Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

O Problema da Dedução do Intruso para Teorias AC-convergentes Localmente Estáveis

por

Daniele Nantes Sobrinho

Orientador: Mauricio Ayala Rincón
Coorientadora: Maribel Fernández

Brasília
2013

Às minhas mães,
Selma Pereira Nantes e
Aura Martins Nantes
Ao meu marido,
João Paulo dos Santos.
Os amores da minha vida...

To be or not to be is true.
– G.Boole

"There are known knowns.
There are things we know we know.
We also know
There are known unknowns.
That is to say
We know there are some things
We do not know.
But there are also unknown unknowns"
– Donald Rumsfeld

Agradecimentos

À Deus, o Criador de todas as coisas, que me manteve firme no meu caminho, auxiliando-me e fortalecendo-me em todos os momentos da minha vida.

À minha mãe, por toda força, por toda a fé, e por tudo que me ensinou. À ela, a pessoa mais forte do mundo, dedico este trabalho e todas as minhas conquistas. Ela é a minha parte mais humana, que me ajuda a fincar os pés no chão e sempre seguir em frente.

À minha vozinha Aura, minha segunda mãe, obrigada por acreditar em mim, pela oração diária, pela presença em minha vida mesmo na distância, pelo amor, proteção e carinho.

Aos meus irmãos, Gizele (a mana Gica) e Lucas Rafael (o amor da minha vida), por fazerem parte da minha vida de forma tão intensa, obrigada pelas ligações para pedir ajuda com a tarefa, e por encherem meu coração de amor, alegria e orgulho.

Ao meu esposo João Paulo, pelo amor, carinho, dedicação, paciência, pela sua presença, pela disposição em me ajudar. Você me ajudou a me manter no caminho quando os dias ficaram difíceis e me ajudou a ver melhor o mundo ao meu redor. Sou uma pessoa melhor ao seu lado.

Ao professor Mauricio Ayala Rincón, pela oportunidade de trabalhar em conjunto, pela dedicação, paciência, profissionalismo, disposição, incentivo e pela orientação. Com ele aprendi a ser uma pesquisadora e ter paixão por aprender, com seu incentivo pude descobrir um mundo novo, e meus pés puderam pisar por lugares que vão ficar para sempre na minha memória.

À professora Maribel Fernández, por ter me ensinado a trabalhar e a pesquisar de forma tão dedicada, delicada e atenta. Obrigada por ter me ensinado a doçura da vida com a pesquisa, e por ter me ajudado tanto na concepção deste trabalho. Obrigada por me receber com tanto carinho e atenção na universidade King's College London.

Aos amigos do Departamento de Matemática da Universidade de Brasília e do Departamento de Informática da King's College London, a presença de vocês neste período ficará para sempre na minha memória. E os amigos fora da matemática, obrigada por fazerem meus dias mais alegres.

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

Ao CNPq, pelo apoio financeiro.

Resumo

Apresenta-se um algoritmo para decidir o problema da dedução do intruso (PDI) para a classe de teorias localmente estáveis normais, que incluem operadores associativos e comutativos (AC). A decidibilidade é baseada na análise de reduções de reescrita aplicadas na cabeça de termos que são construídos a partir de contextos normais e o conhecimento inicial de um intruso. Este algoritmo se baseia em um algoritmo eficiente para resolver um caso restrito de casamento módulo AC de ordem superior, obtido pela combinação de um algoritmo para *Casamento AC com Ocorrências Distintas*, e um algoritmo padrão para resolver sistemas de equações Diofantinas lineares. O algoritmo roda em tempo polinomial no tamanho de um conjunto saturado construído a partir do conhecimento inicial do intruso para a subclasse de teorias para a qual operadores AC possuem inversos.

Os resultados são aplicados para teoria AC pura e a teoria de grupos Abelianos de ordem n dada. Uma tradução entre dedução natural e o cálculo de sequentes permite usar a mesma abordagem para decidir o *problema da dedução elementar* para teorias localmente estáveis com inversos. Como uma aplicação, a teoria de assinaturas cegas pode ser modelada e então, deriva-se um algoritmo para decidir o PDI neste contexto, estendendo resultados de decidibilidade prévios.

Palavras - Chave: sistemas de reescrita de termos; teorias associativas e comutativas; teorias localmente estáveis; grupos Abelianos; protocolos criptográficos; problema da dedução do intruso; casamento e unificação módulo teorias equacionais.

Abstract

We present an algorithm to decide the intruder deduction problem (IDP) for the class of normal locally stable theories, which include associative and commutative (AC) operators. The decidability is based on the analysis of rewriting reductions applied in the head of terms built from normal contexts and the initial knowledge of the intruder. It relies on a new and efficient algorithm to solve a restricted case of higher-order AC-matching, obtained by combining the *Distinct Occurrences of AC-matching* algorithm and a standard algorithm to solve systems of linear Diophantine equations. Our algorithm runs in polynomial time on the size of a saturation set built from the initial knowledge of the intruder for the subclass of theories for which AC operators have inverses.

We apply the results to the Pure AC equational theory and Abelian Groups with a given order n. A translation between natural deduction and sequent calculus allows us to use the same approach to decide the *elementary deduction problem* for locally stable theories with inverses. As an application, we model the theory of blind signatures and derive an algorithm to decide IDP in this context, extending previous decidability results.

Keywords: term rewriting systems; AC-theories; locally stable theories; Abelian groups; cryptographic protocols; intruder deduction problem; matching and unification modulo equational theories.

Conteúdo

Introdução **7**

1 Preliminares **9**
1.1 Termos, contextos e substituições 9
1.2 Álgebras, homomorfismos e congruências 12
1.3 Classes Equacionais 13
1.4 Sistema de Reescrita de Termos 14
1.5 Casamento associativo-comutativo 17
1.5.1 Casamento AC com Ocorrências Distintas 20
1.6 PDI para Grupos Abelianos 24
1.6.1 Abordagem via provas normais 25
1.6.2 Abordagem via generalização da localidade de McAllester 34

2 Teorias Localmente Estáveis Normais **41**
2.1 Problema de Dedução 42
2.2 Teorias Localmente Estáveis 45
2.3 Teorias Localmente Estáveis Normais 52

3 Teorias Localmente Estáveis com Inversos **71**
3.1 Teorias Localmente Estáveis com Inversos 72
3.2 Grupos Abelianos 76
3.2.1 Grupos Abelianos de ordem n 78
3.3 Teoria AC-"pura" 84

4 Problema da Dedução Elementar **86**
4.1 Preliminares 87
4.1.1 Assinaturas Cegas 87
4.2 Capacidade Dedutiva do Intruso 89
4.3 Problema da Dedução Elementar 91
4.3.1 Sistema Dedutivo Linear para o Intruso 92

Conclusão **94**

Introdução

Existem diferentes abordagens para modelar protocolos criptográficos e para analisar suas propriedades de segurança. Uma técnica consiste em provar que um ataque requer resolver um problema algoritmicamente difícil; outro consiste em usar um cálculo de processos, tal como o *spi-calculus* [3], para representar as operações executadas pelos participantes do protocolo e o intruso. A abordagem dedutiva de Dolev e Yao [25], que se abstrai de detalhes algoritmicos e modela um intruso por um sistema dedutivo, tem mostrado com sucesso a existência de falhas em protocolos conhecidos. Um sistema de dedução sob a abordagem de Dolev-Yao especifica como um intruso pode obter nova informação a partir de conhecimento obtido atráves da espionagem da comunição entre participantes honestos do protocolo (no caso de um intruso passivo), ou através da espionagem e a emissão de mensagens fraudulentas (no caso de intruso ativo). Neste contexto encontra-se o *problema da dedução do intruso* (PDI) que é o problema de decidir se um intruso passivo pode obter certa informação a partir de mensagens observadas na rede.

No modelo proposto por Dolev-Yao assume-se a *hipótese da criptografia perfeita*: o conjunto de mensagens é suposto ser uma álgebra livre. Este modelo considera que sistemas de encriptação sejam caixas pretas e assume que um adversário não pode aprender nada de uma mensagem cifrada a menos que conheça a chave adequada. Porém esta hipótese não é realista, uma vez que as primitivas criptográfias podem conter propriedades algébricas que podem ser exploradas por um intruso. Desta forma pode-se postular que verificação automática de protocolos criptográficos *deve* levar em conta que as primitivas criptográficas podem obedecer as propriedades algébricas de certas teorias equacionais.

Considera-se, então, um *relaxamento* do modelo de Dolev-Yao, e agora, a abordagem dedutiva leva em consideração que um intruso pode raciocinar equacionalmente, utilizando as propriedades algébricas das primitivas criptográficas em análise. Muitos trabalhos foram realizados nesta direção, por exemplo, para o caso de teorias equacionais contendo homomorfismo [18, 30], grupos Abelianos [19, 35], ou-exclusivo [16, 19, 30], entre outras.

Associatividade e comutatividade são propriedades satisfeitas por muitas operações binárias (tais como operação de grupos Abelianos, adição e multiplicação em anéis, conjunção e disjunção em lógica). A comutatividade não é tratada apropriadamente pela abordagem da reescrita, uma vez que a identidade $x \oplus y \approx y \oplus x$, leva a uma regra não terminante. No contexto de análise de protocolos criptográficos, é necessário estabelecer procedimentos específicos para tratar teorias equacionais com propriedades associativas e comutativas. Geralmente, os resultados de decidibilidade são obtidos para subclasses

dessas teorias.

Na metodologia proposta em [1], Abadi e Cortier estabelecem condições para análise das relações de dedutibilidade de mensagens e indistinguibilidade para protocolos criptográficos modelados pelo *pi-calculus aplicado* [2]. Esta metodologia vem sendo utilizada em muitos outros trabalhos [5,11,22,23]. Em particular, este trabalho mostra que o problema da dedução do intruso é decidível para teorias *localmente estáveis*, isto é, uma subclasse das teorias equacionais que são representadas por um sistema de reescrita convergente módulo associatividade e comutatividade de algum símbolo de função. No entanto, para garantir a correção desta abordagem, a definição de teorias localmente estáveis dada em [1] precisa ser modificada (este fato foi confirmado via comunicação pessoal com o autor principal de [1]). Neste trabalho, várias modificações são feitas e é proposto um novo método para resolver o problema da dedução do intruso no contexto de teorias localmente estáveis.

De fato, a decidibilidade da relação de dedutibilidade de mensagens pode ser provada para *teorias localmente estáveis normais*, que é baseada na existência de um conjunto saturado de termos finito, computável, que inclui formas normais e nas reduções via reescrita de termos construídos a partir do conhecimento inicial do intruso e de *contextos normais*. Esta modificação, juntamente com outros resultados técnicos que são derivados dela, permite a correção do resultado de decidibilidade proposto em [1] uma vez que o Lema 11 em [1] pode ser provado para esta teoria equacional. A expressão "localmente estável" vem do fato que o estudo das reduções via reescrita em termos "pequenos" é suficiente para prever o comportamento de termos depois de reduções de reescrita em termos arbitrários, este fato nos dá uma caracterização parcial dos termos redutíveis.

Afim de obter a polinomialidade da decidibilidade, é necessário adicionar uma restrição às teorias localmente estáveis normais: a assinatura da teoria equacional tem que conter, para cada símbolo associativo comutativo $\oplus$, seu inverso correspondente $i_{\oplus}$. Isto dá uma outra caracterização de teorias para as quais a relação de dedutibilidade de mensagens é decidível, as teorias *localmente estáveis com inversos*. Além disso, a decidibilidade é polinomial com relação ao tamanho do conjunto saturado (construído a partir do conhecimento inicial do intruso).

A decidibilidade é consequência de um procedimento para resolver um caso restrito de AC-casamento de ordem superior. Para desenvolver este algoritmo, usam-se resultados conhecidos para resolver sistemas de equações diofantinas lineares (SEDL) [13, 17, 27, 39], combinado com um algoritmo polinomial para resolver o problema de Casamento AC com Ocorrências Distintas [9]. Graças ao uso do algoritmo para resolver SEDL sobre os inteiros $\mathbb{Z}$, evita-se uma busca exponencial sobre o espaço de soluções no caso dos símbolos AC.

Os resultados são aplicados na análise do problema da dedução do intruso para a teoria equacional de Grupos Abelianos Finitos, que é modelado via um fragmento de lógica de segunda ordem, e teoria AC pura. A primeira é *localmente estável com inversos* e tem um resultado de decidibilidade exponencial. A segunda é *localmente estável normal* e é um caso particular do *Problema de Programação Inteira* que é NP-completa, está em NP, concordando com resultados prévios [30].

Depois de introduzir a classe de teorias localmente estáveis normais e provar a decidi-

bilidade do PDI para protocolos criptográficos nessa classe, mostramos que o Problema da Dedução Elementar (PDE) introduzido em [41] é também decidível em tempo polinomial com relação ao conjunto saturado de termos. O PDE pode ser descrito da seguinte forma: dado um conjunto Γ de mensagens e uma mensagem M, existe um E-contexto $C[\ldots]$ e mensagens $M_1, \ldots, M_k \in \Gamma$ tais que $C[M_1, \ldots, M_k] \approx_E M$? Aqui, E é a teoria equacional modelando o protocolo criptográfico. Utilizamos esta abordagem para modelar teorias com assinaturas cegas. Utilizando um resultado prévio que relaciona decidibilidade de PDE à decidibilidade do PDI quando a teoria E satisfaz algumas condições, obtemos como aplicação a decidibilidade do PDI para uma subclasse de teorias localmente estáveis normais combinado com a teoria B de assinaturas cegas. Desta forma, generalizamos um resultado de [1]: não é necessário provar que a combinação de teorias E e B é localmente estável normal.

Trabalhos Relacionados

A análise de protocolos criptográficos tem atraído muita atenção nos últimos anos e muitas ferramentas foram desenvolvidas para tentar identificar possíveis ataques, por exemplo, Maude-NPA [26], ProVerif [12], Avispa [4], Yapa [8].

Muitos trabalhos teóricos relacionados à decidibilidade do PDI sob teorias equacionais tem sido obtidos. Em particular, a teoria de grupos Abelianos tem atraído muita atenção uma vez que, combinada com outras propriedades, é parte da estrutura de muitos algoritmos criptográficos (eg. SALARY SUM, IKA.1, MAKEP [23]). O problema da dedução do intruso para Grupos Abelianos pode ser decidido em tempo polinomial não-determinístico, Comon-Lundh e Shmatikov em [19] provam este resultado utilizando a estratégia de provas normais e a propriedade de localidade de McAllester [33].

J. Millen e V. Shmatikov em [35] investigam uma técnica de resolução de problemas que reduz PDI para Grupos Abelianos para um sistemas de equações diofantinas quadráticas. A decidibilidade de tal técnica só foi obtida posteriormente por Shmatikov em [36], pela redução do problema inicial para a solubilidade de um sistema particular de equações diofantinas quadráticas, para o caso de um número limitado de sessões.

Em [30] os autores analisam a decidibilidade de PDI para teorias AC com homomorfismo. A abordagem proposta é baseada na propriedade de localidade de McAllester e também em técnicas de transformações de provas, introduzidas por Gentzen. Neste trabalho, os autores afirmam que o PDI para a teoria de Grupos Abelianos é decídivel em tempo polinomial utilizando as técnicas propostas; no entanto, nenhuma prova deste fato foi encontrada disponível na literatura. A técnica proposta estende a noção de subtermos sintáticos para uma noção mais ampla, que é consistente com os axiomas de associatividade e comutatividade, obtendo um conjunto de subtermos cujo tamanho é exponencial com relação ao conhecimento inicial do intruso. Portanto, dentro desta abordagem a decidibilidade do PDI seria exponencial com relação ao tamanho dos subtermos.

Formulações via cálculo de sequentes do *intruso de Dolev e Yao* [40] tem sido utilizada na formulação de bissimulação aberta do spi-calculus. Em [41], são consideradas técnicas

dedutivas para lidar com protocolos criptográficos com assinaturas cegas que podem ser modelados via combinação de teorias equacionais AC-convergentes mutuamente disjuntas, onde cada teoria equacional contém um único símbolo AC. Como uma abordagem alternativa, a capacidade de dedução do intruso é modelada via um cáculo de sequentes módulo um sistema de reescrita, seguindo a abordagem de [10]. Então, a decidibilidade do PDI é reduzida em tempo polinomial para decidibilidade do PDE.

Combinando as técnicas em [41] e [14], a formulação do PDI para um Protocolo de Carteira Eletrônica com Assinaturas Cegas foi demonstrada redutível em tempo polinomial para PDE. Neste caso a teoria equacional pode ser representado por um sistema de reescrita de termos AC-convergente e a assinatura contém três símbolos AC diferentes além de regras de exponenciação [37], estendendo resultados prévios. Entretanto, nenhum algoritmo para decidir PDE é proposto.

Contribuições

Apresenta-se uma técnica para decidir o PDI para uma subclasse das teorias equacionais convergentes módulo associatividade e comutatividade. A abordagem é baseada em uma propriedade de "estabilidade local" introduzida por [1], ao invés de provar que as regras dedutivas são "locais" no sentido de David McAllester [33] como feito em trabalhos prévios [14, 19, 24, 32].

Uma vez que as técnicas propostas em [1] eram imprecisas e o algoritmo de decidibilidade proposto era exponencial quando tratava de teorias AC, foi preciso definir uma nova metodologia para o tratamento de teorias equacionais que tem a propriedade de serem localmente estáveis bem como um novo algoritmo de decidibilidade adequado para o tratamento de teorias AC.

Para ilustrar os resultados obtidos, a decidibilidade do PDI é estudada para a teoria de grupos Abelianos finitos e a teoria AC pura. Além disso, utilizando uma tradução entre dedução natural e o cálculo de sequentes, uma extensão dos resultados pode ser obtida e então deriva-se um algoritmo para a decidibilidade do PDI para teorias AC combinadas com assinaturas cegas.

Em sumário, as contribuições deste trabalho, introduzidas em detalhes na descrição dos capítulos, são enumeradas abaixo:

1. Demonstração de que técnicas em [30] para tratamento do PDI para grupos Abelianos via generalização de McAllester são de fato exponenciais o que contradiz a afirmação dos autores de que utilizando suas técnicas se pode inferir que o problema é decidível polinomialmente.

2. Um contra-exemplo que contradiz a polinomialidade do algoritmo de decidibilidade proposto por M. Abadi e V. Cortier em [1].

3. Um novo algoritmo para decisão do PDI que utiliza um procedimento para decidir casamento módulo AC.

4. Definição de uma subclasse de teorias para a qual o algoritmo de decidibilidade é polinomial: as *teorias* ***I****-localmente estáveis*. Com um ajuste nas teorias localmente estáveis [1] (com um fator de normalidade), é possível obter a decidibilidade, em tempo polinomial não determinístico, utilizando o algoritmo acima.

5. Aplicação dos resultados para a teoria de grupos Abelianos de ordem n (dada), para a qual não existia um sistema de reescrita conhecido. Esta teoria foi provada ser convergente módulo AC, e é localmente estável com inversos.

6. Aplicação dos resultados para o estudo do PDI para protocolos criptográficos com assinaturas cegas.

Capítulo 1: Preliminares

Neste capítulo, conceitos e definições básicas são introduzidos. As seções iniciais são referentes à teoria de reescrita, os principais conceitos e notações seguem aquelas introduzidas por F. Baader e T. Nipkow em [7]. Na Seção 1.5, problemas clássicos relacionados ao problema do *casamento associativo e comutativo* são introduzidos, e aqueles que se relacionam mais profundamente com as técnicas utilizadas nesta tese, são desenvolvidos com mais detalhes. O problema do *casamento associativo e comutativo - CAC* em si, é NP-completo: uma transformação polinomial do problema Mono-3SAT, que é NP-completo, para CAC pode ser construída. Em especial, o problema *Casamento AC com Ocorrências Distintas-CAC-OD*, que é uma restrição do problema CAC onde toda variável do problema sendo casado tem uma única ocorrência, é introduzido e prova-se que este problema tem um limitante superior polinomial. A metodologia utilizada aqui para decidir tais problemas foi introduzida por D. Benanav, D. Kapur e P. Narendran em [9].

