u_j correspondente a t_j não pode ser obtido por composição. Por hipótese de indução, $u_j \in F(H)$.

Dessa forma, ou $u_j = t_j$ e $\mathsf{inv}_\star(t_i) \in \mathrm{DS}_\star(u_j) \subset \mathrm{Sub}(u_j)$, donde segue que $t_i \in F(H)$. Ou então, $u_j = \mathsf{inv}_\star(t_j)$ e $\mathsf{inv}_\star(t_i) \in \mathrm{DS}_\star(\mathsf{inv}_\star(t_j))$, isto é, $t_i \in \mathrm{DS}_\star(t_j) \subseteq F(H)$.

Em todos os casos, para todo i, $t_i \in F(H)$.

Pelo Lema 7, existe um i, tal que $u \in \mathrm{DS}_\star(t_i)$. Além disso, por minimalidade, $t \neq t_i$ e $t \neq h(t_i)$.

Suponha que $\mathrm{TOP}(t_i) \neq \star$. Então $\mathrm{DS}_\star(t_i) = \{t_i\}$, o que implica em $u = t_i$, donde segue que $t = h(u) = h(t_i)$, o que é uma contradição. Assim, $\mathrm{TOP}(t_i) = \star$ e por issso, $t_i \in \mathrm{Sub}(H) \cup \{\mathsf{inv}_\star(t') \,|\, t' \in \mathrm{Sub}(H), \mathrm{TOP}(H) = \star\}$. Então, $u \in \mathrm{DS}_\star(t_i) \subset F(H)$.

Logo, $t = h(u) \in F(H)$ donde segue que todos os termos da prova de t estão em $F(H)$.

Caso 6. A última regra é uma composição Exp_1

Novamente, a prova de t pode ser representada por:

$$\frac{h(t_1)t_2 \ldots t_n}{h(t_1 \star \ldots \star t_n)\downarrow}\,(\mathsf{Exp}_1)$$

onde $u = h(t_1 \star \ldots \star t_n)\downarrow$ e $\mathrm{TOP}(u) = \star$.

Analogamente ao caso anterior, segue por normalização de prova que, para todo i, $t_i \in F(H)$ ou $t_i \notin F(H)$.

Pelo Lema 5, se $t_i \notin F(H)$ então ou $\mathsf{inv}_\star(t_i) \in \mathrm{DS}_\star(u)$ ou existe um índice $j \neq i$ tal que $\mathsf{inv}_\star(t_i) \in \mathrm{DS}_\star(t_j)$.

No primeiro caso, $\mathsf{inv}_\star(t_i) \in \mathrm{DS}_\star(u) \subseteq \mathrm{Sub}(t) \subseteq F(t)$. Logo, $t_i \in F(t)$.

No segundo caso, $\mathrm{TOP}(t_j) = \star$ (caso contrário, $t_j = \mathsf{inv}_{star}(t_i)$ contradizendo a minimalidade) e então $t_j \in F(H)$. Como no caso anterior, $t_i \in F(H)$.

Para $h(t_1)$, o raciocínio é o mesmo do caso anterior: ou $\mathrm{TOP}(t_1) \neq \star$ ou $h(t_1)$ é obtido por decomposição, donde segue que $t_1 \in F(H)$.

Em todos os casos, todos os termos da prova de t estão em $F(H) \cup F(t)$.

Caso 7. A última regra é Exp_2

A prova de t pode ser representada por:

$$\frac{\mathsf{exp}(t_1, t_2)t_3 \ldots t_n}{\mathsf{exp}(t_1, t_2 \star \ldots \star t_n)\downarrow}\ \mathsf{Exp}_2$$

Seja $u = (t_2 \star \ldots \star t_n)\downarrow$.

Neste caso, $t_2, t_3, \ldots, t_n$ tem exatamente os mesmo papéis de $t_1, ...t_n$ em Exp_1. Por normalização de prova $\mathsf{exp}(t_1, t_2)$ não pode ser obtido por composição, então $\mathsf{exp}(t_1, t_2)$ é obtido por uma decomposição, e por hipótese de indução, $\mathsf{exp}(t_1, t_2) \in F(H)$. Mais ainda $\mathsf{exp}(t_1, t_2) \in \mathrm{Sub}(H)$, donde segue que $t_1, t_2 \in \mathrm{Sub}(H)$.

Agora, para cada índice i ($i > 2$), como no caso anterior, ou t_i é obtido por decomposição e $t_i \in F(H)$ ou então $t_i \neq F(H)$ e assim, $t_i \in DS_\star(u)$, pelo lema 5. Então cada premissa está ou em $F(H)$ ou em $F(t)$, donde, por hipótese de indução, segue que todos os termos da prova de t estão em $F(H) \cup F(t)$.

Caso 8. A última regra é Exp_3

A prova de t pode ser representada por:

$$\frac{H \vdash t_1 \qquad H \vdash t_2}{H \vdash t = \mathsf{exp}(t_1, t_2)}\ (\mathsf{Exp}_3)$$

Neste caso a regra é uma composição. Como $\mathsf{exp}(t_1, t_2) \in \mathrm{Sub}(t) \in F(t)$, as duas premissas estão em $\mathrm{Sub}(t)$, por hipótese de indução, todos os termos da prova de t estão em $F(H) \cup F(t)$.