Na Seção 1.6 são analisadas duas abordagens para o estudo da decidibilidade do PDI para a teoria de Grupos Abelianos. Na Subseção 1.6.1, estuda-se uma abordagem via *provas normais*, proposta por H.Comon-Lundh e V.Shmatikov em [19]. Neste trabalho os autores mostram que a decidibilidade do PDI para o caso de Grupos Abelianos está em NP. Porém a demonstração de um resultado de normalização de prova (Lema 1.3) estava imprecisa e alguns casos não tinham sido analisados,

- uma prova completa pode ser encontrada nesta subseção.

Na Subseção 1.6.2, apresenta-se uma abordagem via *generalização da localidade de McAllester*, proposta por P. Lafourcade, D. Lugiez e R.Treinen em [30]. Neste trabalho os autores afirmam que seguindo as técnicas propostas é possível obter um procedimento de tempo polinomial determinístico para o PDI para o caso de Grupos Abelianos, "melhorando" o resultado proposto em [19], que obteve um algoritmo polinomial não-determinístico. Entretanto, esta afirmação não está sustentada por uma literatura (nem mesmo no trabalho [30]). Dessa forma,

1. mostra-se na Subseção 1.6.2 que seguindo as técnicas propostas pelos autores e utilizando sua generalização da propriedade de localidade de McAllester [33], a decidibilidade do PDI para Grupos Abelianos é respondida em tempo exponencial.

Capítulo 2: Teorias Localmente Estáveis Normais

Este capítulo destina-se ao estudo da decidibilidade do *problema da dedução do intruso* para as *teorias localmente estáveis normais*, que são teorias equacionais que podem ser representadas por sistemas de reescrita de termos convergente módulo AC e que tem a propriedade de serem "estáveis" quanto à aplicação de regras de reescrita, isto é, a análise local de termos redutíveis dá uma caracterização global do espaço de informações que um intruso pode obter através de raciocínio algébrico.

Teorias similares foram introduzidas por M. Abadi e V. Cortier em [1], as chamadas *teorias localmente estáveis*. Neste trabalho os autores afirmam que para esta classe de teorias o problema da dedução do intruso é decidível em tempo polinomial com relação a um conjunto saturado de termos gerado a partir do conhecimento inicial do intruso. A metodologia proposta consiste em analisar localmente as reduções de reescrita e então estende-se o resultado para o caso global. No entanto, muitas imprecisões foram encontradas na prova deste resultado (Lema 11 em [1]), e o resultado acabou por perder-se. Na Seção 2.2 é feito um levantamento dos erros encontrados no trabalho [1]. Além disso,

2. apresenta-se um contra-exemplo para a Proposição 16 de [1] que mostra que o algoritmo de decisão que foi proposto, que era afirmado ser polinomial, na verdade é exponencial.

Afim de obter os resultados esperados, na Seção 2.3,

- a classe de teorias ***N**-localmente estáveis normais* é definida.

Esta classe de teorias é construída a partir de alguns termos na forma normal e contextos normais. Para esta teoria é possível provar o resultado de estabilidade global que a teoria em [1] perdeu. No entanto, para poder obter esse resultado, foram necessários alguns resultados técnicos preliminares, como:

- Uma estratégia de minimização de contextos (Lema 2.1), que evita computação redundante;
- Uma caracterização estrutural de redexes (Lema 2.2), que estabelece uma estrutura básica para os termos construídos que podem reduzir via reescrita;
- Uma classificação das instâncias das variáveis de lados esquerdos de regras de reescrita que são aplicáveis em termos construídos pelo intruso (Proposição 2.2).

Com estes resultados preliminares é possível

- provar que o estudo local das reduções de reescrita, para teorias **N**-localmente estáveis, pode ser estendido de forma a obter uma caracterização dos termos redutíveis, para o caso global (Lema 2.3). Isto é, os termos são "estáveis" via aplicação de regras de reescrita.

Este lema, juntamente com um resultado de igualdade módulo associatividade e comutatividade (Lema 2.4) são fundamentais para obter a decidibilidade do PDI para teorias **N**-localmente estáveis.

Capítulo 3: Teorias Localmente Estáveis com Inversos

Com objetivo de obter a polinomialidade da decidibilidade do PDI para uma subclasse de teorias AC, será necessário considerar a existência de inversos para cada símbolo associativo e comutativo na assinatura da teoria equacional considerada.

3. Um novo algoritmo de decidibilidade é proposto (Lema 3.1), este algoritmo se baseia em uma busca na ávore de representação dos termos de um conjunto saturado que é construído a partir do conhecimento inicial de um intruso.

Uma parte do algoritmo consiste de um caso restrito do problema do casamento módulo AC, chamado *Casamento AC com Ocorrências Distintas*, introduzido na Seção 1.5.1 do Capítulo 2. Uma outra parte recairá em resolver sistemas lineares de equações Diofantinas sobre $\mathbb{Z}$ e os inversos serão interpretados como *inteiros negativos*.

Para a classe de teorias **N**-localmente estáveis, este algoritmo roda em tempo polinomial não determinístico, afim de obter a polinomialidade deterministicamente,

4. define-se a subclasse das teorias **I**-localmente estáveis, que é uma restrição das teorias **N**-localmente estáveis que possuem um inverso correspondente a cada símbolo AC presente na assinatura.

Em [1] os autores afirmam que é possível provar que a teoria equacional de Grupos Abelianos é *localmente estável*, no entanto, nenhuma prova de tal fato foi encontrada no trabalho ou na literatura. Na Seção 3.2 o objetivo é verificar se a teoria equacional de grupos Abelianos é **I**-localmente estável, e com isso garantir que esta teoria é estável para reduções de reescrita. Para isto seria preciso definir um conjunto saturado de termos finito que seja adequado para a teoria de grupos Abelianos, satisfazendo as condições de **I**-estabilidade local, o que não foi possível. Pode ser que exista uma definição adequada para o conjunto saturado de termos, mas esta não foi encontrada.

No entanto,

5. restringindo a teoria de grupos Abelianos para modelos finitos foi possível ilustrar o resultado, como pode ser visto na Subseção 3.2.1.

Para mostrar que a teoria equacional de grupos Abelianos de ordem n (dada) é **I**-localmente estável (Proposição 3.4), foi necessário, definir um sistema de reescrita de termos convergente módulo AC.

- Vale ressaltar que não foi encontrado disponível na literatura de reescrita nenhum estudo relacionado a esta classe de teorias equacionais. Dessa forma, a família de sistemas de reescrita convergentes associados a esta classe de teorias, bem como este exemplo de aplicação, são possivelmente inéditos.

Capítulo 4: Problema da Dedução Elementar

Neste capítulo, o objetivo é relacionar a classe de teorias **N**-localmente estáveis (ou **I**-localmente estáveis) com a decidibilidade do *problema da dedução elementar*(PDE) introduzido por A. Tiu, R. Goré e J. Dawson em [41]. Este problema de decisão foi introduzido pelos autores, porém nenhuma teoria equacional para a qual o problema é decidível foi disponibilizada.

- Utilizando os resultados obtidos nos capítulos anteriores, prova-se que a decidibilidade do PDE está em NP para as teorias **N**-localmente estáveis (Teorema 4.2) e em em P para as teorias **I**-localmente estáveis (Teorema 4.1).

Utilizando métodos teóricos básicos de permutabilidade de regras e eliminação de corte, o trabalho [41] mostra que o PDI reduz polinomialmente para o PDE, que recai no problema de resolver certas equações que dependem da teoria equacional subjacente.

Como aplicação dos resultados anteriores, e utilizando a redução polinomial para o PDE, será mostrado que

6. a decidibilidade do PDI para teorias **N**-localmente estáveis combinadas com a teoria de *assinaturas cegas* está em NP (Corolário 4.2), enquanto que para teorias **I**-localmente estáveis combinadas com assinaturas cegas está em P (Corolário 4.1).

Esta aplicação estende o trabalho [1], uma vez que estuda-se a decidibilidade do PDI para uma combinação de teorias sem que seja necessário provar que a teoria combinada resultante seja **N**-localmente estável (ou **I**-localmente estável).

Capítulo 1

Preliminares

Neste capítulo introduz-se noções básicas de álgebra universal (tais como termos, substituições e identidades) em um nível sintático, e também interpretação semântica dessas noções sintáticas (tais como álgebras, homomorfismos, e classes equacionais), seguindo a notação de [7]. Na Seção 1.5 será mostrado que o problema do *Casamento Associativo e Comutativo (CAC)* é NP-completo (via redução polinomial do problema Mono-3SAT), e um caso particular deste problema *Casamento AC com Ocorrências Distintas* pode ser decidido em tempo polinomial com relação à entrada.

1.1 Termos, contextos e substituições

Definição 1.1 (Assinatura)**.** *Uma* assinatura Σ *é um conjunto de* símbolos de função *onde cada* $f \in \Sigma$ *é associado com um inteiro não-negativo* n*, a* aridade *de* f*. Para* $n \geq 0$*, denote o conjunto de todos os* n*-ários de* Σ *por* $\Sigma^{(n)}$*. Os elementos de* $\Sigma^{(0)}$ *são também chamados de símbolos* constantes*.*

Notação: Denote por $ar(f)$ a aridade de f e por $ar(\Sigma)$ a aridade maximal dos símbolos de função em Σ.

Definição 1.2 (Termos)**.** *Seja* Σ *uma assinatura e* X *um conjunto de variáveis tais que* $\Sigma \cap X = \emptyset$*. O conjunto* $T(\Sigma, X)$ *de todos os* Σ*-termos sobre* X *é definido indutivamente da seguinte forma*

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

Definição 1.3 (Posições)**.** *Seja* Σ *uma assinatura,* X *um conjunto de variáveis disjunto de* Σ*, e* $s, t \in T(\Sigma, X)$*.*

1. *O conjunto de* posições *do termo* s *é o conjunto denotado por* $\mathcal{P}os(s)$*, de palavras sobre os inteiros positivos, que é definido indutivamente como segue:*

- *Se* $s = x$, *então* $\mathcal{P}os(s) := \{\varepsilon\}$, *onde* ε *denota a palavra vazia.*
- *Se* $s = f(s_1, \ldots, s_n)$, *então*

$$\mathcal{P}os(s) := \{\varepsilon\} \cup \bigcup_{i=1}^{n} \{ip \mid p \in \mathcal{P}os(s_i)\}$$

A posição ε *é chamada* posição raiz *do termo* s, *e o símbolo de função ou de variável nesta posição é chamada de* símbolo raiz *de* s. *Além disso, diz-se que* s *é* encabeçado *pelo símbolo na sua posição raiz.*

2. *O* tamanho *de um termo* $|s|$ *é a cardinalidade de* $\mathcal{P}os(s)$.

3. *Para* $p \in \mathcal{P}os(s)$, *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 $p = iq$, $p \in \mathcal{P}os(s)$ *implica que* s *é da forma* $s = f(s_1, \ldots, s_n)$, *com* $i \leq n$.

4. *Para* $p \in \mathcal{P}os(s)$, *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* $\mathcal{V}ar(s)$ *o conjunto de* variáveis ocorrendo em s, *i.e.*

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

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

Definição 1.4 (Subtermos Sintáticos)**.** *O conjunto dos* subtermos sintáticos *de um termo* s *é o conjunto* $st(s)$ *dos subtermos* $s|_p$ *para cada* $p \in \mathcal{P}os(s)$. *Isto é,* $S_{sin}(s) := \bigcup_{p \in \mathcal{P}os(s)} s|_p$.

Definição 1.5 (Termos Básicos)**.** *Seja* Σ *uma assinatura e* X *um conjunto de variáveis tais que* $\Sigma \cap X = \emptyset$. *Um termo* $t \in T(\Sigma, X)$ *é chamado* básico *se e somente se* $\mathcal{V}ar(t) = \emptyset$. *O conjunto de todos os termos básicos sobre* Σ *é denotado por* $T(\Sigma, \emptyset)$ *ou simplesmente* $T(\Sigma)$.

Um símbolo de função binário f é *associativo* se,e somente se, satisfaz o seguinte axioma:

$$f(f(x, y), z) = f(x, f(y, z)). \tag{1.1}$$

Um símbolo função binário f é *comutativo* se, e somente se, satisfaz

$$f(x, y) = f(y, x). \tag{1.2}$$

Na sequência um símbolo de função que é associativo e comutativo será chamado de um *operador AC*.

Um termo t que contenha símbolos de função associativos é frequentemente representado na forma *plana*. Por exemplo, se f é associativo, então $f(a, f(b, c))$ é representado por $f(a\, b\, c)$.

Planificar um termo com respeito a uma função f pode ser feito da seguinte forma: primeiro represente o termo da forma associativa à direita. Tal termo será da forma $f(t_1, f(t_2, \ldots, f(t_{n-1}, t_n)\ldots)$ onde $t_1, t_2, \ldots, t_n$ não são encabeçados por f. Então simplesmente represente o termo como $f(t_1\, t_2\, \ldots\, t_n)$. A planificação de um termo pode ser feita em tempo linear com relação ao tamanho do termo.

Definição 1.6 (Substituição)**.** *Seja Σ uma assinatura e V um conjunto infinito enumerável de variáveis. Uma* substituição *é uma função $\sigma : V \to T(\Sigma, V)$, tal que $x\sigma \neq x$ apenas para um número finito de variáveis $x \in V$. Este conjunto (finito) de variáveis é chamado* domínio *de σ:*

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

Se $Dom(\sigma) = \{x_1, \ldots, x_n\}$, então σ pode ser escrito da seguinte forma:

$$\sigma = \{x_1 \mapsto \sigma(x_1), \ldots, x_n \mapsto \sigma(x_n)\}.$$

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

$$\widehat{\sigma} := x, \text{ se } x \in V$$
$$\widehat{\sigma}(f(s)) := f(\widehat{\sigma_1}(s_1), \ldots, \widehat{\sigma_n}(s_n)), \text{ se } s = f(s_1, \ldots, s_n)$$

O conjunto de todas as $T(\Sigma, X)$-substituições será denotado por $\mathcal{S}ub$.

Observação 1.1. *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 1.7. *Considere a substituição $\sigma = \{x_1 \mapsto t_1, \ldots, x_n \mapsto t_n\}$.O* tamanho *da substituição σ, representado por $|\sigma|$ é definido como $|\sigma| := k + \sum_{i=1}^{k} |t_i|$.*

Definição 1.8 (Σ-contexto)**.** *Seja $\Box$ um novo símbolo que não aparece em $\Sigma \cup V$. Um Σ-contexto é um termo $T(\Sigma, V \cup \{\Box\})$ e pode ser visto com um termo com "*buracos*", representados por $\Box$. Contextos são denotados por C.*

Se $\{p_1, \ldots, p_n\} = \{p \in \mathcal{P}os(C) \mid C|_p = \Box\}$, onde p_i está à esquerda de p_{i+1} na representação por árvore de C, então $C[t_1, \ldots, t_n] := C[t_1]_{p_1} \ldots [t_n]_{p_n}$.

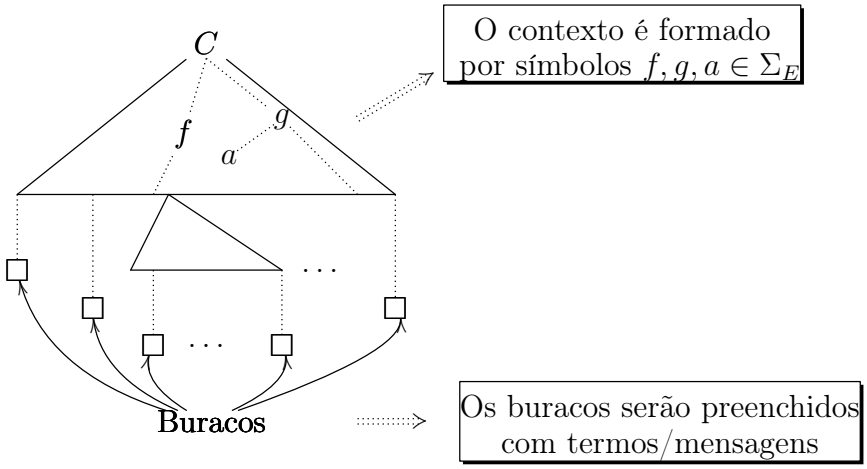


Figura 1.1: Σ-contexto com "buracos"

Definição 1.9 (Σ-identidade)**.** *Seja* Σ *uma assinatura e* V *um conjunto de variáveis infinito e enumerável e disjunto de* Σ*. Uma* Σ*-identidade (ou simplesmente identidade) é um par* $(s, t) \in T(\Sigma, V) \times T(\Sigma, V)$*. O* lado direito *(ld) é dado por* s *e o* lado esquerdo *(le) por* t*.*

Notação: $s \approx t$

Definição 1.10 (Relação de Redução)**.** *Seja* E *um conjunto de* Σ*-identidades. A* relação de redução $\rightarrow_E \subseteq T(\Sigma, V) \times T(\Sigma, V)$ *é definida como*

$$s \rightarrow_E t \text{ sse } \exists\, (l, r) \in E,\ p \in \mathcal{P}os(s),\ \sigma \in \mathcal{S}ub.\ s|_p = \sigma(l) \text{ e } t = s[\sigma(r)]_p.$$

1.2 Álgebras, homomorfismos e congruências

Para uma dada assinatura Σ, uma Σ-álgebra provê uma interpretação de todos os símbolos de função em Σ.

Definição 1.11 (Σ-álgebra)**.** *Seja* Σ *uma assinatura. Uma* Σ*-álgebra* $\mathcal{A}$ *consiste de*

- *um* domínio A*, e*
- *uma aplicação que associa a cada símbolo de função* $f \in \Sigma^{(n)}$ *uma função* $f^{\mathcal{A}} : A^n \rightarrow A$ *(para todo* $n \geq 0$*).*

Se a assinatura é irrelevante ou clara no contexto, usa-se simplesmente o termo "álgebra" ao invés de Σ-álgebra.

Como um exemplo, considere a assinatura $\Sigma_G = \{e, i, f\}$, onde e tem aridade 0, i é unário, e f é binário. O grupo aditivo dos inteiros $\mathcal{Z}$, tem como domínio o conjunto de todos os inteiros $\mathbb{Z}$, e interpreta f como adição de inteiros, i como o inverso aditivo (unário), e e como 0.

Definição 1.12 (Σ-homomorfismo)**.** *Seja Σ uma assinatura, e sejam $\mathcal{A}, \mathcal{B}$ Σ-álgebras. Um* Σ-homomorfismo *$\phi : \mathcal{A} \to \mathcal{B}$ é um mapeamento de A em B tal que para todo $n \geq 0$, $f \in \Sigma^{(n)}$, e $a_1, \ldots, a_n \in A$ tem-se que $\phi(f^{\mathcal{A}}(a_1, \ldots, a_n)) = f^{\mathcal{B}}(\phi(a_1), \ldots, \phi(a_n))$.*

Definição 1.13 (Congruência)**.** *Seja $\mathcal{A}$ uma Σ-álgebra. Uma relação de equivalência $\equiv$ em seu domínio A é chamada de* congruência *em $\mathcal{A}$ se e, somente se, $\equiv$ é compatível com a interpretação de todos os símbolos de função de Σ, isto é, para todo $n \geq 0$, $f \in \Sigma^{(n)}$, e todo $a_1 \equiv b_1, \ldots, a_n \equiv b_n$ em A tem-se que*

$$f^{\mathcal{A}}(a_1, \ldots, a_n) \equiv f^{\mathcal{A}}(b_1, \ldots, b_n)$$

A álgebra quociente *$\mathcal{A}/_{\equiv}$ tem como domínio o conjunto das classes de equivalência $[a]_{\equiv} := \{b \in A \mid a \equiv b\}$, e interpreta os símbolos, $f \in \Sigma^{(n)}$ (para todo $n \geq 0$) como*

$$f^{\mathcal{A}/\equiv}([a_1]_{\equiv}, \ldots, [a_n]_{\equiv}) := [f^{\mathcal{A}}(a_1, \ldots, a_n)]_{\equiv}.$$

Para um assinatura Σ e um conjunto de variáveis X (disjunto), pode-se usar $T(\Sigma, X)$ como domínio de uma Σ-álgebra em que os símbolos de função "interpretam a si mesmos".

Definição 1.14 (Σ-álgebra de termos)**.** *Seja Σ uma assinatura e X um conjunto de variáveis disjunto de Σ. A* Σ-álgebra de termos *$\mathcal{T}(\Sigma, X)$ tem $T(\Sigma, X)$ como domínio, e interpreta os símbolos de função $f \in \Sigma^{(n)}$ (para $n \geq 0$) da seguinte forma:*

$$\begin{aligned} f^{\mathcal{T}(\Sigma,X)} : T(\Sigma, X)^n &\to T(\Sigma, X) \\ (t_1, \ldots, t_n) &\mapsto f(t_1, \ldots, t_n). \end{aligned}$$

1.3 Classes Equacionais

Uma Σ-identidade é um par $s \approx t$ de termos em $T(\Sigma, V)$, para um conjunto infinito enumerável de variáveis V. Intuitivamente, uma identidade acontece em uma Σ-álgebra $\mathcal{A}$ se ela for verdadeira para todas as possíveis maneiras de se substituir as variáveis em s, t por um elemento de A. A definição formal dada abaixo faz uso do fato de que um dado mapeamento de variáveis em elementos de A pode ser unicamente extendido a um homomorfismo.

Definição 1.15. *A Σ-identidade $s \approx t$* acontece *na Σ-álgebra $\mathcal{A}$ ($\mathcal{A} \models s \approx t$) sse para todo homomorfismo $\phi : \mathcal{T}(\Sigma, V) \to \mathcal{A}$ tem-se que $\phi(s) = \phi(t)$.*

Definição 1.16. *Seja Σ uma assinatura e seja E um conjunto de Σ-identidades.*

1. *A Σ-álgebra $\mathcal{A}$ é um* modelo *de E ($\mathcal{A} \models E$) sse toda identidade E acontece em $\mathcal{A}$.*
2. *A classe de todos os modelos de E é chamada de Σ-variedade definida por E. E é denotada por $\mathcal{V}(E)$.*

Definição 1.17. *Seja E um conjunto de Σ-identidades.*

1. *A identidade* $s \approx t$ *é uma* consequência semântica *de* E *(*$E \models s \approx t$*) sse ela acontece em todos os modelos de* E*, isto é, para todo* $\mathcal{A} \in \mathcal{V}(E)$ *tem-se que* $s \approx t$ *acontece em* $\mathcal{A}$*.*

2. *A relação*
$$\approx_E := \{(s,t) \in T(\Sigma, V) \times T(\Sigma, V) \mid E \models s \approx t\}$$
é chamado de teoria equacional *induzida por* E*.*

3. *O conjunto de identidades* E *é chamado* trivial *sse* $\approx_E = T(\Sigma, V) \times T(\Sigma, V)$*.*

Observe que $s \approx t \in E$ implica que $s \approx_E t$. Além disso, a relação $\approx_E$ é uma relação de congruência em $\mathcal{T}(\Sigma, V)$. Pode-se construir a álgebra quociente $\mathcal{T}(\Sigma, V)/_{\approx_E}$.

Definição 1.18 (E-Congruência)**.** *Seja* E *um conjunto de equações. Denote por* Σ_E *o conjunto de todos os símbolos de função ocorrendo em* E *e por* $\approx_E$ *a menor congruência em* $T(\Sigma, V)$ *gerada por* E*, isto é, a menor relação de equivalência gerada por* E *que é compatível com substituições e a estrutura de termos: para toda substituição* σ*, se* $u \approx_E v$*, então para todo termo* t *e* $p \in \mathcal{P}os(t)$*, tal que* $t = t[u\sigma]_p$*,* $t[u\sigma]_p \approx_E t[v\sigma]_p$*.*

Definição 1.19 (Casamento)**.** *O* problema do casamento *é dado por: dados dois termos* s *e* l*, determine se existe uma substituição* σ *tal que* $l\sigma = s$*, e compute* σ *se ele existir.*

Uma substituição σ é dita *casar* um termo s com um termo l se, e somente se, $s = l\sigma$. Neste caso, s é chamado de *padrão* e l de *sujeito*.

Teorema 1.1. *Seja* E *um conjunto de* Σ*-identidades. Se* E *é finito e* $\rightarrow_E$ *é convergente, então* $\approx_E$ *é decidível.*

Definição 1.20 (E-Unificador)**.** *Seja* E *um conjunto de* Σ*-identidades. Dois termos* s *e* t *são chamados* E-unificáveis *se existe uma substituição* σ *tal que* $s\sigma \approx_E t\sigma$*. Tal substituição é chamada* E-unificador *de* s *e* t*.*

1.4 Sistema de Reescrita de Termos

A seguir, E denota um conjunto de Σ-identidades.

Definição 1.21 (Sistema de reescrita de termos)**.** *Um* sistema de reescrita de termos *(SRT) é um conjunto de regras de reescrita. Uma* regra de reescrita *é dada por* $l \rightarrow r$ *onde* $l, r \in T(\Sigma, V)$ *e* l *não é uma variável e* $\mathcal{V}ar(l) \supseteq \mathcal{V}ar(r)$*.*

Observação 1.2 (Redex/Contração)**.** *Um* redex *(ou expressão redutível) é uma instância de um lado esquerdo de uma regra. A* contração *de um redex significa substituí-lo pela instância correspondente do lado direito da regra.*

Definição 1.22 (Relação de reescrita gerada por um SRT)**.** *Seja $\mathcal{R}$ um SRT. A* relação de reescrita $\rightarrow_{\mathcal{R}} \subseteq T(\Sigma, V) \times T(\Sigma, V)$ *é definida por*

$$s \rightarrow_{\mathcal{R}} t \text{ sse existe uma posição } p \in \mathcal{P}os(s) \text{ tal que } s|_p = l\sigma \text{ e } t = s[r\sigma]_p$$

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 SRT $\mathcal{R}$.*

Definição 1.23 (Terminalidade)**.** *Um SRT $\mathcal{R}$ é dito* terminante *se não existem sequências infinitas do tipo $t_1 \rightarrow_{\mathcal{R}} t_2 \rightarrow_{\mathcal{R}} \ldots$.*

Definição 1.24 (Confluência)**.** *Um SRT $\mathcal{R}$ é dito* confluente *se, e somente se,*

$$y_1 \overset{*}{\leftarrow}_{\mathcal{R}} x \overset{*}{\rightarrow}_{\mathcal{R}} y_2 \Rightarrow y_1 \downarrow_{\mathcal{R}} y_2.$$

O símbolo $\overset{*}{\rightarrow}$ representa o *o fecho associativo e comutativo* de $\rightarrow$, *i.e.*, $\overset{*}{\rightarrow} := \overset{+}{\rightarrow} \cup \overset{0}{\rightarrow}$, onde $\overset{+}{\rightarrow} := \bigcup_{i>0} \overset{i}{\rightarrow}$.

Definição 1.25 (Convergência)**.** *Um SRT $\mathcal{R}$ é dito* convergente *quando $\mathcal{R}$ é terminante e confluente.*

Definição 1.26 (Forma Normal)**.** *Um termo t está na* forma normal *(w.r.t $\mathcal{R}$) se não existe um termo s tal que $t \rightarrow_{\mathcal{R}} s$. Se $t \overset{*}{\rightarrow}_{\mathcal{R}} s$ e s está na forma normal então s é uma forma normal de t. Quando está na forma normal é única ($\mathcal{R}$ é convergente), denota-se por $t \downarrow_{\mathcal{R}}$.*

A seguir, o símbolo $\oplus$ representa um operador AC arbitrário.

Definição 1.27 (Encabeçado com $\oplus$)**.** *Seja u um termo na forma normal, u é encabeçado com $\oplus$ se u é da forma $u_1 \oplus u_2 \oplus \ldots \oplus u_n$, $n > 1$. Caso contrário, u não é encabeçado com $\oplus$.*

Definição 1.28 (Átomo)**.** *Seja u um termo, defina a função $atomos(u)$ da seguinte forma:*

- *Se $u = u_1 \oplus u_2 \oplus \ldots \oplus u_n$, onde cada u_i não é encabeçado por $\oplus$ para $1 \leq i \leq n$, então $atomos(u) = \{u_1, \ldots, u_n\}$.*
- *Se u não é encabeçado com $\oplus$, então $atomos(u) = u$.*

Definição 1.29 (Reescrita Módulo E)**.** *Considere um SRT $\mathcal{R}$ e o conjunto de Σ-identidades E. A* relação de reescrita módulo E, *é a relação $\rightarrow_{\mathcal{R}/E}$ definida por:*

$$s \rightarrow_{\mathcal{R}/E} t \text{ sse, existe uma posição } p \in \mathcal{P}os(s) \text{ tal que } s|_p \approx_E l\sigma \text{ e } t = s[r\sigma]_p$$

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

Definição 1.30 (Confluência módulo E)**.** *Um sistema de reescrita $\mathcal{R}$ é E-confluente se, e somente se, para todos os termos s e t tais que $s \approx_{\mathcal{R} \cup E} t$, existem s' e t' tais que $s \overset{*}{\rightarrow}_{\mathcal{R}/E}$, $t \overset{*}{\rightarrow}_{\mathcal{R}/E} t'$ e $s' \approx_E t'$. $\mathcal{R}$ é dito E-convergente se, além disso, $\rightarrow_{\mathcal{R}/E}$ é terminante.*

Onde por $s \approx_{\mathcal{R} \cup E} t$ entende-se: $[s]_{\approx_E} \leftrightarrow^*_{\mathcal{R}/E} [t]_{\approx_E}$

Mais ainda, se $\rightarrow_{\mathcal{R}/E}$ é convergente, então $s \approx_{\mathcal{R}/E} t \Leftrightarrow ([s]_{\approx_E} \downarrow_{\mathcal{R}/E}) = ([t]_{\approx_E} \downarrow_{\mathcal{R}/E})$ acontece. O fecho de equivalência da relação de reescrita, $\overset{*}{\leftrightarrow}_{\mathcal{R}}$, é denotado por $\approx_{\mathcal{R}}$.

Definição 1.31 (Redução na Cabeça)**.** *Seja $\mathcal{R}$ um SRT convergente módulo AC.*

Para uma regra $l \rightarrow r \in \mathcal{R}$ e uma substituição θ tais que

- *ou existe um termo s_1 tal que $s \approx_{AC} s_1$, $s_1 \approx_{AC} l\theta$ e $t = r\theta$;*
- *ou existem termos s_1 e s_2 tais que $s \approx_{AC} s_1 \oplus s_2$, $s_1 \approx_{AC} l\theta$ e $t \approx_{AC} r\theta \oplus s_2$.*

Então $s \overset{h}{\rightarrow} t$.

Neste caso diz-se que a redução ocorre na "cabeça".

Denota-se por Σ_E a assinatura relativa a E, isto é, o conjunto de símbolos de função envolvidos nas identidades de E.

Definição 1.32 (E-contexto)**.** *Seja $\approx_E$ uma teoria equacional e seja Σ_E a assinatura relativa a E. Um E-*contexto *é um termo $T(\Sigma_E, V \cup \{\Box\})$, isto é, um contexto formado com símbolos de função de Σ_E.*

Uma teoria equacional $\approx_E$ induzida por E é dita *convergente* se possuir um SRT associado $\mathcal{R}_E$, convergente.

Definição 1.33 (E-contexto normal)**.** *Seja $\approx_E$ uma teoria equacional convergente e seja $\mathcal{R}_E$ o SRT associado. Seja C um E-contexto com n buracos e seja T o termo obtido de C através da substituição de cada buraco por $x_1, \ldots, x_n$, onde $x_i \neq x_j$, para $i \neq j$ $(1 \leq i, j \leq n)$. O contexto C é dito ser* normal *sse não existem $p \in \mathcal{P}os(C)$, tal que p não é uma posição de buraco e uma regra $l \rightarrow r \in \mathcal{R}_E$ tal que o problema de casamento $T|_p =^? l\sigma$ tenha solução.*

Observação 1.3. *Este conceito pode ser estendido para sistemas de reescrita de termos AC-convergentes: Dada uma teoria equacional $\approx_E$ associada a um SRT AC-convergente $\mathcal{R}_E$, um E-contexto C é dito estar na forma AC-*normal *se não existe posição $p \in \mathcal{P}os(C)$ tal que $C|p =_{AC} l\sigma$ para alguma regra $l \rightarrow r \in \mathcal{R}_E$ e alguma substituição σ.*

Exemplo 1.1. *Considere a assinatura $\Sigma = \{+, i, 0\}$ para grupos Abelianos.*

A teoria equacional de grupos Abelianos é:

$$E_{AG} = \begin{cases} x + (y + z) &= (x + y) + z \\ x + y &= y + x \\ x + 0 &= x \\ x + i(x) &= 0 \\ i(x + y) &= i(x) + i(y) \end{cases}$$

O sistema de reescrita de termos associado é :

$$\mathcal{R}_{AG} = \begin{cases} x + 0 \rightarrow x & (1) \\ x + i(x) \rightarrow 0 & (2) \\ i(i(x)) \rightarrow x & (3) \\ i(0) \rightarrow 0 & (4) \\ i(x + y) \rightarrow i(x) + i(y) & (5) \end{cases}$$

Seja C o seguinte Σ-contexto: $C = i(0) + \Box$.
Observe que

$$\begin{aligned} C &= i(0) + \Box \text{ via regra } i(0) \to 0 \\ &\to 0 + \Box \text{ via regra } x + 0 \to x \\ &\to \Box = C' \end{aligned} \tag{1.3}$$

O E_{AG}-contexto C não está na forma normal *uma vez que reduz para o E_{AG}-contexto C': $C \xrightarrow{*} C'$. O E_{AG}-contexto C' está na forma* normal.

Proposição 1.1. *Seja E uma teoria equacional cujo SRT associado $\mathcal{R}_E$ é convergente. Todo E-contexto C pode ser normalizado para um E-contexto C' via $\mathcal{R}_E$.*

Demonstração. Reduza C a partir do redex na posição mais acima. Repita o procedimento, recursivamente, até obter: C': $C \xrightarrow{*}_{\mathcal{R}_E} C'$. □

Definição 1.34 (Tamanho da Teoria Equacional)**.** *O* tamanho c_E *de uma teoria equacional $\approx_E$ (induzida por E) com SRT associado $\mathcal{R}_E$ e que consiste das regras $\bigcup_{i=1}^{k}\{l_i \to r_i\}$ é definido por $c_E = max_{1\leq i\leq k}\{|l_i|, |r_i|, ar(\Sigma) + 1\}$. Para $\mathcal{R} = \emptyset$, defina $c_E = ar(\Sigma) + 1$.*

Definição 1.35 (E-alien)**.** *Um termo M é dito ser* E-alien *se M é encabeçado por um símbolo $f \notin \Sigma_E$ ou por um nome/constante privado.*

Escrevemos $M == N$ para denotar igualdade sintática de termos básicos.

1.5 Casamento associativo-comutativo

Casamento associativo-comutativo e *algoritmos de unificação* tem um papel importante no raciocínio automático, na verificação de programas, análise de especificação, etc., quando certos operadores tem propriedades associativas-comutativas. Em [9], D. Benanav, D. Kapur, e P. Narendran mostram que o *problema do casamento associativo-comutativo* (Casamento AC) é NP-completo.

Este problema de decisão pode ser formulado da seguinte forma:

Problema 1.1 (Casamento associativo-comutativo - CAC)**.**
Instância: *Um conjunto de variáveis V, uma assinatura Σ que contém símbolos de função associativo e comutativo, e termos $t_1, t_2 \in T(\Sigma, V)$.*
Pergunta: *Existe uma substituição σ tal que $t_1\sigma =_{AC} t_2$?*

Problemas de decisão tem apenas duas soluções possíveis, ou a resposta é "SIM" ou a resposta é "NÃO". Isto é, um problema de decisão Π consiste simplesmente de um conjunto D_Π de *instâncias* e um subconjunto $Y_\Pi \subseteq D_\Pi$ de instâncias-SIM.

Uma instância pertence a D_Π se, e somente se, ela pode ser obtida a partir de uma instância genérica, através da substituição de componentes genéricos por objetos particulares dos tipos especificados; e uma instância pertence a Y_Π se, se somente se, a resposta para pergunta, quando particularizada é "SIM".

Definição 1.36 (Transformação Polinomial)**.** *Uma* transformação polinomial *de um problema de decisão* Π_1 *para um problema de decisão* Π_2 *é uma funcão* $f : D_{\Pi_1} \to D_{\Pi_2}$ *que satisfaz duas condições:*

- f *é computável por um algoritmo de tempo polinomial; e*
- *para todo* $I \in D_{\Pi_1}$, $I \in Y_{\Pi_1}$ *se, e somente se,* $f(I) \in Y_{\Pi_2}$.

Se existir uma transformação polinomial de Π_1 *para* Π_2, *escreva* $\Pi_1 \propto \Pi_2$.

A seguir, será mostrado que CAC é NP-completo. Para isto é necessário mostrar que

- $CAC \in NP$;
- para qualquer outro problema de decisão $\Pi \in NP$, $\Pi \propto CAC$.

O seguinte lema dá uma alternativa para esta prova.

Lema 1.1. *Se* $\Pi_1, \Pi_2 \in NP$, Π_1 *é NP-completo, e* $\Pi_1 \propto \Pi_2$, *então* Π_2 *é NP-completo.*

Abaixo, utilizando a transformação Mono-3SAT $\propto CAC$, juntamente com o fato de Mono-3SAT ser NP-completo, segue que CAC é NP-completo.

Problema 1.2 (3SAT Monótono - Mono-3SAT)**.**
Instância: *Um conjunto de variáveis proposicionais* $U = \{z_1, z_2, \ldots, z_m\}$, *um conjunto de cláusulas* $C = \{c_1, c_2, \ldots, c_n\}$ *onde cada cláusula é um conjunto de três literais, e cada literal é* z_i *ou* $\overline{z_i}$ *para* $1 \leq i \leq m$.
Pergunta: *Existe uma designação de verdade* $I : U \to \{0, 1\}$ *tal que* C *é verdadeiro?*

Teorema 1.2. *Mono-3SAT é NP-completo [28].* □

A seguir, mostra-se que o problema CAC é NP-completo. Para esta prova utiliza-se uma transformação polinomial entre Mono-3SAT e CAC.

Definição 1.37. *Seja* $I : U \to \{1, 0\}$ *uma designação-verdade e uma cláusula* c *então* $Image(c, I) = \{(1, n), (0, m)\}$ *onde* n *é o* número de literais positivos em c *e* m *é o* número de literais negativos em c *via* I.

Teorema 1.3 ([9])**.** *CAC é NP-completo.*

Demonstração. $CAC \in NP$: Sejam t_1, t_2 termos e θ uma substituição tal que $t_1\theta =_{AC} t_2$. Claramente, o tamanho de θ não pode ser maior que $(|t_1| + |t_2|)$. Então, dados dois termos t_1 e t_2 como entrada, deve-se fazer

1. escolha θ tal que $|\theta| \leq (|t_1| + |t_2|)$,

   Existem, no máximo, $k \leq |t_1|$ ocorrências de variáveis do domínio de θ, dado por $\mathcal{D}om(\theta) = \{x_1, \ldots, x_k\}$, em t_1. Para cada variável $x_i \in \mathcal{D}om(\theta)$, associa-se um termo s_i via θ. No total, $\sum_{i=1}^{k} |s_i| \leq |t_2|$. Logo, $|\theta| \leq |t_1| + |t_2|$.

2. aplique θ a t_1 para obter um novo termo t_1', e

3. verifique se $t_1' =_{AC} t_2$.

O passo 2 pode ser feito em tempo polinomial. O passo 3 também pode ser feito em tempo polinomial, uma vez que $ACEQ \in P$ [9].

Logo, $CAC \in NP$ (o passo 1 induz o não-determinismo).

Afirmação: *Mono-3SAT* $\propto$ *CAC.*

Para provar tal afirmação, mostra-se que uma instância de Mono-3SAT é polinomialmente transformável em uma instância de CAC.

Considere a seguinte instância de Mono-3SAT: $U = \{z_1, z_2, \ldots, z_m\}$ um conjunto de variáveis e $C = \{c_1, c_2, \ldots, c_n\}$, um conjunto de cláusulas.

Para a instância de CAC: $U' = \{u_{11}, u_{12}, \ldots, u_{n1}, u_{n2}\}$ um conjunto de variáveis com $U \cap U' = \emptyset$, $V = U \cup U'$ e $\Sigma = \{f, g, 1, 0\}$, onde f é um operador AC, g um operador de aridade n que não é nem comutativo e nem associativo, e 1 e 0 constantes.