Dessa forma, em todos os casos, todos os termos da prova de t estão em $F(T \cup \{t\})$, o que conclui a demonstração da proposição. □

4.2 Deducibilidade um-passo e o problema da dedução do intruso

Neste caso de estudo, a localidade do sistema de dedução $\mathcal{I}_1 \cup \mathcal{I}_2$ não é suficiente para garantir a sua decidibilidade em tempo polinomial, uma vez que, a localidade caracteriza sistemas de dedução finitos. Além disso, com a aplicação de regras $\mathsf{R}_\circ$, com $\circ \in \{+, \star, \bullet\}$ deve-se considerar todas as possibilidades de subtermos módulo AC. Porém existe, em geral, um número exponencial de subtermos módulo AC de um termo dado. A solução proposta por Shmatikov e Comon-Lundh em [CLS03], e que será utilizada aqui é usar a regra $\mathsf{R}_\circ$ com um número arbitrário de hipóteses. Desta forma, o número exponencial de subtermos pode ser evitado. Mas o conjunto de regras de inferência ainda é infinito. Será mostrado que ainda é possível obter um algoritmo polinomial implementando o teste se um termo é dedutível em um passo a partir do conjunto finito T.

Para isto, segue a definição de *deducibilidade em um passo*:

Definição 30 Um termo t é *dedutível em um passo* de um conjunto finito de termos T pelo conjunto $\mathcal{I}_1 \cup \mathcal{I}_2$ de regras de inferência se existe uma regra de inferência R_f de $\mathcal{I}_1 \cup \mathcal{I}_2$ e termos $t_1, \ldots, t_n \in T$ tais que

$$\frac{T \vdash t_1 \qquad \ldots \qquad T \vdash t_n}{T \vdash t = f(t_1, \ldots, t_n)\downarrow}\ \mathsf{R}_f$$

A propriedade de deducibilidade em um passo permite testar se um termo é dedutível em um passo de um conjunto de termos T que é dado, utilizando as regras do conjunto de regras de inferência considerado.

O seguinte lema afirma que a propriedade de deducibilidade em um passo para $\mathcal{I}_1 \cup \mathcal{I}_2$ é decidível em tempo polinomial.

Lema 10 (Polinomialidade da deducidibilidade em um passo) A propriedade de deducibilidade em um passo para o sistema $\mathcal{I}_1 \cup \mathcal{I}_2$ é decidível em tempo polinomial.

Demonstração: Seja $T = \{t_1, \ldots, t_m\}$ o conjunto finito de termos, t um termo na forma normal e $f \in \{\star, J_\star, +, J_+, \bullet, J_\bullet, h, \mathsf{exp}\}$ um símbolo de função.

Na análise de um algoritmo, para mostrar que ele roda em tempo polinomial, deve-se dar um limitante superior polinomial para cada um dos seus estágios. Para isto, são analisados os estágios individuais na descrição do algoritmo para assegurar que cada um possa ser implementado em tempo polinomial.

O algorimo de decisão que será analisado abaixo, roda sobre a entrada de tamanho $||T|| + |t| + 1 = l$, onde $||T|| = \sum_{i=1}^{m} |t_i|$ e $|f| = 1$. A partir de agora, serão estudados os estágios deste algoritmo. O objetivo é mostrar que cada estágio é limitado polinomialmente.

A prova será dividida nos seguintes casos:

Caso 1 $f \in \{J_\star, J_+, J_\bullet, h, \mathsf{exp}\}$, ou seja, f não é um símbolo associativo-comutativo.

Nesse caso, n é fixo, pois f consiste de símbolos de funções unárias e binárias. Logo, n é no máximo 2.

- Suponha que f um símbolo de função unária, isto é, $f \in \{J_\star, J_+, J_\bullet, h\}$.

  Será mostrado que pode ser decidido em tempo polinomial se existe $t_i \in T$, $1 \leq i \leq m$, tal que $f(t_i)\downarrow =_{AC} t$. Para isto, será calculado o custo dessa decisão, i. e, o número de passos elementares para executar esta decisão.

  Denotaremos este custo por $C(f(t_i) \downarrow =_{AC} t)$.

  Tal custo é dado por:

$$C(f(t_i) \downarrow =_{AC} t) = \sum_{i=1}^{m} C(f(t_i) \longrightarrow f(t_i)\downarrow) + \sum_{i=1}^{m} C(S_i),$$

onde m é o número de possibilidades para i, $C(f(t_i) \longrightarrow f(t_i)\downarrow)$ é o custo de normalizar $f(t_i)$ e $C(S_i)$ é o custo de responder o problema de unificação $S_i = \left\{f(t_i)\downarrow =^{?}_{AC} t\right\}$.

Pelo Lema 2, $\mathcal{R}$ é convergente módulo AC então, para cada i, existe um inteiro k_i, tal que a forma normal de $f(t_i)$ é obtida por uma derivação cujo comprimento é limitado por k_i. Isto é, para cada i, existe um inteiro k_i tal que

$$f(t_i) \xrightarrow{(k_i)} f(t_i)\downarrow .$$

Observe que, para normalizar $f(t_i)$, em cada passo, todo o termo será percorrido afim de encontrar possíveis instâncias de regras de $\mathcal{R}$ (para normalização será usada a estratégia de redução mais à esquerda) e então uma regra é aplicada. Para a normalização toda, são aplicadas k_i regras, para cada i, $1 \leq i \leq m$.