Pode-se mostrar que dois termos $t_1, t_2 \in T(\Sigma, V)$ podem ser construídos em tempo polinomial com respeito à entrada de tal forma que C é satisfatível se, e somente se, existe um θ tal que $\theta(t_1) =_{AC} t_2$.

Primeiro, para construir a transformação polinomial, defina:

$$H : \text{Cláusulas} \rightarrow \text{ Termos}$$
$$H(c_i) = f(z_1\, z_2\, z_3\, u_{i1}\, u_{i2}) \text{ se } c_i = \{z_1, z_2, z_3\} \text{ ou se } c_i = \{\overline{z_1}, \overline{z_2}, \overline{z_3}\}$$

e

$$G : \text{Cláusulas} \rightarrow \text{ Termos}$$
$$G(c_i) = f(1\,1\,1\,0\,0) \text{ se } c_i = \{z_1, z_2, z_3\}$$
$$= f(0\,0\,0\,1\,1) \text{ se } c_i = \{\overline{z_1}, \overline{z_2}, \overline{z_3}\}$$

Agora, sejam $t_1 = g(s_1\, s_2\, \ldots\, s_n)$ onde $s_i = H(c_i)$ e $t_2 = g(s_1'\, s_2'\, \ldots\, s_n')$ onde $s_i' = G(c_i)$. Estes termos podem ser construídos em tempo polinomial com respeito à entrada.

- Suponha que exista um θ tal que $\theta(t_1) =_{AC} t_2$.

  Seja $I : U \rightarrow \{1, 0\}$ definida por $I(v) = \theta(v)$.

  Uma vez que g não é nem associativa e nem comutativa, para todo i, $\theta(s_i) =_{AC} s_i'$.

  Suponha que $c_i = \{z_1, z_2, z_3\}$. Então, por construção, $s_i = H(c_i) = f(z_1\, z_2\, z_3\, u_{i1}\, u_{i2})$ e $s_i' = G(c_i) = f(1\,1\,1\,0\,0)$ e então, $\theta(f(z_1\, z_2\, z_3\, u_{i1}\, u_{i2})) =_{AC} f(1\,1\,1\,0\,0)$. Observe que isto é verdade se, e somente se, 3 e apenas 3 das variáveis em $\{z_1, z_2, z_3, u_{i1}, u_{i2}\}$ mapeiam para 1 via substituição θ. Como, no máximo ambas as variáveis u_{i1} e u_{i2} mapeiam para 1 via θ, então ou z_1, z_2 ou z_3 mapeiam para 1 via θ. Portanto, a cláusula c_i é satisfeita por I.

  Da mesma forma, se $c_i = \{\overline{z_1}, \overline{z_2}, \overline{z_3}\}$ então $\theta(f(z_1\, z_2\, z_3\, u_{i1}\, u_{i2})) =_{AC} f(0\,0\,0\,1\,1)$ e então z_1, z_2 ou z_3 mapeiam para 0 via θ e então $\overline{z_1}, \overline{z_2}$ ou $\overline{z_3}$ mapeiam para 1 via θ.

  Logo, C é satisfeito por I pois $I = \theta$ e toda cláusula é satisfeita via I.

- Suponha que C é satisfatível.

  Seja $I : U \to \{0, 1\}$ uma atribuição de verdade satisfazendo C. Uma substituição θ satisfazendo $\theta(t_1) =_{AC} t_2$ será construída.

  Particione C nas seguintes classes:

$$
\begin{aligned}
P_1 &= \{c_i \,|\, c_i \text{ é positivo e } Image(c_i, I) = \{(1,1),(0,2)\}\} \\
P_2 &= \{c_i \,|\, c_i \text{ é positivo e } Image(c_i, I) = \{(1,2),(0,1)\}\} \\
P_3 &= \{c_i \,|\, c_i \text{ é positivo e } Image(c_i, I) = \{(1,3),(0,0)\}\} \\
N_1 &= \{c_i \,|\, c_i \text{ é negativo e } Image(c_i, I) = \{(0,1),(1,2)\}\} \\
N_2 &= \{c_i \,|\, c_i \text{ é negativo e } Image(c_i, I) = \{(0,2),(1,1)\}\} \\
N_3 &= \{c_i \,|\, c_i \text{ é negativo e } Image(c_i, I) = \{(0,3),(1,0)\}\}
\end{aligned}
$$

  Defina

$$
\begin{aligned}
\theta(v) &= I(v) \text{ para } v \in U \\
\theta(u_{i1}) &= 1 \text{ se } c_i \in P_1 \cup P_2 \cup N_2 \cup N_3 \\
\theta(u_{i1}) &= 0 \text{ se } c_i \in P_3 \cup N_1 \\
\theta(u_{i2}) &= 1 \text{ se } c_i \in P_1 \cup N_3 \\
\theta(u_{i2}) &= 0 \text{ se } c_i \in P_2 \cup P_3 \cup N_1 \cup N_2
\end{aligned}
$$

  Para $c_i \in P_1 \cup P_2 \cup P3$ tem-se que

$$\theta(s_i) = \theta(H(c_i)) =_{AC} f(1\,1\,1\,0\,0) = G(c_i) = s'_i$$

  e que para $c_i \in N_1 \cup N_2 \cup N_3$

$$\theta(s_i) = \theta(H(c_i)) =_{AC} f(0\,0\,0\,1\,1) = G(c_i) = s'_i.$$

  Logo, para todo i, $\theta(s_i) =_{AC} s'_i$ e $\theta(g(s_1\, s_2\, \ldots s_n)) =_{AC} g(s'_1\, s'_2\, \ldots s'_n)$.

□

1.5.1 Casamento AC com Ocorrências Distintas

Em uma versão restrita de AC-casamento, onde toda variável no termo sendo "casado" tem uma única ocorrência, o problema tem um limitante superior $\mathcal{O}(|s| \times |t|^3)$, onde s e t são respectivamente o padrão e o sujeito.

Problema 1.3 (CAC-OD:CAC com Ocorrências Distintas)**.**
Instância: *Um conjunto de símbolos de variáveis V, uma assinatura Σ que contém símbolos de função associativos e comutativos, e termos $t_1, t_2 \in T(\Sigma, V)$ tais que toda variável em t_2 ocorre apenas uma vez.*
Questão: *Existe uma substituição σ tal que $t_1\sigma =_{AC} t_2$?*

O seguinte teorema afirma que CAC-OD pode ser resolvido em tempo polinomial com relação à $|s|$ e $|t|$. A ideia por traz do algoritmo é a seguinte: se dois termos, digamos t_1 e t_2 que não possuam nenhuma variável em comum podem ser "casados" com s_1 e s_2 respectivamente, então uma substituição que faz ambos casamentos "simultaneamente" pode ser encontrada. Esta substituição é simplesmente a *união* das duas substituições iniciais, uma vez que, nenhum conflito é possível.

IDEIA DA PROVA. Para casar dois termos planificados da forma $t = f(t_1 \dots t_n)$ e $s = f(s_1 \dots s_n)$ será necessário: para cada t_i encontrar um s_j que pode ser casado, de forma que dois t_i's não são casados com o mesmo s_j. Em outras palavras, é necessária uma bijeção $\pi : \{1, \dots, n\} \to \{1, \dots, n\}$ tal que t_i pode ser casado com $s_{\pi(i)}$. Esta bijeção pode ser encontrada recursivamente através dos seguintes passos:

- Para cada t_i encontre todos os s_j's que casam com ele. Isto pode ser feito através de uma busca por exaustão.
- Forme um grafo G bipartido não-direcionado n-por-n com nós correspondendo a cada t_i e s_j tal que existe uma aresta entre os nós t_i e s_j se, e somente se, t_i pode ser casado com s_j.
- Verifique se existe um casamento no grafo G de tamanho n.

Um casamento M em um grafo $G = (V, E)$ é um subconjunto das arestas com a propriedade que duas arestas de M não compartilham o mesmo vértice.

Dado um grafo $G = (V, E)$ o *Problema do Casamento de Grafos* é o problema de encontrar um casamento maximal M de G.

Suponha que $B = (W, E)$ seja um grafo que tenha a seguinte propriedade: O conjunto de vértices W pode ser particionado em dois conjuntos V e U e cada aresta em E tem um vértice em V e um vértice em U. B é chamado *Grafo Bipartido* $B = (V, U, E)$.

Lema 1.2 ([9]). *Sejam $t = f(t_1 \dots t_n)$ e $s = f(s_1 \dots s_n)$ dois termos planificados, onde t_i's não são variáveis. Se existir uma bijeção $\pi : \{1, \dots, n\} \to \{1, \dots, n\}$ e uma substituição ψ tal que $\psi(t_i) =_{AC} s_{\pi(i)}$ então $\psi(t) =_{AC} s$.*

Teorema 1.4 ([9]). *Sejam $t = f(t_1 \dots t_n)$ e $s = f(s_{n+1}\, s_{n+2} \dots s_{n+m})$ onde f é um operador AC, $\mathcal{V}ar(s) \cap \mathcal{V}ar(t) = \emptyset$ e #(ocorrências de v em t)=1 para todo $v \in \mathcal{V}ar(t)$. Seja $G = \langle V, U, E\rangle$ um grafo bipartido com*

$V = \{i \mid i \leq n$ e t_i não é uma variável$\}$

$\overline{V} = \{1, \dots, n\} - V$

$U = \{n + 1, \dots, n + m\}$

$E = \{(i, j) \mid i \in V$ e $j \in U$ e existe θ tal que $\theta(t_i) =_{AC} s_j\}$

Então, vale o seguinte:

Existe ψ tal que $\psi(t) =_{AC} s$ se, e somente se

1. *Existe um casamento máximo M de G com $|M| = |V|$;*
2. *$n \leq m$ e*

3. $m > n \implies \overline{V} \neq \emptyset$.

Demonstração. ($\Rightarrow$) Suponha que existe ψ tal que $\psi(t) =_{AC} s$ então as condições 1, 2 e 3 valem.

Sejam t, s termos satisfazendo as condições do teorema e $G = \langle V, U, E\rangle$ definido acima. Como, por hipótese, existe ψ tal que $\psi(t) =_{AC} s$, então existe um casamento maximal M em G, basta tomar $\theta = \psi$. Observe que $|M| = |V|$, uma vez que os termos de $\overline{V}$ podem ser associados aos termos de s de várias maneiras. Temos que $n \leq m$ ou $m > n$. No último caso, $\overline{V} \neq \emptyset$. O caso em que $n > m$ é absurdo.

($\Leftarrow$) Suponha que $1, 2$ e 3 aconteçam.

Uma vez que $|M| = |V|$, e M é um casamento, então, para cada $i \in V$ existe um único $\{i, j\} \in M$. Para cada i seja θ_i uma susbstituição tal que $\theta_i(t_i) =_{AC} s_j$ onde $\{i, j\} \in M$. Por definição de E sabe-se que pelo menos um tal θ_i existe.

Seja ψ' a substituição definida por $\psi' = \cup_{i \in V} \theta_i$.

Observe que ψ' é bem definida uma vez que as variáveis em t_i e t_j são sempre distintas para $i \neq j$.

- Suponha que $\overline{V} = \emptyset$.

  Então $m \leq n$ (pela condição 3). Uma vez que $n \leq m$ (2) segue que $m = n$. A aplicação definida por $\pi(i) = j$ se $\{i, j\} \in M$ define uma funcão injetora de V sobre U. De fato, suponha que $\pi(i) = \pi(i')$. Então $\{i, \pi(i)\} \in M$ e $\{i', \pi(i')\} \in M$. Agora, se $i \neq i'$ então $\{i, \pi(i)\} \in M$ e $\{i', \pi(i')\} \in M$ seriam arestas distintas de M com um elemento em comum, $\pi(i)$ e $\pi(i')$. Entretanto, como M é um casamento, isto não pode acontecer, dessa forma $i = i'$.

  Além disso, π satisfaz $\pi(t_i) = s_{\pi(i)}$ e uma vez que $\theta_i(t_i) = \psi'(t_i)$, pela definição de ψ', então $\psi'(t_i) = s_{\pi(i)}$. Logo, pelo Teorema 1.2 , $\psi'(t) =_{AC} s$.

- Suponha que $\overline{V} \neq \emptyset$.

  Suponha que $\overline{V} = \{n_1, \ldots, n_k\}$ e seja $U' = \{j \mid j \in U$ e para todo $i, i \in V \Rightarrow \{i, j\} \in M\}$. Seja $U - U' = \{m_1, \ldots, m_p\}$. Seja ψ a substituição definida por:

$$\psi(v) = \begin{cases} s_{m_i}, & \text{para } v = t_{n_i},\ i \in \{1, \ldots, k-1\} \\ f(s_k \ldots s_{m_p}), & \text{para } v = t_{n_k} \\ \psi'(v), & \text{caso contrário.} \end{cases}$$

  Portanto, $\psi(t) =_{AC} s$.

□

O *problema do casamento para grafos bipartidos* é um caso especial do problema de casamento para grafos, o algoritmo de casamento de grafos bipartidos [38] resolve o problema para o casamento do grafo bipartido $B = (V, U, E)$ em tempo $\mathcal{O}(min(|V|, |U|).|E|)$.

Teorema 1.5 ([9]). *CAC-OD pode ser resolvido em tempo polinomial.*

Demonstração. Dados dois termos $t = f(t_1 \ldots t_n)$ e $s = f(s_{n+1} \ldots s_{n+m})$ tais que $\mathcal{V}ar(s) \cap \mathcal{V}ar(t) = \emptyset$ e #(ocorrências de v em t para todo $v \in \mathcal{V}ar(t)) = 1$, e o grafo $G = \langle V, U, E \rangle$ pode-se encontrar um casamento maximal M de G em $\mathcal{O}(min(|V|, ||U|).|E|)$ utilizando o algoritmo de casamento para grafos bipartidos. As condições 2 e 3 do Teorema 1.4 podem ser checadas em tempo linear. Observe que, dado o grafo $G = \langle V, U, E \rangle$, tem-se que $|V| \leq n \leq m$ e $|E| \leq n.m \leq m^2$ e, portanto, pode-se determinar se existe θ tal que $t\theta =_{AC} s$ em tempo $\mathcal{O}(m^3)$.

Técnica para obter o grafo bipartido G do Teorema 1.4:

Para determinar o grafo $G = \langle V, U, E \rangle$ e determinar se existe uma substituição adequada escrevemos um algoritmo recursivo que primeiro tenta encontrar o conjunto de arestas em E atráves de chamadas de si mesmo em entradas t_i e s_j para cada i e j.

Seja $T(|t|, |s|)$ o tempo tomado por este algoritmo. Observe que a expressão:

$$\begin{aligned} T(|t|, |s|) &\leq \sum_{j=n+1}^{n+m} \sum_{i=1}^{n} T(|t_i|, |s_j|) + km^3 \text{ para algum } k \\ &\leq \sum_{j=n+1}^{n+m} (T(|t_1|, |s_j|) + \ldots + T(|t_n|, |s_j|)) + km^3 \\ &\leq (T(|t_1|, |s_{n+1}|) + \ldots + T(|t_n|, |s_{n+m}|)) + km^3 \end{aligned} \tag{1.4}$$

representa os testes de AC-casamento entre cada t_i e s_j, onde $1 \leq i \leq n$ e $1 \leq j \leq m$.

Este algoritmo irá terminar eventualmente uma vez que se tem que checar apenas as condições 2 e 3. Agora, pode-se mostrar por indução que $T(|t|, |s|) \leq k.|t|.|s|^3$, assumindo que $T(|t_i|, |s_j|) \leq k.|t_i|.|s_j|^3$ da seguinte forma:

$$\begin{aligned} \sum_{j=n+1}^{n+m} \sum_{i=1}^{n} T(|t_i|, |s_j|) + km^3 &\leq \left[\sum_{j=n+1}^{n+m} \sum_{i=1}^{n} k.|t_i|.|s_j|^3 \right] + km^3 \\ &\leq k. \left[\sum_{j=n+1}^{n+m} |s_j|^3 \right] . \left[\sum_{i=1}^{n} |t_i| \right] + km^3 \\ &\leq k. \left[\sum_{j=n+1}^{n+m} |s_j| \right]^3 . \left[\sum_{i=1}^{n} |t_i| \right] + km^3 \\ &\leq k. \left[\sum_{i=1}^{n} |t_i|.|s|^3 \right] + k.|s|^3 \\ &\leq k.|s|^3 \left(1 + \sum_{i=1}^{n} |t_i| \right) \\ &\leq k.|s|^3.|t| \end{aligned} \tag{1.5}$$

O caso em que o símbolo de função que encabeça t e s não é nem associativo e nem comutativo é trivial. □

1.6 PDI para Grupos Abelianos

Nesta seção comparam-se de dois trabalhos primordiais que propuseram métodos para o estudo da decidibilidade do *Problema da Dedução do Intruso* (PDI) levando em consideração a teoria de grupos Abelianos.

A relação de dedução mais conhecida neste contexto é conhecido como *modelo de Dolev-Yao*: o intruso pode formar pares e textos cifrados a partir de termos conhecidos, decompor pares, e decifrar termos cifrados quando ele conhece a chave de decriptação. Neste caso, assume-se *a criptografia perfeita*: o conjunto de mensagens é suposto ser uma álgebra livre, o que não é realista, uma vez que as primitivas criptográficas podem conter propriedades algébricas. Neste contexto, o seguinte problema de dedução é estudado:

Problema da dedução do intruso (PDI): Dado um conjunto finito de mensagens T e um segredo s, um intruso passivo pode deduzir s de T?($T \vdash^? s$)

A relação $T \vdash^? s$ é decidível em tempo polinomial para o intruso de Dolev-Yao. Este resultado é obtido pelo teorema de localidade de D.McAllester [33].

D. McAllester considera sistemas de dedução que são representados por conjuntos finitos de cláusulas de Horn e prova que existe um algoritmo de tempo polinomial para decidir a dedutibilidade de um termo s a partir de um conjunto finito de termos T se o sistema de dedução tem a chamada *propriedade de localidade*, que garante que qualquer prova pode ser transformada em uma prova onde todos os nós são subtermos sintáticos de T e s (a teoria do intruso $T \vdash s$ dado pelas regras da Tabela 1.1 é *local*).

(A) $\dfrac{u \in T}{T \vdash u}$	(E) $\dfrac{T \vdash u \quad T \vdash v}{T \vdash \{u\}_v}$	(D) $\dfrac{T \vdash \{u\}_v \quad T \vdash v}{T \vdash u}$
(P) $\dfrac{T \vdash u \quad T \vdash v}{T \vdash \langle u, v\rangle}$	(UL) $\dfrac{T \vdash \langle u, v\rangle}{T \vdash u}$	(UR) $\dfrac{T \vdash \langle u, v\rangle}{T \vdash v}$

Tabela 1.1: Capacidades do Intruso de Dolev-Yao

O intruso pode deduzir qualquer mensagem que fizer parte do seu conhecimento inicial (A); o intruso pode cifrar (respect. decifrar) mensagens utilizando chaves que podem ser deduzidas (E) (respect. (D)); o intruso pode criar pares de mensagens utilizando mensagens que puderam ser deduzidas anteriormente (P); o intruso pode separar pares de mensagens que ele deduziu anteriormente (UL ou UR).

No entanto, relaxando a hipótese da criptografia perfeita, busca-se obter resultados de decidibilidade da relação de dedução, levando em consideração a capacidade de raciocínico algébrico do intruso.

PDI módulo E : dado um conjunto finito de mensagens T e um segredo s, um intruso passivo pode deduzir s de T levando em consideração a teoria equacional E?