Esta normalização pode ser representada por:

$$\underbrace{f(t_i) \rightarrow f_1(t_i^1) \rightarrow f_2(t_i^2) \rightarrow \ldots \rightarrow f_{k_i}(t_i^{k_i})}_{k_i-\text{passos}} = f(t_i)\downarrow .$$

O custo de normalizar $f(t_i)$, para cada i, será definido recursivamente da seguinte forma:

$$C(f(t_i) \rightarrow f_1(t_i^1)) = |f(t_i)| + 1,$$

já que toda a extensão do termo $f(t_i)$ é percorrida e então aplicada uma regra. Assim,

$$C(f_{j-1}(t_i^{j-1}) \rightarrow f_j(t_i^j)) = C(f_{j-2}(t_i^{j-2}) \rightarrow f_{j-1}(t_i^{j-1})) + |f_{j-1}(t_i^{j-1})| + 1, \quad 1 \leq j \leq k_i.$$

Logo

$$\begin{aligned} C(f(t_i) \overset{*}{\rightarrow} f(t_i)\downarrow) &= C(f_{k_i-1}(t_i^{k_i-1}) \rightarrow f_{k_i}(t_i^{k_i})) \\ &= C(f_{k_i-2}(t_i^{k_i-2}) \rightarrow f_{k_i-1}(t_i^{k_i-1})) + |f_{k_i-1}(t_i^{k_i-1})| + 1 \\ &= |f(t_i)| + \left(\sum_{j=1}^{k_i-1} |f_j(t_i^j)|\right) + k_i \end{aligned}$$

Afirmação: $|f_j(t_i^j)| \leq |f(t_i)| + j$, para $1 \leq j \leq k_i$, $1 \leq i \leq m$.

De fato, com exceção das regras

$$\begin{cases} \mathrm{J}_\bullet(h(x) \bullet y) \to h(\mathrm{J}_+(x)) \bullet \mathrm{J}_\bullet(y) & \text{(I)} \\ \mathsf{exp}(e_\bullet, x) \to h(e_+ * x) & \text{(II)} \end{cases}$$

todas as outras regras de $\mathcal{R}$ produzem um termo menor do que o termo anterior, ou seja, $|f(t_i)\downarrow|$ atinge seu maior valor quando apenas as regras (I) e (II) são aplicadas em todos os passos. Suponha que apenas as regras (I) e (II) são aplicadas então, para todo j,

$$|f_j(t_i^j)| = |f(t_i)| + j.$$

Portanto, para aplicação de regras arbitrárias, segue que

$$|f_j(t_i^j)| = |f(t_i)| + j.$$

Assim,

$$|f(t_i)\downarrow| \leq |f(t_i)| + k_i, \quad 1 \leq i \leq m \tag{4.1}$$

Logo,

$$\begin{aligned} C(f(t_i) \xrightarrow{*} f(t_i)\downarrow) &= |f(t_i)| + \left(\sum_{j=1}^{k_i-1} |f_j(t_i^j)|\right) + k_i \\ &\leq |f(t_i)| + \left(\sum_{j=1}^{k_i-1} |f(t_i)| + j\right) + k_i \\ &= |f(t_i)| + \left[(k_i-1)|f(t_i)| + \frac{(k_i-1)(k_i-1+1}{2}\right] + k_i \\ &= k_i|f(t_i)| + \frac{(k_i-1)k_i}{2} + k_i \\ &= k_i\left(|f(t_i)| + \frac{k_i-1}{2} + 1\right) \\ &= k_i\left(|f(t_i)| + \frac{k_i+1}{2}\right) \end{aligned}$$

Portanto, para cada i,

$$C(f(t_i) \longrightarrow^* f(t_i)\!\downarrow) \leq k_i \left(|f(t_i)| + \frac{k_i + 1}{2} \right). \tag{4.2}$$

Observação: Para um termo t qualquer, considere a medida $m(t)$ dada por:

$$\begin{aligned} m(t) \;&:=\; |t| + |\,\{p \in \mathcal{O}(t) \,|\, \exists\, p' \leq p \text{ tal que } top(t|_p) = h \text{ e } top(t|_{p'}) = J_\bullet\}\,| \\ &+\; |t| \cdot |\,\{p \in \mathcal{O}(t) \,|\, (t|_p)|_\varepsilon = \mathsf{exp}\}\,| + |\,\{p \in \mathcal{O}(t) \,|\, top(t|_p) = \bullet \text{ e } top(t|_{p1}) = J_\bullet\}\,|. \end{aligned}$$

Note que com a aplicação de qualquer regra essa medida diminui estritamente. Além disso

$$m(t) \leq 3|t|^2 + |t|.$$

Logo, $m(t)$ é limitada polinomialmente.

Dessa forma, para todo i,

$$k_i \leq m(f(t_i)) \leq 3|f(t_i)|^2 + |f(t_i)|.$$

Seja $c := \max\limits_{1 \leq i \leq m} k_i$ e, para todo i existe um índice j tal que $k_i \leq c \leq m(f(t_j))$. Assim, o inteiro c é limitado polinomialmente e

$$C(f(t_i) \longrightarrow^* f(t_i)\!\downarrow) \leq c \left(|f(t_i)| + \frac{c+1}{2} \right)$$

Como $|f(t_i)| \leq l$ segue que

$$C(f(t_i) \longrightarrow^* f(t_i)\downarrow) \leq cl + \frac{c(c+1)}{2}.$$

Portanto, para cada i, o custo da normalização de $f(t_i)$ é limitado por um polinômio sobre l.

Note que, $f(t_i)\!\downarrow =_{AC} t$ só faz sentido quando $|f(t_i)\!\downarrow| = |t|$ e $top(t) = f$.

Para calcular o custo de decidir se $f(t_i) = t$, será adotada a seguinte estratégia:

Para cada posição $p \in \mathcal{O}(t)$, procura-se uma única posição $p' \in \mathcal{O}(f(t_i)\downarrow)$ tal que $t|_p = f(t_i)\!\downarrow|_{p'}$.

Caso não existam tais posições segue que $f(t_i)\downarrow \neq t$.

Agora se existirem tais p e p', buscam-se para cada uma das posições $p_j \in \mathcal{O}(t)$ que sobraram, uma única posição $p'_j \in \mathcal{O}(f(t_i)\downarrow)$ (que não foi utilizada anteriormente) tal que $t|_{p_j} = f(t_i)|_{p'_j}$. Este processo será repetido até que todas as posições de t tenham sido analisadas.

Se, no final deste processo, para toda posição p de t, existir uma posição p' de $f(t_i)\downarrow$, tal que $t|_p = (f(t_i)\downarrow)|_{p'}$ então $f(t_i)\downarrow =_{AC} t$.

Assim,

$$\begin{aligned} C(f(t_i) =^? t) &\leq |t||f(t_i)\downarrow| \\ &\leq |t|(|f(t_i)| + c) \\ &\leq l(l+c) \\ &= l^2 + lc \end{aligned} \tag{4.3}$$

onde a segunda desigualdade é consequência de (4.1) e a terceira desigualdade segue do fato de que $|t|, |f(t_i)| \leq l$. Portanto, custo de decidir se existe $t_i \in T$ tal que $f(t_j)\downarrow =_{AC} t$ é dado por

$$\begin{aligned} C(f(t_i)\downarrow =_{AC} t) &= \sum_{j=1}^{m} C(f(t_j) \longrightarrow f(t_j)\downarrow) + \sum_{j=1}^{m} C(f(t_j) =^? t) \\ &\leq \left(\sum_{i=1}^{m} cl + \frac{c(c+1)}{2}\right) + (\sum_{i=1}^{m} l^2 + lc) \\ &= m\left(cl + \frac{c(c+1)}{2}\right) + m(l^2 + lc) \\ &= ml^2 + 2mcl + m\left(\frac{c(c+1)}{2}\right) \end{aligned}$$

Logo,

$$C(f(t_i)\downarrow =_{AC} t) \leq ml^2 + 2mcl + m\left(\frac{c(c+1)}{2}\right)$$

ou seja, o número de passos elementares para decidir se existe $t_i \in T$ tal que $f(t_i)\downarrow =_{AC} t$ é limitado por um polinômio sobre l, donde segue que o problema é decidível em tempo polinomial.

- Quando $f = exp$, o objetivo é mostrar que pode ser decidido em tempo polinomial se existem $t_i, t_j \in T, 1 \leq i, j \leq m$ tais que $\mathsf{exp}(t_i, t_j) \downarrow =_{AC} t$. Como no caso anterior, será mostrado que o custo de normalizar $\mathsf{exp}(t_i, t_j) \downarrow$ e o custo de decidir se $\mathsf{exp}(t_i, t_j) \downarrow =^{?}_{AC} t$ são limitados por polinômios sobre a entrada l.

  Como $\mathcal{R}$ é convergente módulo AC, para todo $t_i, t_j \in T$ existe um inteiro k_{ij} tal que

$$\mathsf{exp}(t_i, t_j) \xrightarrow{(k_{ij})} \mathsf{exp}(t_i, t_j) \downarrow$$

  Seja $c' = \mathsf{max}_{1 \leq i,j \leq m}(k_{ij})$. Analogamente ao caso anterior, $c' \leq m(f(t_j))$, para algum índice j.

  Então, segue de 4.2 juntamente com $|\mathsf{exp}(t_i, t_j)| \leq l$ que

$$C(\mathsf{exp}(t_i, t_j) \xrightarrow{*} \mathsf{exp}(t_i, t_j) \downarrow) \leq c' \left(l + \frac{c' + 1}{2} \right)$$

  Além disso, por (4.3) tem-se que

$$C(\mathsf{exp}(t_i, t_j) \downarrow =?_{AC} t) \leq |t|(|\mathsf{exp}(t_i, t_j) \downarrow |) \leq l^2 + lc'.$$

  Assim, o custo de decidir se existem $t_i, t_j \in T$ tais que $\mathsf{exp}(t_i, t_j) \downarrow =_{AC} t$ é dado por:

$$\begin{aligned} C(\mathsf{exp}(t_i, t_j) \downarrow =_{AC} t) &= \sum_{j'=1}^{m} \sum_{i'=1}^{m} C(\mathsf{exp}(t_{i'}, t_{j'}) \xrightarrow{*} \mathsf{exp}(t_{i'}, t_{j'}) \downarrow) + \\ &\quad \sum_{j'=1}^{m} \sum_{i'=1}^{m} C(\mathsf{exp}(t_i, t_j) \downarrow =?_{AC} t) \\ &\leq \sum_{j'=1}^{m} \sum_{i'=1}^{m} c' \left(l + \frac{c' + 1}{2} \right)) + \sum_{j'=1}^{m} \sum_{i'=1}^{m} (l^2 + lc') \\ &= m^2 l^2 + 2m^2 lc' + m^2 \frac{c'(c' + 1)}{2} \end{aligned}$$

  Logo, o problema de deducibilidade um-passo é decidível em tempo polinomial.

Caso 2: f é um símbolo associativo-comutativo, ou seja, $f \in \{\star, +, \bullet\}$.

Para facilitar os cálculos faça $f = \circ$.

Quando $\circ \in \{\star, +\}$ apenas as propriedades de grupo Abeliano de um único símbolo são utilizadas e o problema se resume em resolver um sistema de equações lineares sobre $\mathbb{Z}$.

O objetivo é mostrar que dado um conjunto finito de termos $T = \{t_1, \ldots, t_m\}$ e um termo t, existem termos $t_1, \ldots, t_n \in T$ tais que $(t_1 \circ t_2 \circ \ldots \circ t_n) \downarrow = t$.