A seguir, o problema da dedução do intruso será estudado para a teoria equacional E de Grupos Abelianos, que é induzida pelos axiomas abaixo:

$(x \oplus y) \oplus z$	$=$	$x \oplus (y \oplus z)$	$i(0)$	$=$	0
$x \oplus y$	$=$	$y \oplus x$	$0 \oplus x$	$=$	x
$i(x \oplus y)$	$=$	$i(x) \oplus i(y)$	$x \oplus i(x)$	$=$	0
$i(i(x))$	$=$	x			

Tabela 1.2: E: Axiomas de Grupo Abelianos para o operador $\oplus$

Para ilustrar o uso de uma teoria equacional E no raciocínio dedutivo, adiciona-se às regras dedutivas de Dolev-Yao (Tabela 1.3) as seguintes regras relacionadas à teoria equacional:

$(\oplus)\ \dfrac{T \vdash u \quad T \vdash v}{T \vdash u \oplus v}$	(I) $\dfrac{T \vdash u}{T \vdash i(u)}$	$(\approx_E)\ \dfrac{T \vdash u \quad u \approx_E v}{T \vdash v}$

Tabela 1.3: Capacidades do intruso com teoria equacional

Considerando um operador associativo e comutativo $\oplus$ interpretado como um operador arbitrário de grupo Abeliano, e adotando como teoria equacional $\approx_E$ a relação de congruência gerada pelas identidades na Tabela 1.3, as regras adicionais da Tabela 2.2 significam: o intruso pode introduzir a função $\oplus$, aplicando em duas mensagens previamente deduzidas (Regra $(\oplus)$); o intruso pode introduzir a função i, aplicando em uma mensagem previamente deduzida (Regra (I)); o intruso pode raciocinar algébricamente utilizando a teoria equacional imersa no protocolo (Regra $(\approx_E)$). A propriedade de localidade de D. McAllester implica, de acordo com H. Comon-Lundh e V. Shamatikov, em [19], que $T \vdash^? s$ está em NP, como será mostrado na Subseção 1.6.1. Em um trabalho posterior, P.Lafourcade, D. Lugiez e R. Treinen, em [30], afirmam que seguindo suas técnicas, o PDI é decidível em tempo polinomial, o que não é o caso, como será mostrado na Subseção 1.6.2

1.6.1 Abordagem via provas normais

H.Comon-Lundh e V.Shmatikov, em [19] propuseram um método para mostrar que, se $T \vdash s$, então existe uma prova na qual apenas subtermos de $T \cup \{s\}$ aparecem. Em outras palavras, o trabalho consiste em mostrar que o sistema de regras de inferência de Dolev-Yao, estendido com a teoria de Grupos Abelianos tem a propriedade de localidade.

Para isto, considera-se o sistema de reescrita de termos $\mathcal{R}_E$ associado à teoria equacional de grupos Abelianos:

$i(x \oplus y)$	$\rightarrow$	$i(x) \oplus i(y)$	$0 \oplus x$	$\rightarrow$	x
$i(i(x))$	$\rightarrow$	x	$x \oplus i(x)$	$\rightarrow$	0
$i(0)$	$\rightarrow$	0			

Tabela 1.4: $\mathcal{R}_E$: sistema de regras de reescrita para Grupo Abelianos

Este sistema de reescrita é convergente módulo associatividade e comutatividade do operador binário $\oplus$, este fato pode ser verificado utilizando a ferramenta CiME2 [20]. Pode-se, então, considerar as formas normais de um termo de $T(\Sigma, X)$ construído a partir da assinatura $\Sigma = \{\oplus, i, 0\}$ de grupos Abelianos. O objetivo é mostrar que o sistema de regras de inferência de Dolev-Yao estendido com a teoria de grupos Abelianos tem a propriedade de localidade, para isto, considere a seguinte noção de subtermos:

Definição 1.38 ($St(T)$)**.** *Seja T um conjunto de termos, seja $St(T)$ o menor conjunto tal que :*

- *se $t \in T$ então $t \in St(T)$;*
- *se $t \in T$ então $i(t) \downarrow \in St(T)$;*
- *se $\langle u, v\rangle \in St(T)$ então $u, v \in St(T)$;*
- *se $\{u\}_k \in St(T)$ então $u, k \in St(T)$;*
- *se $u \in St(T)$ então $atomos(u) \in St(T)$;*

Observe que número de elementos em $St(T)$ é linear no tamanho de T (o *tamanho* de um conjunto de termos é definido como a soma do número de nós em cada membro de T).

A seguir, aplicações repetidas da regra $(\oplus)$ serão combinadas para evitar o número exponencial de combinações de provas possíveis que podem ser feitas módulo associatividade e comutatividade. Dessa forma, a regra $(\oplus)$ será substituída pela seguinte regra mais geral, cujo número de premissas é arbitrário:

$$\frac{T \vdash u_1 \qquad \ldots \qquad T \vdash u_n}{T \vdash u_1 \oplus \ldots \oplus u_n}\,(GX)$$

Observação 1.4. *Assumindo que T e s estão na forma normal, se existir uma prova de $T \vdash s$, obtém-se outra prova pela normalização (via reescrita) dos termos em cada passo de inferência: normalizar não impede a aplicação de $(A), (UL), (UR)$ ou (D) e para as outras regras, passos de igualdade módulo E podem ser adiados para depois de sua aplicação. Na sequência, a menos que seja afirmado o contrário, assume-se que todos os termos são mantidos na forma normal e as aplicações da regra ($\approx_E$) estão implícitas.*

A seguir todos os resultados são com base no sistema de regras de inferência $\mathcal{S}$:

O tamanho de uma prova é dada pelo seu número de nós. Uma prova é *simples* se todo nó $T \vdash v$ ocorrer no máximo uma vez em cada ramo.

Lema 1.3 ([19])**.** *Se existir uma prova simples e minimal $\mathcal{P}$ de uma das seguintes formas:*

$$\frac{\dfrac{\vdots}{T \vdash \langle u, v\rangle}}{T \vdash u} \qquad \frac{\dfrac{\vdots}{T \vdash \langle v, u\rangle}}{T \vdash u} \qquad \frac{\dfrac{\vdots}{T \vdash \{u\}_v} \quad \dfrac{\vdots}{T \vdash v}}{T \vdash u}$$

(A) $\dfrac{u \in T}{T \vdash u}$	(E) $\dfrac{T \vdash u \qquad T \vdash v}{T \vdash \{u\}_v}$	(D) $\dfrac{T \vdash \{u\}_v \qquad T \vdash v}{T \vdash u}$
(P) $\dfrac{T \vdash u \qquad T \vdash v}{T \vdash \langle u, v\rangle}$	(UL) $\dfrac{T \vdash \langle u, v\rangle}{T \vdash u}$	(UR) $\dfrac{T \vdash \langle u, v\rangle}{T \vdash v}$
(GX) $\dfrac{T \vdash u_1 \qquad \ldots \qquad T \vdash u_n}{T \vdash u_1 \oplus \ldots \oplus u_n}$	(I) $\dfrac{T \vdash u}{T \vdash i(u)}$	$(\approx_E)$ $\dfrac{T \vdash u \qquad u \approx_E v}{T \vdash v}$

Tabela 1.5: Sistema $\mathcal{S}$: sistema de regras de Dolev-Yao estendido com grupos Abelianos

Então $\langle u, v\rangle \in St(T)$ *(respectivamente,* $\langle v, u\rangle \in St(T)$ *e* $\{u\}_v \in St(T)$ *).*

Demonstração. Suponha que exista uma prova minimal e simples $\mathcal{P}$ de $T \vdash u$ utilizando as regras de $\mathcal{S}$. A demonstração é por indução no tamanho da prova $|\mathcal{P}|$ e a análise é feita com base na última regra aplicada em $\mathcal{P}$.

1. A última regra é (UL).

   Então $\mathcal{P}$ tem a forma

   $$(UL)\ \dfrac{\dfrac{\mathcal{P}'}{T \vdash \langle u, v\rangle}}{T \vdash u}$$

   Observe que $T \vdash \langle u, v\rangle$ pode ser obtido de uma das seguintes formas:

   - ou $T \vdash \langle u, v\rangle$ foi obtido via uma aplicação de (P);
     Neste caso $\mathcal{P}'$ pode ser representado da seguinte forma:

     $$(P)\ \dfrac{\dfrac{\mathcal{P}'_1}{T \vdash u} \qquad \dfrac{\mathcal{P}'_2}{T \vdash v}}{(UL)\ \dfrac{T \vdash \langle u, v\rangle}{T \vdash u}}$$

     E isto contradiz a hipótese de que $\mathcal{P}$ é uma prova minimal.
   - ou $T \vdash \langle u, v\rangle$ foi obtido via uma aplicação de (A);
     Neste caso, $\langle u, v\rangle \in T \subseteq St(T)$, e o resultado segue.
   - ou $T \vdash \langle u, v\rangle$ foi obtido via uma aplicação de (UL), (UR) ou (D);
     Neste caso, tem-se que $\mathcal{P}'$ é uma prova de $T \vdash \langle u, v\rangle$ obtida via uma aplicação de (UL), (UR) ou (D) tal que $|\mathcal{P}'| \leq |\mathcal{P}|$. Aplicando a hipótese de indução segue o resultado.

- ou $T \vdash \langle u, v\rangle$ foi obtido via uma aplicação de (GX), (I) ou $(\approx_E)$.

  Observe que as regras (GX) e (I) não podem ter sido aplicadas para obter $T \vdash \langle u, v\rangle$, uma vez que o símbolo cabeça é $\langle \_, \_\rangle$ e não, $\oplus$ ou i. Uma possibilidade seria aplicar a regra $(\approx_E)$, mas as identidades presentes na teoria equacional gerada por E não contém $\langle \_, \_\rangle$, portanto, existem algumas seguintes possibilidades de prova $\mathcal{P}'$:

$$(\approx_E)\ \frac{\dfrac{\mathcal{P}''}{T \vdash \langle u, v\rangle \oplus 0}}{T \vdash \langle u, v\rangle} \qquad (\approx_E)\ \frac{\dfrac{\mathcal{P}''}{T \vdash \langle u, v\rangle \oplus i(w) \oplus w}}{T \vdash \langle u, v\rangle}$$

$$(\approx_E)\ \frac{\dfrac{\mathcal{P}''}{T \vdash i(i(\langle u, v\rangle))}}{T \vdash \langle u, v\rangle}$$

  E outras possibilidades que são similares. Em todo caso, tem-se que $\langle u, v\rangle$ é subtermo das premissas. Procedendo recursivamente, de baixo para cima, tem-se que ou a regra (A), (UL), (UR) ou (D) foi aplicada e o resultado segue.

□

A seguir, a definição formal de provas normais, definida por H. Comon-Lundh e V. Shmatikov em [19]:

Definição 1.39 (Provas Normais)**.** *Uma prova simples $\mathcal{P}$ de $T \vdash u$ é* normal *se*

- *$u \in St(T)$ e todo nó que não é uma folha de $\mathcal{P}$ está rotulado com $T \vdash v$ com $v \in St(T)$;*
- *ou $\mathcal{P} = C[\mathcal{P}_1, \ldots, \mathcal{P}_n]$ e toda prova $\mathcal{P}_i$ é uma prova normal de algum $T \vdash v_i$, com $v_i \in St(T)$ e C é construído utilizando apenas as regras P, E, GX e I.*

O seguinte lema garante a existência de provas normais para um sistema de regras de inferência enriquecido com a teoria de Grupos Abelianos. Este lema foi proposto em [19], porém a demonstração deste resultado apresentava algumas imprecisões. Principalmente, para a parte da prova relacionada à aplicação da regra (GX). No trabalho, os autores afirmam que sempre que $T \vdash u = (u_1 \oplus \ldots \oplus u_n)\downarrow$ é obtido via uma aplicação da regra (GX) em subprovas $\mathcal{P}_i$ de $T \vdash u_i \oplus v_i$, para u_i e v_i possivelmente vazios $(1 \leq i \leq n)$, se $u_i \oplus v_i$ for enquadrado no tipo c) (ver a prova do Lema 1.4), então este termo pode ser eliminado da prova de $T \vdash u$. Este fato não é verdade, como pode ser visto na demonstração abaixo.

Lema 1.4. *Se existir uma prova de $T \vdash u$ então existe uma prova normal de $T \vdash u$.*

Demonstração. Seja $\mathcal{P}$ uma prova de $T \vdash u$. A prova será dividida em dois casos segundo a Definição 1.39 de provas normais.

1. Suponha que $u \in St(T)$.

   Prova-se por indução no tamanho da prova de $T \vdash u$.

   Base da Indução. A prova consiste de uma aplicação da regra (A). Isto é,

$$\frac{u \in T}{T \vdash u}\,(A)$$

   O resultado segue por vacuidade, uma vez que não existem outros nós em $\mathcal{P}$.

   Hipótese de Indução. Para toda prova $\mathcal{P}'$ de $T \vdash v$, com $v \in St(T)$ e tal que $|\mathcal{P}'| \leq |\mathcal{P}|$ existe uma prova normal $\mathcal{P}''$ de $T \vdash v$.

   Pode-se assumir, sem perda de generalidade, que a prova é *simples*. Se este não for o caso, simplifique a prova e aplique a hipótese de indução.

   Passo indutivo. Serão analisados todos os casos possíveis para última inferência:

   - Se a última regra é (P) (ou E, que é tratado de maneira similar).
     Isto é, $u = \langle u_1, u_2 \rangle$ e é obtido da seguinte forma:

$$\frac{\dfrac{\mathcal{P}_1}{T \vdash u_1} \quad \dfrac{\mathcal{P}_2}{T \vdash u_2}}{T \vdash u = \langle u_1, u_2 \rangle}\,(P)$$

     Observe que $u_1, u_2 \in St(u) \subseteq St(T)$ e $|\mathcal{P}_i| \leq |\mathcal{P}|$, para $i = 1, 2$. Por hipótese de indução, existe uma prova normal $\mathcal{P}_i'$ de $T \vdash u_i$ $(i = 1, 2)$. E então, existe uma prova normal $\mathcal{P}'$ de $T \vdash u$ dada por:

$$\frac{\dfrac{\mathcal{P}_1'}{T \vdash u_1} \quad \dfrac{\mathcal{P}_2'}{T \vdash u_2}}{T \vdash u = \langle u_1, u_2 \rangle}\,(P)$$

   - Se a última regra é (I).
     Então $u = i(v)\downarrow$ e $\mathcal{P}$ é obtida da seguinte maneira:

$$\frac{\dfrac{\mathcal{P}_1}{T \vdash v}}{T \vdash u = i(v)\downarrow}\,(I)$$

     Isto é, existe uma prova de $\mathcal{P}_1$ de $T \vdash v$ que é menor que $\mathcal{P}$. Como, por definição, $St(T)$ é fechado para aplicação de inversos, segue que $v \in St(T)$. Por hipótese de indução, existe uma prova normal $\mathcal{P}_1'$ de $T \vdash v$. Aplicando-se a regra (I), obtem-se uma prova normal $\mathcal{P}'$ de $T \vdash u$.

   - Se a última regra é (UL) (a prova é similar para (UR) ou (D)).
     Suponha que $\mathcal{P}$ é minimal (caso contrário, a hipótese de indução pode ser aplicada em uma prova menor de $T \vdash u$). $\mathcal{P}$ é da seguinte forma:

$$\frac{\dfrac{\mathcal{P}_1}{T \vdash \langle u, v \rangle}}{T \vdash u}$$

Pelo Lema 1.3, $\langle u, v\rangle \in St(T)$ (respectivamente, $\langle v, u\rangle, \{u\}_v \in St(T)$). Aplicando a hipótese de indução, obtém-se uma prova normal $\mathcal{P}'_1$ de $T \vdash \langle u, v\rangle$ (respectivamente, de $T \vdash \langle v, u\rangle$ e $T \vdash \{u\}_v$). Segue, então, uma prova normal $\mathcal{P}'$ de $T \vdash u$:

$$\dfrac{\dfrac{\mathcal{P}'_1}{T \vdash \langle u, v\rangle}}{T \vdash u}$$

- Se a última regra é (GX).

  Suponha que u está na forma normal e considere o contexto maximal C tal que $C[\mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_n] = \mathcal{P}$ e todo nó de C é obtido por uma regra (GX) ou por uma regra (I) (tal contexto existe, pelo menos o nó na posição raiz é obtido desta forma). Transforme a prova, juntando todas as aplicações de (GX) em uma só e comutando (GX) e (I) de forma que todas as aplições de (I) ocorram antes das aplicações de (GX).

  Considere o caso em que as raízes de $\mathcal{P}'_1, \ldots, \mathcal{P}'_n$ são rotuladas respectivamente com $T \vdash u_1 \oplus v_1, \ldots, T \vdash u_n \oplus v_n$, onde os $u'_j s$ e os $v'_j s$ $(1 \leq j \leq n)$ são eventualmente nulos, e tais que $u = (u_1 \oplus \ldots \oplus u_n)\downarrow$ e $(v_1 \oplus \ldots \oplus v_n)\downarrow = 0$. Observe que considerar as premissas de $T \vdash u$ dessa forma trata, de uma forma geral, o caso em que u vem sido construído ao decorrer da prova, com alguns subtermos sendo eliminados e outros subtermos sendo "juntados".

  Considere a seguinte prova $\mathcal{P}'$ de $T \vdash u$:

$$\dfrac{\dfrac{\mathcal{P}'_1}{T \vdash u_1 \oplus v_1} \quad \ldots \quad \dfrac{\mathcal{P}'_n}{T \vdash u_n \oplus v_n}}{T \vdash u = (u_1 \oplus \ldots \oplus u_n)\downarrow}\,(GX)$$

  Suponha que cada $u_j \oplus v_j$ está na forma normal $(1 \leq j \leq n)$, observando que alguns dos $u'_j s$ e $v'_j s$ podem ser nulos. A seguir vamos considerar todos os casos possíveis para cada $u_j \oplus v_j$:

  a) $u_j \neq 0$ e $v_j \neq 0$.
  Como, por hipótese, $u_j \oplus v_j$ já está na forma normal, tem-se que $(u_j \oplus v_j)\downarrow$ é encabeçado com $\oplus$. Pela maximalidade de C a última regra aplicada em $\mathcal{P}'_j$ para obter $u_j \oplus v_j$ não pode ser (GX). Nos casos em que $u_j \oplus v_j$ é obtido por uma aplicação de (D), (UL) ou (UR), segue pelo Lema 1.3 que $u_j \oplus v_j \in St(T)$. Como $St(T)$ é fechado para aplicação de inversos, segue que, se a última regra aplicada em $\mathcal{P}'_j$ é (I), e então $u_j \oplus v_j \in St(T)$.

  b) $v_j = 0$ e $u_j \neq 0$
  Este caso se divide em dois subcasos:

  b.1) u_j é encabeçado com $\oplus$.
  Neste caso, $\mathcal{P}'_j$ é uma prova simples de $T \vdash u_j$. Como, por hipótese, u_j é encabeçado por $\oplus$, e pela maximalidade de C, u_j não pode ser obtido por (GX), segue que u_j foi obtido via aplicação de (UL), (UR), (D)

ou (I). Para os três primeiros casos, aplica-se o Lema 1.3, obtendo-se $u_j \in St(T)$. Para o caso em que u_j é obtido via aplicação da regra (I), tem-se que $u_j = u'_j \oplus v'_j$ e daí, a seguinte derivação:

$$\dfrac{\dfrac{\mathcal{P}''_j}{T \vdash i(u'_j) \oplus i(v'_j)}}{T \vdash u'_j \oplus v'_j}\,(\mathrm{I})$$

Observe que $i(u'_j) \oplus i(v'_j)$ é encabeçado por $\oplus$. Como a prova é minimal, não pode ter sido obtido por uma aplicação de (I), como C é maximal, também não pode ter sido obtido por (GX). Dessa forma, $i(u'_j) \oplus i(v'_j)$ foi obtido por (A), (UL), (UR) ou (D). Em todos os casos, segue que $i(u'_j) \oplus i(v'_j) \in St(T)$. Como $St(T)$ é fechado para aplicação de inversos, segue que $u'_j \oplus v'_j = u_j \in St(T)$.

b.2) u_j não é encabeçado com $\oplus$.
Neste caso $\mathcal{P}'_j$ é uma prova simples de u_j. Observe que, se u_j foi obtido por (A), (E) ou (P), então $u_j \in St(u) \subseteq St(T)$. Se u_j foi obtido por (UL), (UR) ou (D), então, pelo Lema 1.3 $u_j \in St(T)$.

c) $u_j = 0$ e $v_j \neq 0$.
Este caso representa a situação em que existe uma prova $\mathcal{P}'_j$ de $T \vdash v_j$ é uma prova $\mathcal{P}''_t$ de $T \vdash u_t \oplus i(v_j)$, para algum índice $t \in \{1, \ldots, n\}$. Neste caso, $\mathcal{P}'_j$ não é uma prova de um subtermo de u, porém é uma prova necessária para eliminar o subtermo $v_t = i(v_j)$ e isolar o subtermo u_t que permanecerá na estrutura de u ao final da prova $\mathcal{P}$.