Caso 2.1: Se $\circ = +$, o problema se transforma em encontrar inteiros $y_1, \ldots, y_m$ que podem ser eventualmente nulos, tais que

$$(y_1 t_1 + y_2 t_2 + \ldots + y_m t_m) \downarrow = t$$

onde y_i é número de repetições do termo t_i, para $1 \leq i \leq m$ e y_i pode ser arbitrariamente nulo. Sejam $u_1, \ldots, u_k$ termos tais que, para cada índice $i \in \{1, \ldots, m\}$, o termo t_i pode ser escrito da seguinte forma:

$$t_i = \alpha_{i1} u_1 + \alpha_{i2} u_2 + \ldots + \alpha_{ik} u_k,$$

com $\alpha_{ij}\, (1 \leq j \leq k)$ são inteiros não simultaneamente nulos.

Para que $(y_1 t_1 + y_2 t_2 + \ldots + y_m t_m) \downarrow = t$ é preciso que

$$\begin{aligned} t &= \left(y_1 \left(\sum_{j=1}^{k} \alpha_{1j} u_j \right) + \ldots + y_m \left(\sum_{j=1}^{k} \alpha_{mj} u_j \right) \right) \downarrow \\ &= \left(\left(\sum_{i=1}^{m} y_i \alpha_{i1} \right) u_1 + \ldots + \left(\sum_{i=1}^{m} y_i \alpha_{ik} \right) u_k \right) \downarrow \\ &= J_+ \left(\left(\sum_{i=1}^{m} y_i \alpha'_{i1} \right) u'_1 + \ldots + \left(\sum_{i=1}^{m} y_i \alpha'_{ir} \right) u'_r \right) + \\ &\quad + \left(\sum_{i=1}^{m} y_i \alpha'_{r+1} \right) u'_{r+1} + \ldots + \left(\sum_{i=1}^{m} y_i \alpha'_{ik} \right) u'_k \end{aligned}$$

Assim, existem inteiros $\gamma_1, \ldots, \gamma_k$ tais que

$$t = J_+(\gamma_1 u'_1 + \gamma_2 u'_2 + \ldots \gamma_r u'_r) + \gamma_{r+1} u'_{r+1} + \ldots + \gamma_k u'_k,$$

donde segue que

$$\begin{cases} \gamma_1 &= \alpha'_{11}y_1 + \alpha'_{21}y_2 + \ldots + \alpha'_{m1}y_m \\ \vdots & \qquad\qquad \vdots \\ \gamma_k &= \alpha'_{1k}y_1 + \alpha'_{2k}y_2 + \ldots + \alpha'_{mk}y_m \end{cases}$$

E o problema se resume em resolver um sistema de equações lineares sobre $\mathbb{Z}$.

Observe que o algoritmo da eliminação de Gauss usado para resolver sistemas lineares é um procedimento da classe P.

Caso 2.2: Se $\circ = \star$, o problema se transforma em encontrar inteiros $x_1, \ldots, x_m$ que podem ser eventualmente nulos, tais que

$$(t_1^{x_1} \star \ldots \star t_m^{x_m}) \downarrow = t.$$

onde x_i é número de repetições do termo t_i, para $1 \leq i \leq m$ e x_i pode ser arbitrariamente nulo.

Como no caso anterior, para cada índice $i \in \{1, \ldots, m\}$, o termo t_i pode ser escrito da seguinte forma:

$$t_i = u_1^{a_{i1}} \star u_2^{a_{i2}} \star \ldots \star u_k^{a_{ik}}$$

com a_{ij} $(1 \leq j \leq k)$ inteiros não simultaneamente nulos.

Para que $(t_1^{x_1} \star \ldots \star t_m^{x_m}) \downarrow = t$ é preciso que

$$\begin{aligned} t &= \left(\left(\prod_{j=1}^{k} u_j^{a_{1j}} \right)^{x_1} \star \ldots \star \left(\prod_{j=1}^{k} u_j^{a_{mj}} \right)^{x_m} \right) \downarrow \\ &= \left(\left(\prod_{j=1}^{k} u_j^{a_{1j}x_1} \right) \star \ldots \star \left(\prod_{j=1}^{k} u_j^{a_{mj}x_m} \right) \right) \downarrow \\ &= u_1^{(a_{11}x_1 + \ldots + a_{m1}x_m)} \star \ldots \star u_k^{(a_{1k}x_1 + \ldots + a_{mk}x_m)} \\ &= J_\star \left({u'_1}^{\sum_{i=1}^{m} a'_{i1}x_i} \star \ldots \star {u'_r}^{\sum_{i=1}^{m} a'_{ir}x_i} \right) \star \\ &\quad \star {u'_{r+1}}^{\sum_{i=1}^{m} a'_{ir+1}x_i} \star \ldots \star {u'_k}^{\sum_{i=1}^{m} a'_{ik}x_i} \end{aligned}$$

Assim, existem inteiros $b_1, \ldots, b_k$, não simultaneamente nulos, tais que

$$t = J_\star({u'_1}^{b_1} \star \ldots \star {u'_r}^{b_r}) \star {u'_{r+1}}^{b_{r+1}} \star \ldots \star {u'_k}^{b_k},$$

donde segue que

$$\begin{cases} b_1 &= a'_{11}x_1 + \ldots + a'_{m1}x_m \\ \vdots & \vdots \\ b_k &= a'_{1k}x_1 + \ldots + a'_{mk}x_m \end{cases}$$

Novamente, o problema se resume em resolver um sistema de equações lineares sobre $\mathbb{Z}$. Utilizando o método da eliminação de Gauss pode-se concluir que o problema acima é limitado polinomialmente.

Caso 2.3: Se $\circ = \bullet$, o problema se transforma em encontrar inteiros $z_1, \ldots, z_m$ que podem ser eventualmente nulos, tais que

$$(t_1^{z_1} \bullet \ldots \bullet t_m^{z_m}) \downarrow = t,$$

onde z_i é número de repetições do termo t_i, para $1 \leq i \leq m$ e z_i pode ser arbitrariamente nulo.

Como nos casos anteriores, para cada índice $i \in \{1, \ldots, m\}$, o termo t_i pode ser escrito da seguinte forma:

$$t_i = u_1^{d_{i1}} \bullet u_2^{d_{i2}} \bullet \ldots \bullet u_k^{d_{ik}}$$

com d_{ij} $(1 \leq j \leq k)$ inteiros não simultaneamente nulos.

Para que $(t_1^{z_1} \bullet \ldots \bullet t_m^{z_m}) \downarrow = t$ é preciso que

$$\begin{aligned} t &= \left(\left(\prod_{j=1}^{k} u_j^{d_{1j}} \right)^{z_1} \bullet \ldots \bullet \left(\prod_{j=1}^{k} u_j^{d_{mj}} \right)^{z_m} \right) \downarrow \\ &= (u_1^{(d_{11}z_1 + \ldots + d_{m1}z_m)} \bullet \ldots \bullet u_k^{(d_{1k}z_1 + \ldots + d_{mk}z_m)}) \downarrow \\ &= h \left(\left(\sum_{i=1}^{m} d'_{i1}z_i \right) u'_1 + \ldots + \left(\sum_{i=1}^{m} d'_{ir}z_i \right) u'_r \right) \bullet \\ &\quad \bullet u'_{r+1}{}^{\sum_{i=1}^{m} d'_{ir+1}z_i} \bullet \ldots \bullet u'_k{}^{\sum_{i=1}^{m} d'_{ik}z_i} \end{aligned}$$

Assim existem inteiros $\beta_1, \ldots, \beta_k$ não simultaneamente nulos, tais que

$$t = h(\beta_1 u'_1 + \ldots + \beta_r u'_r) \bullet u'^{\beta_{r+1}}_{r+1} \bullet \ldots \bullet u'^{\beta_k}_k,$$

donde segue que

$$\left\{\begin{array}{rcl} \beta_1 & = & d'_{11}z_1 + \ldots + d'_{m1}z_m \\ \vdots & & \vdots \\ \beta_k & = & d'_{1k}z_1 + \ldots + d'_{mk}z_m \end{array}\right. \qquad \left\{\begin{array}{rcl} \beta_{r+1} & = & d'_{1r+1}z_1 + \ldots + d'_{m1}z_m \\ \vdots & & \vdots \\ \beta_k & = & d'_{1k}z_1 + \ldots + d'_{mk}z_m \end{array}\right.$$

E o problema se resume em resolver dois sistemas de equações lineares sobre $\mathbb{Z}$. Como nos casos anteriores, basta utilizar o algoritmo da eliminação de Gauss, cujo custo é limitado polinomialmente.

Portando, o problema de deducibilidade um-passo é decidível em tempo polinomial.

□

Com todos os conceitos estabelecidos pode-se provar que o problema sobre a possibilidade de um intruso obter certa informação s (o segredo) a partir de um conhecimento prévio T, usando suas capacidades de dedução, é decidível em tempo polinomial. Essa prova consiste em resolver o problema de dedução do intruso através de um algoritmo de saturação.

Teorema 3 O problema da dedução do intruso é decidível em tempo polinomial para o sistema de inferência $\mathcal{I}_{\mathsf{EP}}$.

Demonstração: Para provar este teorema é suficiente mostrar que o problema pode ser decidido com a execução de um número polinomial de vezes o algoritmo do lema de deducibilidade em um passo. Pela localidade do sistema de regras de inferência $\mathcal{I}_1 \cup \mathcal{I}_2$, se existe uma prova de $T \vdash s$ então existe uma prova que percorre apenas $F(T \cup \{s\})$.

O algoritmo consiste em saturar o conhecimento do intruso adicionando os termos de $F(T \cup \{s\})$ que são dedutíveis em um passo do conhecimento inicial T.

A entrada é composta por um conjunto finito T de termos, que representa o conhecimento do intruso, e um termo s que pode ser o segredo.

O algoritmo de saturação pode ser representado da seguinte forma:

Entrada: T , s

Saída: SIM ou NÃO, segundo s derivável de T

Algoritmo:

$T' := \emptyset$ $T'' := T$

enquanto $T'' \neq T'$ faça

$T' := T''$

para todo $u \in F(T \cup \{s\})$ faça

se u é dedutível em um passo de T' então $T'' := T'' \cup \{u\}$

fim para todo

fim enquanto

se $s \in T''$ então retorne SIM

senão retorne NÃO.

Depois de $|F(T \cup \{s\})|$ iterações do *loop* para todo o algoritmo pára. Agora, basta verificar se o termo s está no conjunto final T. Observe que este algoritmo é limitado polinomialmente pois, o número de iterações do *loop* enquanto é limitado pelo tamanho de $F(T \cup \{s\})$; pelo Lema 8, a noção de subtermos F é linear no tamanho de T e s. E, pelo Lema 10, o problema da deducibilidade em um passo é decidível em tempo polinomial.

Portanto, o problema da dedução do intruso é decidível em tempo polinomial. □

Capítulo 5

Conclusão

A verificação de protocolos é notoriamente difícil, e mesmo protocolos muito simples que parecem completamente inofensivos podem ter sérias falhas de segurança, como foi dramaticamente demonstrado pela falha do protocolo de Needham-Schroeder encontrada por Lowe [Low95]. Esse protocolo foi utilizado durante 17 anos até que a falha foi detectada.

Classicamente, a verificação de protocolos criptográficos era baseada na *hipótese da criptografia perfeita* que afirma que é impossível obter qualquer informação sobre uma mensagem encriptada sem saber exatamente a chave utilizada para decriptá-la. Infelizmente, um intruso pode utilizar propriedades das primitivas criptográficas em combinação com as regras do protocolo afim de obter uma mensagem secreta. Muitos resultados relacionados a segurança de protocolos já foram obtidos, tanto para o problema da dedução do intruso (intruso passivo) quanto para a preservação de segurança sobre ataques ativos.