Suponha que existam m termos $u_j \oplus v_j$ que se enquadram nos casos $a)$, $b.1)$ ou $b.2)$. Reorganize as provas de tal forma que $u_1 \oplus v_1, \ldots, u_k \oplus v_k$ estejam no caso $a)$, $u_{k+1} \oplus v_{k+1}, \ldots, u_m \oplus v_m$ estejam nos casos $b.1)$ ou $b.2)$ e $u_{m+1} \oplus v_{m+1}, \ldots, u_n \oplus v_n$ estejam no caso $c)$.

$$\underbrace{u_1 \oplus v_1 \ldots u_k \oplus v_k}_{\text{Caso a)}}\ \underbrace{u_{k+1} \oplus v_{k+1} \ldots u_m \oplus v_m}_{\text{Caso b.1) ou b.2)}}\underbrace{u_{m+1} \oplus v_{m+1} \ldots u_n \oplus v_n}_{\text{Caso c)}}$$

Considere um índice $p > m$. Como $(v_1 \oplus \ldots \oplus v_n) \downarrow = 0$, segue que existe um índice j tal que $i(v_p) \in atomos(u_j \oplus v_j)$.

i) Se $u_j \oplus v_j$ pertence ao caso $a), b)$ ou $c)$ então, segue do raciocínio acima que, $u_j \oplus v_j \in St(T)$. Como $atomos(u_j \oplus v_j) \in St(T)$ segue que $i(v_p) \in St(T)$ e, consequentemente, $v_p \in St(T)$. Observe que a prova $\mathcal{P}'_p$ de $T \vdash v_p$ é tal que $|\mathcal{P}'_p| \leq |\mathcal{P}|$. Por hipótese de indução, segue que existe uma prova normal de $T \vdash v_p$.

ii) Se $u_j \oplus v_j$ pertence ao caso $d)$, então $u_j = 0$ e $v_j \neq 0$. Além disso, $i(v_p) \in atomos(v_j)$.

- Suponha que v_j não é encabeçado por $\oplus$:
  Então $i(v_p) = v_j$ e tanto v_p quando v_j são desnecessários na prova de $T \vdash u$, o que contradiz o fato de $\mathcal{P}$ ser uma prova minimal.
- Suponha que v_j é encabeçado por $\oplus$:
  Suponha que $v_j = v_{j1} \oplus v_{j2}$. Observe que $T \vdash v_j$ não pode ser obtido por uma aplicação de (GX) então, pelo raciocínio acima, $v_j \in St(T)$. Por hipótese, $i(v_p) \in atomos(v_j) \subseteq St(T)$ e, consequentemente, $v_p \in St(T)$. Por hipótese de indução, existe uma prova normal de $T \vdash v_p$.

Logo, para todo i, $1 \leq i \leq n$, existe uma prova normal $\mathcal{P}_i''$ de $T \vdash u_i \oplus v_i$, e portanto, com uma aplicação de (GX), segue uma prova normal $\mathcal{P}'$ de $T \vdash u$.

2. Suponha que $\mathcal{P} = C[\mathcal{P}_1, \ldots, \mathcal{P}_n]$.

   Considere uma prova minimal $\mathcal{P}$ de $T \vdash u$.

   O objetivo é provar que $\mathcal{P}$ pode ser escrita como $\mathcal{P} = C[\mathcal{P}_1, \ldots, \mathcal{P}_n]$ onde $\mathcal{P}_1, \ldots, \mathcal{P}_n$ são subárvores maximais e normais de $\mathcal{P}$ cujas raízes são rotuladas com $T \vdash v_i$ respectivamente e $v_i \in St(T)$ para todo i. Além disso, C é construído utilizando apenas as regras (P), (E), (GX) e (I).

   A prova segue por indução no tamanho de C:

   - Se $|C| = 0$ (isto é, C é vazio) então $u \in St(T)$.
   - A última regra é (UL) (respectivamente, (UR) ou (D)).
     Neste caso,

     $$(UL)\ \dfrac{\dfrac{\mathcal{P}'}{T \vdash \langle u, v\rangle}}{T \vdash u}$$

     Então, pelo Lema 1.3, $\langle u, u\rangle \in St(T)$ (respectivamente, $\langle v, u\rangle$ e $\{u\}_v$). Observe que, como $\langle u, v\rangle \in St(T)$, segue pela definição de subtermos (Definição 1.38), tem-se que $u \in St(T)$. Este caso foi estudado no primeiro item da demonstração deste lema e agora, o objetivo é provar o segundo caso de provas normais de $T \vdash u$, isto é, o caso em que $u \notin St(T)$.
   - Se a última regra é (P).

     $$\dfrac{\dfrac{\mathcal{P}_1'}{T \vdash v} \quad \dfrac{\mathcal{P}_2'}{T \vdash w}}{T \vdash u = \langle v, w\rangle}\,(P)$$

     Aplicando-se a hipótese de indução em $\mathcal{P}_1'$ e $\mathcal{P}_2'$, segue o resultado.
   - Se a última regra é (E).

     $$\dfrac{\dfrac{\mathcal{P}_1'}{T \vdash v} \quad \dfrac{\mathcal{P}_2'}{T \vdash k}}{T \vdash u = \{v\}_k}\,(E)$$

Aplicando-se a hipótese de indução em $\mathcal{P}'_1$ e $\mathcal{P}'_2$, segue o resultado.

- Se a última regra é (GX).

  Suponha que $\mathcal{P}$ tenha a seguinte forma, onde ocorrências sucessivas de aplicações da regra (GX) foram combinadas na única aplicação abaixo. Isto é, cada $T \vdash u_i$ não foi obtido via uma aplicação de (GX), $1 \leq i \leq n$.

$$(GX)\ \frac{\dfrac{\mathcal{P}'_1}{T \vdash u_1} \quad \ldots \quad \dfrac{\mathcal{P}'_n}{T \vdash u_n}}{T \vdash u = u_1 \oplus \ldots \oplus u_n}$$

  O resultado segue pela aplicação da hipótese de indução nas provas $\mathcal{P}'_1, \ldots, \mathcal{P}'_n$.

- Se a última regra é (I).

$$(I)\ \frac{\dfrac{\mathcal{P}'_1}{T \vdash v}}{T \vdash u = i(v)}$$

  Aplicando-se a hipótese de indução em $\mathcal{P}'_1$ segue o resultado.

□

Definição 1.40 (Derivabilidade Imediata)**.** *$T \vdash u$ é* imediatamente derivável *se existirem termos $u_1, \ldots, u_n \in T$ tais que $T \vdash u$ é obtido de $T \vdash u_1, \ldots, T \vdash u_n$ por uma única aplicação de uma regra de inferência de (E, P, GX, I).*

Teorema 1.6 ([19])**.** *Dado um conjunto finito de termos básicos T, e um termo básico u, a derivabilidade de $T \vdash u$ está em NP no caso de Grupos Abelianos.*

Demonstração. Para provar a pertinência na classe NP, considere o seguinte procedimento:

1. Escolha um subconjunto S de $St(T \cup \{u\})$ que contenha u (Existem $2^{|St(T \cup \{u\})|}$ possíveis conjuntos).

2. Escolha uma ordem $s_1 > s_2 > \ldots > s_n$ nos termos de $S \cap St(T)$ (existem $n!$ possíveis ordens).

3. Para cada $i = 1, \ldots, n$, verifique que $T \cup \{s_1, \ldots, s_{i-1}\} \vdash s_i$ é imediatamente derivável.

Este algoritmo está em NP pois existem no máximo $\mathcal{O}(|St(T \cup \{u\})|)$ passos (isto é, um número polinomial) e cada passo pode ser completado em tempo não determinístico polinomial.

Se o algoritmo tiver sucesso então $T \vdash u$ é derivável. Caso contrário, o resultado baseia-se no Lema 1.4: se $T \vdash u$ é derivável, então existe uma prova normal de $T \vdash u$, da qual pode-se derivar uma ordem em $St(T \cup \{u\})$. □

1.6.2 Abordagem via generalização da localidade de McAllester

P. Lafourcade, D. Lugiez e R. Treinen, em [30], baseados na técnica de localidade proposta por David McAllester [33], propõem uma generalização da localidade de D. McAllester, que será utilizada para o estudo do problema da deducão do intruso para teorias equacionais associativas e comutativas com homomorfismo. Neste trabalho os autores afirmam que seguindo as técnicas propostas é possível provar que o PDI para Grupos Abelianos é decidível em tempo polinomial, "melhorando" o trabalho proposto por H.Comon-Lund e V. Shmatikov em [19] e discutido na Subseção 1.6.1.

Os autores observam que a existência de uma prova *local* pode ser verificada em tempo polinomial uma vez que existe apenas um número polinomial de instâncias relevantes das regras de dedução (As instâncias relevantes são instâncias por subtermos de um problema dado). Verificar a existência de uma prova local recai em calcular a interseção de um fecho de dedução do conhecimento inicial com o conjunto de termos relevantes. O Algoritmo 1 calcula a restrição do fecho de dedução de T_0 para o conjunto de termos relevantes.

Diz-se w é *dedutível em um passo* de T, se w puder ser obtido de T com apenas uma aplicação de uma regra do sistema de prova. Denota-se no algoritmo abaixo a relação de dedução em um passo por $\vdash^{\leq 1}$. No algoritmo 1, $S_{sin}(T_0, w)$ denota o conjunto dos

Algoritmo 1 Algoritmo de McAllester para verificar a existência de uma prova local

1: **Input:** T_0, w
2: $T \leftarrow T_0$
3: **while** $\exists s \in S_{sin}(T_0, w)$ such that ($T \vdash^{\leq 1} s$ and $s \notin T$) **do**
4: $\quad T \leftarrow T \cup \{s\}$
5: **end while**
6: **return** $w \in T$

subtermos sintáticos de $T_0 \cup \{w\}$ (Definição 1.4).

Existem duas restrições para esta abordagem:

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

Porém estas restrições dão origem a certos problemas quando se opera módulo associatividade e comutatividade, uma vez que o conjunto de subtermos é dinâmico e não estático, isto é, pode variar, já que a estrutura do termo varia módulo associatividade e comutatividade.

Exemplo 1.2. *Considere o termo $t = (f(a+b)+c)+d$, onde $+$ é um símbolo de função AC, f é um símbolo de função que não é associativo e nem comutativo, e os termos a, b, c, d são constantes. O conjunto dos* subtermos sintáticos *$st(t)$ de t, é dado por:*

$$st(t) = \{t, f(a+b)+c, f(a+b), a+b, a, b, c, d\}.$$

Porém, $t =_{AC} t' = f(a+b)+(c+d)$ *e neste caso, o conjunto dos subtermos sintáticos é*

$$st(t') = \{t', f(a+b), c+d, a+b, a, b, c, d\}.$$

O mesmo pode ser feito para cada possível combinação dos subtermos de t *módulo associatividade e comutatividade de* $+$*. Isto é, para cada termo da classe de congruência módulo* AC *de* t*, existe um conjunto de subtermos sintáticos diferente.*

Seja $\oplus$ um símbolo de função binário que é associativo e comutativo. Considere a seguinte regra de dedução para introdução de $\oplus$:

$$(\oplus)\ \frac{T \vdash u \qquad T \vdash v}{T \vdash u \oplus v}$$

Para utilizar esta regra seria necessário considerar todos os possíveis subtermos módulo AC. Existe, em geral, um número exponencial de subtermos módulo AC de um dado termo (Exemplo 1.2). Para evitar a necessidade de computar todas as possíveis combinações, a regra $(\oplus)$ será utilizada com um número arbitrário de hipóteses, seguindo a ideia proposta por [19], via regra (GX):

$$(GX)\ \frac{T \vdash u_1 \qquad \ldots \qquad T \vdash u_n}{T \vdash u \oplus \ldots \oplus u_n}$$

Observe que utilizando a regra, pode-se evitar um número exponencial de subtermos módulo AC. No entanto, ainda é necessário lidar com um número infinito de regras, uma vez que n é arbitrário. Para sobrepor este problema, será definido, para cada teoria equacional, um conjunto de subtermos adequado, que limita o número de execuções do laço **while** no Algoritmo 1.

Na definições abaixo uma função S que mapeia um conjunto de subtermos em um conjunto de subtermos é utilizada. Essa função corresponde a uma noção de subtermos, que pode variar de acordo com a teoria equacional considerada.

Definição 1.41 (Prova S-local)**.** *Seja* S *uma função que mapeia um conjunto de termos em um conjunto de termos. Uma prova* P *de* $T \vdash w$ *é* S-local *se todos os nós são rotulados por algum* $T \vdash v$*, com* $v \in S(T \cup \{w\})$*.*

Definição 1.42 (S-localidade)**.** *Um sistema de prova é* S-local *se sempre que existir uma prova de* $T \vdash w$ *então também existe uma prova* S*-local de* $T \vdash w$*.*

Na sequência, o seguinte modelo de dedução de Dolev-Yao é estendido com uma teoria equacional E que pode ser representada por um sistema de reescrita de termos convergente módulo AC. Neste caso, consideram-se termos na forma normal módulo AC, ao invés de permitir raciocínio equacional ilimitado módulo a teoria equacional.

Seja Σ uma assinatura que pode ser particionada da seguinte forma

$$\Sigma = \{\langle \_, \_ \rangle, \{\_\}\_, \oplus\} \uplus \Sigma^{-}$$

onde $\oplus$ é um operador binário AC, Σ^{-} é composto de símbolos de função e $\uplus$ denota união disjunta.

$$\text{(A)}\ \frac{u \in T}{T \vdash u\downarrow} \qquad \text{(P)}\ \frac{T \vdash u \quad T \vdash v}{T \vdash \langle u, v\rangle\downarrow}$$

$$\text{(UL)}\ \frac{T \vdash r}{T \vdash u\downarrow}\ \text{se}\ \langle u, v\rangle = r\downarrow \qquad \text{(UR)}\ \frac{T \vdash r}{T \vdash v\downarrow}\ \text{se}\ \langle u, v\rangle = r\downarrow$$

$$\text{(E)}\ \frac{T \vdash u \quad T \vdash v}{T \vdash \{u\}_v\downarrow} \qquad \text{(D)}\ \frac{T \vdash r \quad T \vdash v}{T \vdash u\downarrow}\ \text{se}\ \{u\}_v = r\downarrow$$

$$\text{(F)}\ \frac{T \vdash u_1 \quad \ldots \quad T \vdash u_n}{T \vdash f(u_1, \ldots, u_n)\downarrow}\ f \in \Sigma^- \qquad \text{(GX)}\ \frac{T \vdash u_1 \quad \ldots \quad T \vdash u_n}{T \vdash (u_1 \oplus \ldots \oplus u_n)\downarrow}$$

Tabela 1.6: Sistema $\mathcal{D}$: Sistema de prova de Dolev-Yao operando em formas normais módulo teoria equacional E

A regra (GX) permite que o intruso construa um novo termo a partir de um número arbitrário de termos já conhecidos, utilizando o operador AC $\oplus$. Observe que, as regras da Tabela 1.6 representam um enfraquecimento da *hipótese da criptografia perfeita*, dando ao intruso o poder de utilizar raciocínio equacional módulo um conjunto dado E de axiomas equacionais.

Teorema 1 em [30] *Seja S uma função que mapeia um conjunto de termos em um conjunto de termos, e P um sistema de prova. Se:*

- *o conjunto $S(T)$ pode ser construído em tempo $\mathcal{K}_1$,*
- *P é S-local,*
- *dedutibilidade em um passo em P é decidível em tempo $\mathcal{K}_2$.*

então a demonstrabilidade no sistema de prova P é decidível em tempo $\mathcal{K}_1 \times \mathcal{K}_2$.

Demonstração. Para a prova deste teorema, considera-se o Algoritmo 1 descrito no início desta subseção, com a diferença que no laço **while** a noção de subtermos S é utilizada ao invés do conjunto dos *subtermos sintáticos de* $T_0 \cup \{w\}$.

Seja $n = |T_0| + |w|$, onde T_0 é o conhecimento inicial do intruso e w é o termo para o qual se quer verificar se $T \vdash w$ acontece (no primeiro passo do Algoritmo 1 $T \leftarrow T_0$). O número de iterações do laço é limitado pelo número de instâncias das conclusões das regras do sistema de prova por termos em $S(T_0 \cup \{w\})$. Logo, por hipótese, o número de iterações do laço **while** é limitado por $\mathcal{K}_1(n)$. Como uma consequência, a execução do algoritmo toma, no máximo, tempo $\mathcal{K}_1(n) \times \mathcal{K}_2(n)$. Pela S-localidade do sistema de prova, a existência de uma prova é equivalente à existência de uma prova local. □

Este teorema generaliza o resultado de McAllester porque:

- O tamanho do conjunto dos *subtermos sintáticos* do conjunto T é polinomial no tamanho de T, e este fato pode não ser verdade para uma noção de subtermos S definida para uma teoria equacional.

- dedutibilidade em um-passo é decidível em tempo polinomial para um sistema de prova finito. É necessário um algoritmo para testar decidibilidade em um passo para cada nova teoria equacional considerada.

Na seguinte subseção um procedimento para decidir a dedutibilidade em um passo para teorias equacionais que contenham símbolo de função $\oplus$ que é associativo e comutativo será proposto.

dedutibilidade em um passo para teorias AC

A seguir, um algoritmo que mostra como decidir a dedutibilidade em um passo para a regra (GX) será proposto. Note que decidir a dedutibilidade em um passo para as outras regras da Tabela 2.6 (que envolvem símbolos de função que não são associativos e nem comutativos) é direto, uma vez que não é necessário verificar combinações.

O Algoritmo 2 abaixo foi proposto em [31] que é a versão estendida do trabalho [30]. Este algoritmo transforma o problema de testar a dedutibilidade em um passo na solubilidade de um sistema de equações Diofantinas lineares. O domínio sobre o qual o sistema é solucionado depende da teoria equacional considerada.

Para o Algoritmo 2 a seguir, considere um conjunto finito de termos $T = \{t_0, \ldots, t_n\}$ e um termo s para o qual se quer testar se $T \vdash s$. Seja $A = \{a_1, \ldots, a_m\}$ o conjunto dos átomos de $T \cup \{s\}$ (ver Definição 1.28). Seja t um termo e u um átomo de t. Denota-se por $\gamma(u, t)$ o número de ocorrências do átomo u em t.

Algoritmo 2 Algoritmo para reduzir dedutibilidade em um passo em SLDE

1: **Entrada:** $T := \{t_0, \ldots, t_n\}$ e s
2: **Saída:** Um sistema $D(T, s)$ de equações Diofantinas lineares sobre as variáveis $X = \{x_0, \ldots, x_n\}$ tal que $T \vdash_E s$ se, e somente se, $D(T, s)$ é solúvel em um domínio que depende de E.
3: A cada t_i associa-se a variável x_i, $i = 1, \ldots, n$.
4: Para cada átomo a_i de s, introduz-se a equacão

$$\gamma(a_i, s) = \gamma(a_i, t_0)x_0 + \ldots + \gamma(a_i, t_n)x_n$$

que estabelece que o número de ocorrências de a_i em s é igual à soma do número de ocorrências de a_i em uma soma de $t'_j s$. O sistema $D(T, s)$ é a conjunção dessas equações:

$$D(T,s) = \begin{cases} \gamma(a_1, t_0)x_0 + \ldots + \gamma(a_1, t_n)x_n = \gamma(a_1, s) \\ \gamma(a_2, t_0)x_0 + \ldots + \gamma(a_2, t_n)x_n = \gamma(a_2, s) \\ \vdots \\ \gamma(a_m, t_0)x_0 + \ldots + \gamma(a_m, t_n)x_n = \gamma(a_m, s) \end{cases}$$

O seguinte lema mostra que o problema da dedutibilidade em um passo para a regra (GX) é redutível para o problema da solvabilidade de sistemas de equações Diofantinas sob

um domínio que depende da teoria equacional considerada. Este lema pode ser encontrado em [31] que é a versão estendida do artigo [30].