Neste trabalho foi estudado o problema da dedução do intruso para um protocolo de carteira eletrônica, introduzido em [BCLD07a], cuja teoria equacional é composta por propriedades algébricas. Estas propriedades algébricas contam com os axiomas de três grupos Abelianos e algumas regras para exponenciação expressas de forma que a unificação seja decidível. Apesar de teorias equacionais que contam com axiomas de grupos Abelianos e exponenciação modular já terem sido estudadas (ver [Shm04, CKRT03]), não é possivel

utilizar diretamente a combinação desses resultados como em [CR05], uma vez que essas teorias, da forma em que são utilizadas na execução do protocolo, não são disjuntas. Dessa forma foi estudado um novo procedimento de decisão para esse problema na presença de um intruso possuindo capacidades complexas de dedução que são modeladas através dessa teoria equacional introduzida por [BCLD07a].

Este estudo baseou-se na abordagem clássica de Dolev-Yao [DY81], que consiste em modelar um ataque através de um sistema de dedução. Inicialmente, para um sistema de dedução sem propriedades algébricas, o problema se $T \vdash s$ é decidido em tempo polinomial, já que a teoria do intruso é local. Este resultado segue do Lema de Tratabilidade introduzido por D. McAllester em [McA90], que afirma que se um sistema de regras de inferência tem a propriedade de *localidade*, então a relação de dedução é decidida em tempo polinomial. Agora, como as primitivas criptográficas do protocolo estudado tem propriedades algébricas, que podem ser exploradas pelo intruso, será preciso adaptar este resultado para garantir a polinomialidade do problema de derivabilidade em questão.

Foi feita uma análise detalhada sobre a adaptação desta técnica para provar a polinomialidade do problema da dedução do intruso, que foi proposta em [BCLD07a]. Para execução do protocolo, foram utilizados símbolos de função com propriedades aritméticas, como $\{\bullet, \star, +\}$, interpretados como operadores de grupos Abelianos, entre outros símbolos. O objetivo era mostrar que o novo sistema de dedução, que representa a capacidade do intruso e que faz uso destes símbolos, tem a propriedade de localidade. Primeiramente, foi introduzido o sistema de regras de reescrita AC-convergente associado a essa teoria. E então, provado que o par $(\mathcal{R}, AC)$ satisfaz propriedade do variante finito, o que garante que a unificação é decidível para EP, já que é decidível para teoria AC. Como ferramentas para o estudo da localidade, foram estabelecidos lemas de natureza técnica para provar resultados posteriores.

As demonstrações desses lemas em [BCLD07a] são omitidas ou contem algumas imprecisões e muitas vezes erros que precisaram ser corrigidos para validar os resultados.

Por exemplo, foi preciso estabelecer um nova ordem de prioridade, para aplicação das regras do sistema de reescrita utilizado, que faz uso das chamadas *regras de extensão* para que então, os lemas técnicos 4 e 5 fossem, de fato, demonstrados.

A forma em que a noção semântica de subtermos F foi definida em [BCLD07a] não é suficiente para garantir a F-localidade do sistema de inferência que modela a capacidade do intruso. Esta falha foi resolvida na prova da proposição 2, no caso onde a última regra é um composição do tipo $\mathsf{R}_\circ$. Para solucionar este problema, foi preciso uma alteração na definição de F através da adição do símbolo de função binária $\bullet$ no subconjunto $\{\mathsf{inv}_\circ(t) \,|\, t \in \mathrm{Sub}(T), \mathrm{TOP}(t) = \circ, \quad \circ \in \{\star, +\}\}$ que compõe F. Ainda nesta proposição, muitas outras imprecisões foram corrigidas e subcasos que não tinham sido analisados, foram incluídos.

O resultado de McAllester só pode ser utilizado para sistemas finitos de regras de dedução. Na extensão do modelo de Dolev-Yao utilizada, a presença das regras ($\mathsf{R}_\circ$), onde $\circ \in \{\bullet, \star, +\}$ são símbolos associativos e comutativos, transforma o sistema de regras de dedução em um conjunto infinito. Para contornar este problema foi considerada uma generalização do resultado de localidade para os operadores AC, que consiste em saturar o conhecimento do intruso acrescentando os termos de $F(T \cup s)$ que são dedutíveis em um passo a partir do seu conhecimento inicial T. O problema de deducibilidade em um passo, cuja demonstração é omitida no trabalho original [BCLD07a], foi provado em detalhe na última seção do capítulo 4. Finalmente, depois que todos os resultados foram estabelecidos e provados, o problema da dedução do intruso foi demonstrado ser decidível em tempo limitado polinomialmente.

Muitos resultados relacionados à segurança de protocolos criptográficos, mediante à presença de intrusos passivos com as mais variadas e complexas capacidades algébricas, tem sido estudados. Existe ainda uma vastidão de resultados a serem obtidos, principalmente relacionados à segurança na presença de um *intruso ativo*.

Para a maioria das teorias equacionais, que podem ser utilizadas na modelagem de

um protocolo criptográfico, o problema de segurança na presença de intrusos ativos é ainda indecidível. Para alguns subcasos, foi possível analisar a questão da segurança, como é o caso de teorias equacionais com ou-exclusivo e grupos Abelianos e também para exponenciação modular (como pode ser visto em [CLS03, CKRT03]), entre outros.

Ainda há muito trabalho a fazer também, quando se trata de um algoritmo geral que decida o problema da segurança, independente da teoria equacional utilizada na modelagem do protocolo ou da capacidade algébrica do intruso (passivo ou ativo).

Como pode ser visto, a Teoria da Reescrita tem sido utilizada como uma ferramenta adicional para colaborar com a busca de soluções para o problema de segurança em protocolos criptográficos que são executados em ambientes não confiáveis. Tal problema tem chamado muita atenção dada sua importância e dificuldade.

Referências Bibliográficas

[ACD07] M. Arnaud, V. Cortier, and S. Delaune. Combining algorithms for deciding knowledge in security protocols. In *Research Report 6118, INRIA, 28 pages*, 2007.

[BCLD07a] B. Bursuc, H. Comon-Lundh, and S. Delaune. Deducibility constraints, equational theory and electronic money. In *Rewriting, Computation and Proof*, volume 4600 of *Lecture Notes in Computer Science*, pages 196–212. Springer-Verlag, 2007.

[BClD07b] S. Bursuc, H. Comon-lundh, and D. Delaune. Associative-commutative deducibility constraints. In *Proceedings of the 24th Annual Symposium on Theoretical Aspects of Computer Science (STACS'07)*, volume 4393 of *Lecture Notes in Computer Science*, pages 634–645. Springer-Verlag, 2007.

[BN98] F. Baader and T. Nipkow. *Term Rewriting and All That.* Cambridge University Press, 1998.

[BP05] B. Blanchet and A. Podelski. Verification of cryptographic protocols: Tagging enforces termination. *Theoretical Computer Science*, 333(1-2):67–90, 2005.

[BS99] F. Baader and W. Snyder. Unification theory. In A. Robinson and A. Voronkov, editors, *Handbook of Automated Reasoning*, chapter 1, pages 1–85. Elsevier, 1999.

[CDL06] V. Cortier, S. Delaune, and P. Lafourcade. A survey of algebraic properties used in cryptographic protocols. *Journal of Computer Security*, 14(1):1–43, 2006.

[CKRT03] Y. Chevalier, R. Küsters, M. Rusinowitch, and M. Turuani. Deciding the security of protocols with Diffie-Hellman exponentiation and products in exponents. In *FSTTCS*, volume 2914 of *Lecture Notes in Computer Science*, pages 124–135. Springer-Verlag, 2003.

[CLC05] H. Comon-Lundh and V. Cortier. Tree automata with one memory, set constraints and cryptographic protocols. *Theoretical Computer Science*, 331(1):143–214, 2005.

[CLD04] H. Comon-Lundh and S. Delaune. The finite variant property: How to get rid of some algebraic properties. In *Research Report LSV-04-17, Laboratoire Spécification et Vérification, ENS Cachan, France, 21 pages*, 2004.

[CLS03] H. Comon-Lundh and V. Shmatikov. Intruder deductions, constraint solving and insecurity decision in presence of exclusive or. In *Proc. 18th IEEE Symposium on Logic in Computer Science (LICS 2003)*, pages 271–280. IEEE Comp. Soc. Press, 2003.

[CM96] E. Contejean and C Marché. CiME: Completion modulo E. In *Proc. of Rewriting Techniques and Applications (RTA 1996)*, volume 1103 of *Lecture Notes in Computer Science*, pages 416–419. Springer-Verlag, 1996.

[CR05] Y. Chevalier and M. Rusinowitch. Combining intruder theories. In *Caires, L., Italiano, G.F., Monteiro, L., Palamidessi, C., Yung, M.(Eds) (ICALP'05)*, volume 3580 of *Lecture Notes in Computer Science*, pages 639–651. Springer-Verlag, 2005.

[DJ90] N. Dershowitz and J-P. Jouannaud. Rewrite systems. In J. van Leeuwen, editor, *Handbook of Theoretical Computer Science*, volume B, chapter 6, pages 243–320. Elsevier, 1990.

[DY81] D. Dolev and A. Yao. On the security of public keys protocols. In *Proc. 22nd Annual Symp. on Foundations of Computer Science*, pages 350–357. IEEE, 1981.

[Geh94] W. Gehrke. Detailed catalogue of canonical term rewriting systems generated automatically. *Research Institute for Symbolic Computation*, 1994.

[KNW03] D. Kapur, P. Narendran, and L. Wang. An E-unification algorithm for analyzing protocols that use modular exponentiation. In *Proc. 14th International Conference on Term Rewriting and Applications, (RTA'03)*, volume 2706 of *Lecture Notes in Computer Science*, pages 165–179. Springer-Verlag, 2003.

[Low95] G. Lowe. An attack on the Needham-Schroeder public key authentication protocol. *Information Processing Letters*, 56(3):131–133, 1995.

[Low99] G. Lowe. Towards a completeness result for model checking of security protocols. *Journal of Computer Security*, 7(2-3):89–146, 1999.

[McA90] D. McAllester. Automatic recognition of tractability in inference relations. *Journal of the ACM*, 40:284–303, 1990.

[RS05] R. Ramanujam and S. P. Suresh. Decidability of context-explicit security protocols. *Journal of Computer Security*, 13:135–165, 2005.

[RT01] M. Rusinowitch and M. Turuani. Protocol insecurity with finite number of sessions is NP-complete. In *14th IEEE Computer Security Foundations Workshop (CSFW 2001)*, pages 174–190. IEEE Comp. Soc., 2001.

[RT03] M. Rusinowitch and M. Turuani. Protocol insecurity with finite number of sessions, composed keys is NP-complete. *Theoretical Computer Science*, 299(1-3):451–475, 2003.

[Shm04] V. Shmatikov. Decidable analysis of cryptographic protocols with products and modular exponentiation. In *Proc. 13th European Symposium on Programming (ESOP'04)*, volume 2986 of *Lecture Notes in Computer Science*, pages 355–369. Springer-Verlag, 2004.