Lema 2 em [31] *Seja $T_S = \{t_1, \ldots, t_n\}$ um conjunto de termos e w_S o termo para o qual se quer decidir se $T_S \vdash w_S$. Considere o seguinte sistema de equações:*

$$S = \begin{cases} c_{1,1}x_1 + \ldots + c_{1,n}x_n = d_1 \\ \vdots \\ c_{m,1}x_1 + \ldots + c_{m,n}x_n = d_m \end{cases}$$

Suponha que $w_S = d_1.A_1 \oplus \ldots \oplus d_m.A_m$, onde $A = \{A_1, \ldots, A_m\}$ é o conjunto dos átomos de T_S. Para todo i, $1 \leq i \leq n$, suponha que $t_i = c_{1,i}.A_1 \oplus \ldots \oplus c_{m,i}.A_m$.

O sistema de equações (S) é satisfatível se, e somente se, $T_s \vdash w_s$ usando (A) e (GX).

Demonstração. ($\Rightarrow$) Se (S) é satisfatível então existe uma solução α de (S) tal que:

$$\begin{cases} c_{1,1}\alpha(x_1) + \ldots + c_{1,n}\alpha(x_n) = d_1 \\ \vdots \\ c_{m,1}\alpha(x_1) + \ldots + c_{m,n}\alpha(x_n) = d_m \end{cases} \tag{1.6}$$

Logo, pode-se computar w_S a partir de T_S e α:

$$\begin{aligned} &\alpha(x_1)t_1 \oplus \ldots \oplus \alpha(x_n)t_n \\ &= \alpha(x_1)(c_{1,1}A_1 \oplus \ldots c_{m_1}A_m) \oplus \ldots \oplus \alpha(x_n)(c_{1,n}A_1 \oplus \ldots \oplus c_{m,n}A_m) \\ &= c_{1,1}\alpha(x_1)A_1 \oplus \ldots \oplus c_{1,n}\alpha(x_n)A_1 \oplus \ldots \oplus c_{m_1}\alpha(x_1)A_m \oplus \ldots \oplus c_{m,n}\alpha(x_n)A_m \\ &= d_1A_1 \oplus \ldots \oplus d_mA_m = w_S \end{aligned} \tag{1.7}$$

Isto é, $w_S = \alpha(x_1)t_1 \oplus \ldots \oplus \alpha(x_n)t_n$e, portanto, $T_S \vdash w_S$ via (GX).

($\Leftarrow$) Seja P uma prova de $T_S \vdash w_S$, utilizando apenas (A) e (GX). Pode-se construir o sistem (S) a partir de T_S e w_S. Por hipótese, $w_s = d_1A_1 \oplus \ldots \oplus d_mA_m$ onde $A_1, \ldots, A_m$ são átomos de T_S. Além disso,

$$\begin{aligned} t_1 &= c_{1,1}A_1 \oplus \ldots \oplus c_{m,1}A_m \\ &\vdots \\ t_n &= c_{1,n}A_1 \oplus \ldots \oplus c_{m,n}A_m \end{aligned}$$

Como $T_S \vdash w_S$, então existem $x_1, \ldots, x_n$ tais que:

$$x_1t_1 \oplus \ldots \oplus x_nt_n = w_S$$

Isto é,

$$\begin{aligned} x_1(c_{1,1}A_1 \oplus \ldots \oplus c_{m,1}A_m) \oplus \ldots \oplus x_n(c_{1,n}A_1 \oplus \ldots \oplus c_{m,n}A_m) &= w_S \\ (c_{1,1}x_1 \oplus \ldots \oplus c_{1_n}x_n)A_1 \oplus \ldots \oplus (c_{m_1}x_1 \oplus \ldots \oplus c_{m,n}x_n)A_m &= w_S \end{aligned}$$

Portanto existe uma decomposição de d_i em $c_{i,j}$, dando origem ao seguinte sistema:

$$\begin{cases} c_{1,1}x_1 \oplus \ldots \oplus c_{1,n}x_n = d_1 \\ \vdots \qquad\qquad \vdots \\ c_{m,1}x_1 \oplus \ldots \oplus c_{m,n}x_n = d_m \end{cases}$$

que é satisfatível. □

Observação 1.5. *O domínio no qual o sistema de equações Diofantinas é resolvido depende da teoria equacional que é considerada:*

- ***Caso AC puro.*** *Obtém-se um sistema de equações Diofantinas sobre os* $\mathbb{N}$*. A solvabilidade de um sistema de equações Diofantinas sobre os naturais (*$\mathbb{N}$*) é um problema NP-completo [39]. Portanto, existe um algoritmo em NP para checar dedutibilidade em um passo para esta teoria. O mesmo vale para a teoria equacional* ***AC+homomorfismo*** *[31].*
- ***Caso Grupo Abeliano.*** *Considere o caso em que* $\oplus$ *é o operador de grupo Abelianos. Neste caso obtém-se um sistema de equações Diofantinas sobre* $\mathbb{Z}$*, cuja solvabilidade está em P [13, 17, 27, 39].*

Grupos Abelianos

Na introdução do trabalho [30] os autores afirmam que o problema da dedução do intruso no caso dos axiomas equacionais de grupos Abelianos é decidível em tempo polinomial (deterministicamente) seguindo as técnicas de generalização de McAllester.

Considere o caso em que $\oplus$ é o operador de Grupos Abelianos.

$(x \oplus y) \oplus z = x \oplus (y \oplus z)$	$0 \oplus x = x$
$x \oplus y = y \oplus x$	$x \oplus i(x) = 0$

Figura 1.2: E_{AG}: Teoria equacional de Grupos Abelianos

$0 \oplus x \to x$	$i(i(x)) \to x$
$x \oplus i(x) \to 0$	$i(0) \to 0$
	$i(x \oplus y) \to i(x) \oplus i(y)$

Figura 1.3: $\mathcal{R}_{AG}$: SRT de Grupos Abelianos módulo AC

Assumindo que nenhum termo encabeçado por $\oplus$ contem um átomo e seu inverso (apenas termos na forma normal são considerados), pode-se redefinir a função γ:

- se u é um átomo de t que não é encabeçado com I então $\gamma(u, t)$ para o número de ocorrências do átomo u em t,

- caso contrário, se $I(u)$ é um átomo de t, então $\gamma(u,t)$ denota o inverso do número de ocorrências de $I(u)$ em t.

Neste caso, obtém-se um sistema de equações Diofantinas lineares sobre $\mathbb{Z}$, que pode ser decidido em tempo polinomial.

Pelo Teorema 1 em [30], para obter a decidibilidade da relação de dedução para a teoria equacional de Grupos Abelianos, é necessário provar que o sistema $\mathcal{D}$ dado na Figura 1.6 é S-local, dado uma definição de subtermos S adequada.

Definição 1.43 (Subtermos S)**.** *Defina o conjunto de subtermos $S(t)$ de um termo t como o menor conjunto $S(t)$ tal que :*

- $t \in S(t)$*;*
- *se* $\langle u, v\rangle \in S(t)$ *então* $u, v \in S(t)$*;*
- *se* $\{u\}_k \in S(t)$ *então* $u, k \in S(t)$*;*
- *se* $u \in S(t)$ *então* $atomos(u) \in S(t)$ *;*
- *se* $i(u) \in S(t)$ *então* $u \in S(t)$*.*

Definição 1.44 ($I(T)$)**.** *Seja T um conjunto de termos, $I(T)$ é o conjunto das formas normais de todos os termos de T cujo o operador i é aplicado uma vez, isto é,*

$$I(T) := \{i(t)\downarrow \mid t \in T\}$$

Definição 1.45 (S_{T_I})**.** $S_{T_I}(T) = S(T \cup I(T))$*.*

Definição 1.46 ($SI_{\oplus}(T)$)**.** *Seja T um conjunto de termos. Defina $SI_{\oplus}(T)$ como o conjunto de todas as combinações de todos os termos de $S_{T_I}(T)$ pelo símbolo $\oplus$, isto é,*

$$SI_{\oplus}(T) := \left\{ \bigoplus_{s \in M} s \mid M \subseteq S_{T_I}(T) \right\} \tag{1.8}$$

Observe que o tamanho de $SI_{\oplus}(T)$ é exponencial no tamanho de $S_{T_I}(T)$.

Teorema 1.7 (S-localidade)**.** *Se existe uma prova de $T \vdash u$ então existe uma prova $SI_{\oplus}$-local de $T \vdash u$.*

Demonstração. A demonstração deste teorema consiste de vários lemas e técnicas de trasformação de prova. Para mais detalhes, veja o artigo [30]. □

Pelo Teorema 1 em [30], a demonstrabilidade no sistema de prova $\mathcal{D}$ é decídivel em tempo $\mathcal{K}_1 \times \mathcal{K}_2$, onde $\mathcal{K}_1$ denota a complexidade de tempo para se construir $SI_{\oplus}(T)$ e $\mathcal{K}_2$ representa a complexidade para se decidir a dedutibilidade em um passo para a teoria de grupos Abelianos. Desta forma, a demonstrabilidade no sistema $\mathcal{D}$ é exponencial em $|S_{T_I}(T)|$ e não polinomial como foi afirmado.

Capítulo 2

Teorias Localmente Estáveis Normais

Este capítulo destina-se ao estudo da decidibilidade do *problema da dedução do intruso* para uma subclasse de teorias equacionais: as *teorias localmente estáveis normais*. Esta subclasse de teorias pode ser representada por um sistema de reescrita de termos convergente módulo associatividade e comutatividade para o qual, dado um conjunto finito de mensagens Γ representando o conhecimento inicial do intruso, pode-se construir um conjunto saturado de termos (representado por $sat(\Gamma)$), que representa a informação extra que o intruso pode deduzir.

A decidibilidade baseia-se no estudo local das reduções de reescrita em termos relativamente "pequenos", que consistem de contextos formados por símbolos de função da assinatura relativa à teoria equacional considerada e outros nomes/constantes que são públicos, e cujos buracos podem ser preenchidos por um intruso (passivo) a partir de um conjunto de informações obtido através da observação de uma comunicação secreta. Essa classe de teorias tem como propriedade ser *estável*, isto é, a análise local dá uma caracterização do espaço de informações que um intruso pode obter através de raciocínio algébrico.

Esta metodologia foi introduzida inicialmente por M. Abadi e V. Cortier em [1], onde foi definida a classe das teorias *localmente estáveis* para a qual a decidibilidade da relação de dedutibilidade seria decidível em tempo polinomial com relação ao tamanho do conjunto $sat(\Gamma)$. Entretanto, a definição proposta não garantia a corretude do resultado de decidibilidade, uma vez que, quando feito um levantamento do estudo local das reduções, para um estudo global, o resultado perdia-se. Bem como, o algoritmo de decidibilidade, afirmado ser de tempo polinomial, tinha na verdade, complexidade exponencial, como pode ser visto na Seção 2.2.

Afim de obter a corretude do resultado, foi necessário adicionar uma condição à definição de uma teoria ser *localmente estável*: se $M \in sat(\Gamma)$ então $M \downarrow \in sat(\Gamma)$, onde $sat(\Gamma)$ é um conjunto finito e computável criado a partir de um conhecimento inicial Γ e que será definido na Seção 2.1. Mais ainda, para evitar computações desnecessárias, o estudo é feito em contextos normais. Neste capítulo, prova-se que o problema da dedução do intruso é decidível para teorias localmente estáveis normais. A polinomialidade só poderá ser obtida para uma classe ainda mais restrita de teorias, as chamadas *teorias*

localmente estáveis com inversos que será abordada no próximo capítulo. Partes deste capítulo foram publicadas no *7th Workshop on Logical and Semantic Frameworks, with Applications (LSFA 2012)* [6].

2.1 Problema de Dedução

Seja Σ um assinatura e E um conjunto de Σ-identidades. A teoria equacional $\approx_E$ representa as propriedades algébricas presentes nas primitivas criptográficas de um protocolo de segurança, bem como a capacidade de raciocínio algébrico de um intruso passivo.

Dado um conjunto finito $\Gamma = \{M_1, \ldots, M_n\}$ de termos básicos, que representa a informação disponível para um intruso, pode-se perguntar se um dado termo básico M pode ser deduzido de Γ usando raciocínio algébrico módulo um conjunto de identidades E. Esta relacão é descrita $\Gamma \vdash^? M$, e denota o *problema da dedução do intruso módulo* E.

Como foi visto na Seção 1.6, a relação de dedução mais conhecida neste contexto é conhecida como *modelo de Dolev-Yao* e é representada pelas regras da Tabela 1.1 (ver Capítulo 2). Relaxando a hipótese da criptografia perfeita, isto é, dando ao intruso a capacidade de raciocinar equacionalmente sobre as propriedades algébricas envolvidas no protocolo criptográfico, adicionam-se as regras (f_I) e $(\approx_E)$ abaixo. De agora em diante, o estudo da dedução do intruso baseia-se exclusivamente no raciocínio algébrico que pode ser induzido pelas identidades de E, dessa forma, apenas as regras da Tabela 2.1 serão consideradas. As regras remanescentes (UL), (UR), (D), (E) e (P) são disjuntas e podem ser analisadas separadamente.

$$(id)\ \frac{M \in \Gamma}{\Gamma \vdash M} \qquad (f_I)\ \frac{\Gamma \vdash M_1 \quad \ldots \quad \Gamma \vdash M_n}{\Gamma \vdash f(M_1, \ldots, M_n)}, f \in \Sigma_E \qquad (\approx_E)\ \frac{\Gamma \vdash N}{\Gamma \vdash M}, M \approx_E N$$

Tabela 2.1: Sistema $\mathcal{N}$: um sistema de dedução natural para dedução equacional do intruso

A partir deste capítulo regra (A) (axioma) introduzida anteriormente será renomeada para (id) (identidade) para fins notacionais. A regra (f_I) representa a *introdução de função* dos símbolos de função da assinatura Σ que estão presentes no conjunto de identidades de E (representado por Σ_E).

De acordo com o sistema de regras $\mathcal{N}$ tem-se que é permitido ao intruso:

1. deduzir cada mensagem que ele observou durante uma comunicação secreta (**Regra** (id));

2. aplicar funções, que fazem parte da assinatura relativa a um conjunto de identidades E imerso nas primitivas criptográficas do protocolo, às mensagens que ele pôde deduzir a partir do seu conhecimento inicial (**Regra** (f_I));

3. raciocinar algebricamente baseado na teoria equacional $\approx_E$ (**Regra** $(\approx_E)$).

A seguir, a menos que seja afirmado o contrário, chama-se de teoria equacional E a teoria equacional $\approx_E$ induzida pelas Σ-identidades de E.

A proposição abaixo dá uma caracterização algébrica preliminar do raciocínio dedutivo de um intruso passivo.

Proposição 2.1. *Seja E uma teoria equacional, M um termo básico e $\Gamma = \{M_1, \ldots, M_n\}$ um conjunto finito de termos básicos. Então $\Gamma \vdash M$ se, e somente se, existe um E-contexto C e termos $M'_1, \ldots, M'_r \in \Gamma$ tais que $C[M'_1, \ldots, M'_r] \approx_E M$.*

Demonstração. ($\Rightarrow$) Suponha que $\Gamma \vdash M$. A prova é por indução no tamanho da derivação $\mathcal{D}$ de $\Gamma \vdash M$:

Base da Indução $|\mathcal{D}| = 1$

Neste caso, $\Gamma \vdash M$ foi obtido via uma aplicação da regra (id). Portanto, $M \in \Gamma$ e $C[M] \approx_E M$ para um E-contexto C vazio.

Passo Indutivo Seja $\mathcal{D}$ uma derivação de $\Gamma \vdash M$. Para qualquer derivação $\mathcal{D}'$ de $\Gamma \vdash M'$ tal que $|\mathcal{D}'| < |\mathcal{D}|$ segue o resultado. A prova segue através da análise da última regra aplicada na derivação de $\Gamma \vdash M$.

1. A regra aplicada é (f_I)

   (a) f é um símbolo de função que não é associativo e nem comutativo.

   $$\frac{\dfrac{\mathcal{D}_1}{\Gamma \vdash M_1} \quad \ldots \quad \dfrac{\mathcal{D}_r}{\Gamma \vdash M_r}}{\Gamma \vdash M = f(M_1, \ldots, M_r)}\,(f_I)$$

   Por hipótese de indução, $M_i \approx_E C_i[M_{i1}, \ldots, M_{in_i}]$ para E-contextos C_i e termos $M_{i_j} \in \Gamma$, $1 \leq i \leq r$ e $1 \leq j \leq n_i$.

   Portanto,

   $$\begin{aligned} M &\approx_E f(C_1[M_{11}, \ldots, M_{1n_1}], \ldots, C_r[M_{r1}, \ldots, M_{rn_r}]) \\ &= C^*[M_{11}, \ldots, M_{1n_1}, \ldots, M_{r1}, \ldots, M_{rn_r}] \end{aligned}$$

   para algum E-contexto C^* e termos $M_{11}, \ldots, M_{1n_1}, \ldots, M_{r1}, \ldots, M_{rn_r} \in \Gamma$ e o resultado segue.

   (b) $f = \oplus$, onde $\oplus$ é um símbolo de função AC.

   Suponha que $\Gamma \vdash M = M_1 \oplus \ldots \oplus M_n$ (para algum $n \in \mathbb{N}$) é o termo na raiz da árvore de derivação. Suponha, sem perda de generalidade, que cada M_i não seja encabeçado por $\oplus$. Então, a árvore de prova deve ter a seguinte forma:

   $$\frac{\dfrac{\mathcal{D}_1}{\Gamma \vdash M_{i1}} \quad \ldots \quad \dfrac{\mathcal{D}_r}{\Gamma \vdash M_{ir}}}{\Gamma \vdash M = M_1 \oplus \ldots \oplus M_n}$$

   Para cada $j \in \{1, \ldots, r\}$ onde $r \in \mathbb{N}$ e $r \leq n$, tem-se o seguinte:

   - ou M_{i_j} é um termo de $\{M_1, \ldots, M_n\}$;

- ou é uma "soma" (via $\oplus$) cujos argumentos são termos de $\{M_1, \ldots, M_n\}$.

Em todo caso, por hipótese de indução, $M_{i_j} \approx_E C_j[M_{j_1}, \ldots, M_{j_{t_j}}]$ para E-contextos C_j e termos $M_{j_1}, \ldots, M_{j_{t_j}} \in \Gamma$, $1 \leq j \leq r$.

Portanto,

$$\begin{aligned} M &\approx_E M_{i_1} \oplus \ldots \oplus M_{i_r} \\ &= C_1[M_{11}, \ldots, M_{1t_1}] \oplus \ldots \oplus C_r[M_{r1}, \ldots, M_{rt_r}] \\ &= C^*[M_{11}, \ldots, M_{1t_1}, \ldots, M_{r1}, \ldots, M_{rt_r}] \end{aligned}$$

para algum E-contexto C^* e termos $M_{11}, \ldots, M_{1t_1}, \ldots, M_{r1}, \ldots, M_{rt_r} \in \Gamma$ e o resultado segue.

2. A regra aplicada é $\approx_E$

   Então

$$\frac{\dfrac{\mathcal{D}'}{\Gamma \vdash N}}{\Gamma \vdash M} \approx_E$$

   Por hipótese de indução, $N \approx_E C[M_1, \ldots, M_t]$ para algum E-contexto C e termos $M_1, \ldots, M_t \in \Gamma$. Uma vez que $N \approx_E M$ o resultado segue.

($\Leftarrow$) Suponha que $M \approx_E C[M_1, \ldots, M_r]$ para um E-contexto C e $M_1, \ldots, M_r \in \Gamma$. Por definição, C é formado usando apenas símbolos de função da assinatura Σ_E e seu tamanho é finito. O E-contexto C pode ser escrito como

$$C[M_1, \ldots, M_r] = f(C_1[M_{1_1}, \ldots, M_{1_{r_1}}], \ldots, C_n[M_{n_1}, \ldots, M_{n_{r_n}}])$$

para algum $f \in \Sigma_E$ com aridade n, E-contextos $C_1, \ldots, C_n$ e termos $M_{1_1}, \ldots, M_{n_{r_n}} \in \Gamma$ tais que $C_1[M_{1_1}, \ldots, M_{1_{r_1}}] \approx_E N_1, \ldots, C_n[M_{n_1}, \ldots, M_{n_{r_n}}] \approx_E N_n$, onde os termos $N_1, \ldots, N_n$ são tais que $M \approx_E f(N_1, \ldots, N_n)$. Como $|C_i| \leq |C|$ para $1 \leq i \leq n$, segue, por hipótese de indução, que $\Gamma \vdash N_1, \ldots, \Gamma \vdash N_n$.

Então,

$$\dfrac{\begin{array}{c}(\approx_E)\dfrac{\dfrac{\mathcal{P}_1}{\Gamma \vdash N_1}}{\Gamma \vdash C_1[M_{1_1}, \ldots, M_{1_{r_1}}]} \quad \ldots \quad (\approx_E)\dfrac{\dfrac{\mathcal{P}_n}{\Gamma \vdash N_n}}{\Gamma \vdash C_n[M_{n_1}, \ldots, M_{n_{r_n}}]} \\ (f_I)\end{array}}{(\approx_E)\dfrac{\Gamma \vdash f(C_1[M_{1_1}, \ldots, M_{1_{r_1}}], \ldots, C_n[M_{n_1}, \ldots, M_{n_{r_n}}])}{\Gamma \vdash M}}$$

□

Sempre que $C[M_1, \ldots, M_n] \approx_E M$ for decidível para algum E-contexto C e termos $M_1, \ldots, M_n \in \Gamma$, tem-se que o problema da dedução do intruso também será decidível. Este é um problema de unificação equacional de ordem superior, uma vez que a unificação ocorre em composições arbitrárias de símbolos de funções aplicados em termos. M. Abadi e V.Cortier em [1], propuseram um método para decidir tal problema de unificação, para as teorias chamadas *Localmente Estáveis*.

2.2 Teorias Localmente Estáveis

Em [1] , M.Abadi e V.Cortier consideram teorias equacionais com alguns símbolos associativos e comutativos que possuem um sistema de reescrita de termos associado $\mathcal{R}$ que é convergente módulo AC. Os autores desenvolveram a metodologia dentro da linguagem do *pi-cálculo aplicado* [2]. A seguir, as noções e os resultados principais deste trabalho serão reescritas utilizando a linguagem adotada e descrita no Capítulo 1.

Nesta seção, os resultados principais relacionados à decidibilidade do problema da dedução do intruso para uma subclasse de teorias AC, a saber, as teorias localmente estáveis serão comentados. Como poderá ser visto, o resultado apresentado pelos autores contém muitas imprecisões e erros, tanto conceituais quanto de complexidade. Conforme os problemas apareçam, comentários e contra-exemplos serão apresentados. Todos os contra-exemplos e correções apresentadas no decorrer deste trabalho foram confirmadas com o autor principal do trabalho [1].

A partir de um conjunto finito Γ de mensagens, que representa o conhecimento inicial do intruso, será definido um conjunto dos termos que podem ser deduzidos de Γ. Este conjunto satisfaz algumas propriedades de fechamento, como poderá ser visto a seguir. O seguinte conceito de *somas arbitrárias* é necessário:

Definição 2.1 ($sum_{\oplus}(S, \tilde{n})$)**.** *Seja $\oplus$ um símbolo de função arbitrário em Σ_E para uma teoria equacional $\approx_E$ induzida por um conjunto de identidades E. Escreva $\alpha \cdot_{\oplus} M$ para o termo $M \oplus \ldots \oplus M$, α vezes ($\alpha \in \mathbb{N}$). Dado um conjunto S de termos e um conjunto $\tilde{n}$ de nomes, escreva $sum_{\oplus}(S, \tilde{n})$ para o conjunto de somas arbitrárias dos termos em S e outros nomes, fechado módulo AC:*

$$sum_{\oplus}(S, \tilde{n}) = \left\{ \begin{array}{l|l} (\alpha_1 \cdot_{\oplus} T_1) \oplus \ldots \oplus (\alpha_n \cdot_{\oplus} T_n) & \alpha_i, \beta_j \in \mathbb{N}^* \\ \oplus & n_i \notin \tilde{n} \\ (\beta_1 \cdot_{\oplus} n_1) \oplus \ldots \oplus (\beta_k \cdot_{\oplus} n_k) & T_i \in S \end{array} \right\}$$

Tipicamente, os nomes em $\tilde{n}$ serão privados e os outros públicos.

Defina $sum(S) = \bigcup_{i=1}^{k} sum_{\oplus_i}(S, \tilde{n})$, onde $\oplus_1, \ldots, \oplus_k$ são símbolos associativos e comutativos da teoria.

Dada uma teoria equacional $\approx_E$ induzida pelo conjunto de equações E, um SRT $\mathcal{R}_E$ convergente módulo AC associado a E e um conjunto Γ de mensagens, sempre que for possível construir o conjunto $sat(\Gamma)$, através do fechamento via as regras do Sistema $\mathcal{N}$ da Tabela 2.1, obtém-se que a teoria equacional $\approx_E$ é *localmente estável*. Este conceito busca caracterizar o conjunto $sat(\Gamma)$ como *estável* na aplicação de contextos "pequenos". Aqui o conceito de pequeno é arbitrário e limitado pelo tamanho da teoria c_E (Definição 1.34). Esta restrição garante que o contexto seja grande o suficiente para que alguma regra de reescrita de $\mathcal{R}_E$ possa ser aplicada.

Na definição abaixo, a aplicação de uma regra de reescrita na cabeça de contextos "pequenos" aplicado a somas arbitrárias de termos de $sat(\Gamma)$ é novamente um contexto

"pequeno" C' aplicado a somas de termos em $sat(\Gamma)$. O tamanho de C' é limitado por c_E^2 mas outros limitantes podem ser utilizados.

Definição 6 de [1](Localmente Estável) *Uma teoria equacional E convergente módulo AC é* localmente estável *se, para todo conjunto finito $\Gamma = \{M_1, \ldots, M_n\}$ de termos básicos e na forma normal, existe um conjunto finito e computável $sat(\Gamma)$, fechado módulo AC, tal que*

1. *$M_1, \ldots, M_n \in sat(\Gamma)$, e $m \in sat(\Gamma)$ para todo $m \in fn(\Gamma)$;*
2. *se $M_1, \ldots, M_k \in sat(\Gamma)$ e $f(M_1, \ldots, M_k) \in st(sat(\Gamma))$, então $f(M_1, \ldots, M_k) \in sat(\Gamma)$, $f \in \Sigma_E$;*
3. *se $C[S_1, \ldots, S_l] \xrightarrow{h} M$, onde C é um E-contexto tal que $|C| \leq c_E$ e $fn(C) \cap \tilde{n} = \emptyset$, onde $S_1, \ldots, S_l \in sum_{\oplus}(sat(\Gamma), \tilde{n})$ para algum símbolo $AC \oplus$ (ou $S_i \in sat(\Gamma)$ se não existir símbolo AC), então existe um E-contexto C', um termo M', e $S'_1, \ldots, S'_k \in sum_{\oplus}(sat(\Gamma), \tilde{n})$ (ou $S'_1, \ldots, S'_k \in sat(\Gamma)$ se não existir símbolo AC), tal que $|C'| \leq c_E^2$, $fn(C') \cap \tilde{n} = \emptyset$, e $M \xrightarrow{*} M' =_{AC} C'[S'_1, \ldots, S'_k]$;*
4. *se $M \in sat(\Gamma)$ então $\Gamma \vdash M$.*

O conjunto $sat(\Gamma)$ pode não ser único ou minimal. Qualquer conjunto que satisfaça as 4 condições acima é adequado para os próximos resultados.

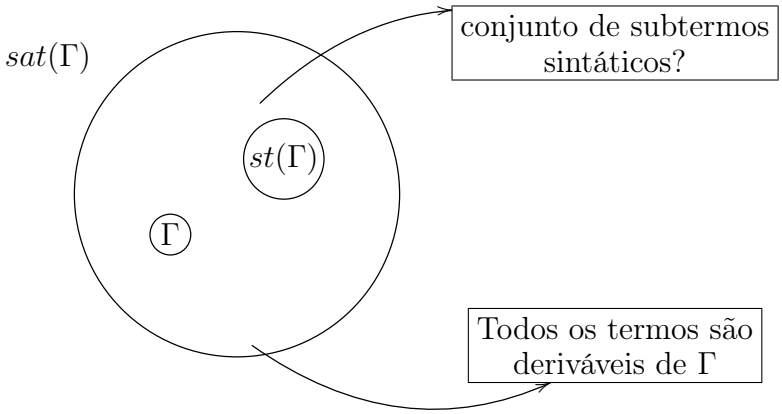


Figura 2.1: Conjunto $sat(\Gamma)$

Observação 2.1. *Note que a condição de $sat(\Gamma)$ ser* fechado módulo AC *faz com que $|sat(\Gamma)|$ seja pelo menos exponencial em $|\Gamma|$ sempre que Σ_E contiver pelo menos um símbolo de função AC.*

Observação 2.2. *Dado um termo M, a expressão $fn(M)$ representa o conjunto dos* nomes/constantes *que ocorrem em M e que não estão em $\tilde{n}$.*

Observação 2.3. *Na presença de símbolos de função AC, o conjunto dos subtermos sintáticos de um termo varia módulo AC, como foi mostrado no Exemplo 1.2.*

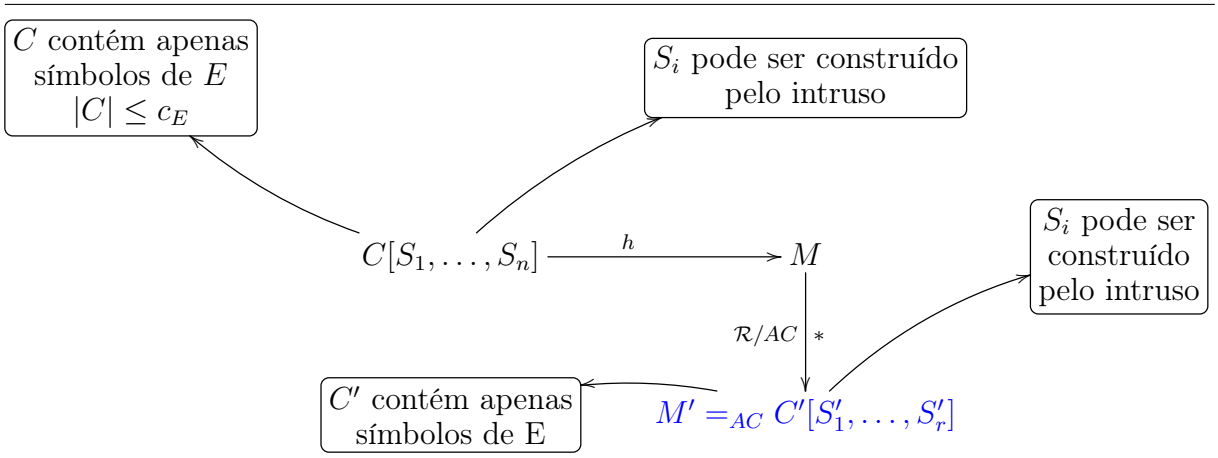


Figura 2.2: Condição 3 da Definição de $sat(\Gamma)$

Observação 2.4. *A regra 3 da Definição 6 em [1] busca garantir a estabilidade das reduções de reescrita:*

O seguinte Lema tem por objetivo generalizar a regra 3 da Definição 6 em [1]. Ele pode ser visto como um levantamento da estabilidade local para a *estabilidade global*, o que resulta em uma caracterização dos termos dedutíveis por um intruso passivo a partir de um conhecimento inicial Γ, utilizando a teoria equacional gerada por E. O objetivo é provar que aplicação de regras de reescrita em contextos de tamanhos arbitrários, aplicados a termos de $sat(\Gamma)$, em posições arbitrárias, é novamente um contexto aplicado a termos de $sat(\Gamma)$.

Lema 11 em [1] *Seja E uma teoria localmente estável. Seja $\Gamma = \{M_1, \ldots, M_n\}$ um conjunto de termos básicos e na forma normal. Para todo contexto C_1 tal que $fn(C_1) \cap \tilde{n} = \emptyset$, para todo $M_i \in sat(\Gamma)$, para todo termo T tal que $C_1[M_1, \ldots, M_k] \rightarrow T$, existe um contexto C_2 tal que $fn(C_2) \cap \tilde{n} = \emptyset$ e termos $M'_j \in sat(\Gamma)$ tal que $T \xrightarrow{*} C_2[M'_1, \ldots, M'_l]$.*

A demonstração deste Lema em [1] contém sérias imprecisões. A prova é dividida em dois casos:

1. A redução ocorre dentro de um dos termos M_i;

   Este caso se subdivide em outros dois casos:

   (a) $M_i \xrightarrow{h} M'_i$, para algum $i = 1, \ldots, k$.

   Por hipótese, E é localmente estável, e a prova segue pela Definição 6 de [1].

   (b) $M_i \rightarrow M'_i$, por uma redução que não ocorre na cabeça ($i = 1, \ldots, k$).

   A prova seria por indução na estrutura de M_i. Suponha que exista uma posição $q \in \mathcal{P}os(M_i)$ tal que $M_i|_q \xrightarrow{h} M'_{iq}$. Para que as condições da Definição 6 de [1] sejam alcançadas, é preciso garantir que $M_i|_q = C[M_{i1}, \ldots, M_{ir}]$ para um contexto C, com $|C| \leq c_E$ e termos $M_{i1}, \ldots, M_{ir} \in sat(\Gamma)$ e pelas hipóteses sobre $M_1, \ldots, M_r$, as condições não são necessariamente alcançadas. Logo, não é possível aplicar a hipótese de indução.

Este caso não pode ser provado com a Definição 6 em [1]. Este fato foi confirmado via comunicação pessoal com o autor principal de [1].

2. A redução não ocorre dentro dos termos M_i;

   Em certo momento na prova deste caso, afirma-se o seguinte:

   "(...)Tem-se que $T_2 == C_2[S_1, \ldots, S_k]$ para algum contexto C_2 tal que $|\_ \oplus C_2| \leq |M_0| \leq c_E$. "

   Este fato segue se a seguinte implicação é verdadeira: se $C[M_1, \ldots, M_k] = l\sigma$ para alguma regra $l \to r \in \mathcal{R}$ e substituição σ, então $|C| \leq |l|$. E este fato não é sempre verdade.

   Contra-exemplo: Considere o seguinte SRT:

   $$\mathcal{R} = \{x + 0 \to x;\ i(i(x)) \to x;\ x + i(x) \to 0; i(x + y) \to i(x) + i(y)\}.$$

   Considere o contexto $C[\_] = i(i(i(\_ + \_)))$ e os termos A e B. Observe que

   $$C[A, B] = i(i(i(A + B))) \xrightarrow{h} i(A + B)(\text{via regra } i(i(x)) \to x).$$

   Mas, $|C| > |i(i(x))|$.

Com os problemas descritos acima, o Lema responsável pelo levantamento da estabilidade de reduções de reescritas locais, para reduções de reescrita globais não segue. O que torna impossível provar os resultados preliminares para que o teorema de decidibilidade seja demonstrado em [1]:

Teorema 2 em [1] *Para teorias equacionais localmente estáveis, a dedução é decidível. Mais precisamente, dado um conjunto* Γ *e um termo* M*, uma vez que* $M\downarrow$ *e* $sat(\Gamma)$ *são computados,* $\Gamma \vdash M$ *pode ser decidido em tempo polinomial em* $M\downarrow$ *e* $sat(\Gamma)$*.*

Além disso, vale ressaltar que, mesmo que fosse possível provar o Lema 11 em [1], a polinomialidade afirmada no Teorema 2 em [1] não ocorre. Como pode ser visto em [1], a demonstração deste teorema segue, dentre outros resultados, da Proposição abaixo:

Proposição 16 em [1] *Seja* $\Gamma = \{M_1, \ldots, M_n\}$ *um conjunto de termos básicos,* M *um termo básico, e* $M\downarrow$ *seu conjunto de formas normais. Então* $\Gamma \vdash M$ *se, e somente se, existe um termo* $T \in M\downarrow$*, um contexto* C*, e termos* $M'_1, \ldots, M'_k \in sat(\Gamma)$ *tal que* $fn(C) \cap \tilde{n} = \emptyset$ *e* $T == C[M'_1, \ldots, M'_k]$*.*

Observe que $\Gamma \vdash M$ pode ser decidido checando se $M\downarrow$ é da forma $C[M_1, \ldots, M_k]$ com $M_1, \ldots, M_k \in sat(\Gamma)$.

M.Abadi e V.Cortier, em [1] afirmam que a existencialidade na Proposição acima pode ser verificada em tempo polinomial. Para isto, as seguintes afirmações são feitas:

- "Uma vez que $sat(\Gamma)$ é computado, verificar se existe C e $M_1, \ldots, M_k \in sat(\Gamma)$ tal que $fn(C) \cap \tilde{n} = \emptyset$ e $M\downarrow == C[M_1, \ldots, M_k]$ pode ser feito em tempo $\mathcal{O}(|M||\Gamma|^2)$. O procedimento pode ser descrito da seguinte forma:

1. Organize $sat(\Gamma)$ pelo tamanho dos termos (com custo $|sat(\Gamma)|^2$).
2. Para cada termo $T \in sat(\Gamma)$ (de termos de tamanho maximal para termos de tamanho minimal), verifique se T é igual a um subtermo de M. Quando este for o caso, delete este subtermo de M. Existem $|M|$ subtermos em M, e o teste de igualdade tem custo de $|T| < |\Gamma|$ computações, logo, este laço pode ser feito em tempo $|M||\Gamma|^2$.
3. Verifique se a parte remanescente de M ainda contém nomes privados em $\tilde{n}$. Se não for o caso, então o contexto C foi encontrado e $M_1, \ldots, M_k \in sat(\Gamma)$ tal que $fn(C) \cap \tilde{n} = \emptyset$ e $M \downarrow == C[M_1, \ldots, M_k]$; caso contrário, tal contexto não existe."

"Este procedimento é correto porque, ao eliminar-se subtermos de M que são iguais aos termos de $sat(\Gamma)$, inicia-se com termos em $sat(\Gamma)$ de tamanho maximal. Desta forma, conclui-se que $\Gamma \vdash M$ é decidível em tempo polinomial".

O seguinte contra-exemplo mostra que o procedimento proposto não pode ser executado em tempo polinomial:

Contra-Exemplo

Seja M um termo básico e na forma normal, e considere o seguinte conjunto:

$$sat(\phi) = \{T_{a1}, \ldots, T_{ar_a}, T_{b1}, \ldots, T_{br_b}, \ldots, T_{z1}, \ldots, T_{zr_z}\},$$

onde os termos estão organizados de forma crescente. O termo T_{kj} denota o j-ésimo termo de tamanho k.

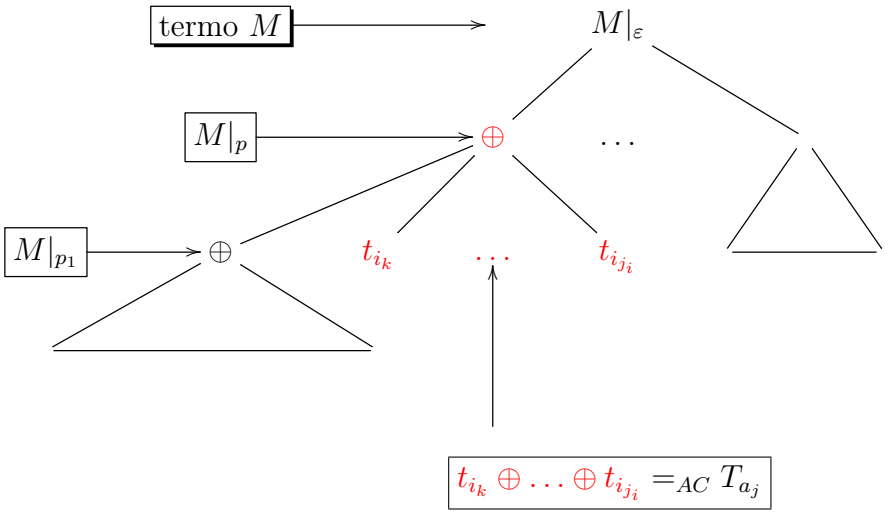
Suponha que cada T_{k_j} seja encabeçado por $\oplus$, isto é, tenha a forma:

$$T_{k_j} = t_1^j \oplus t_2^j \oplus \ldots \oplus t_k^j$$

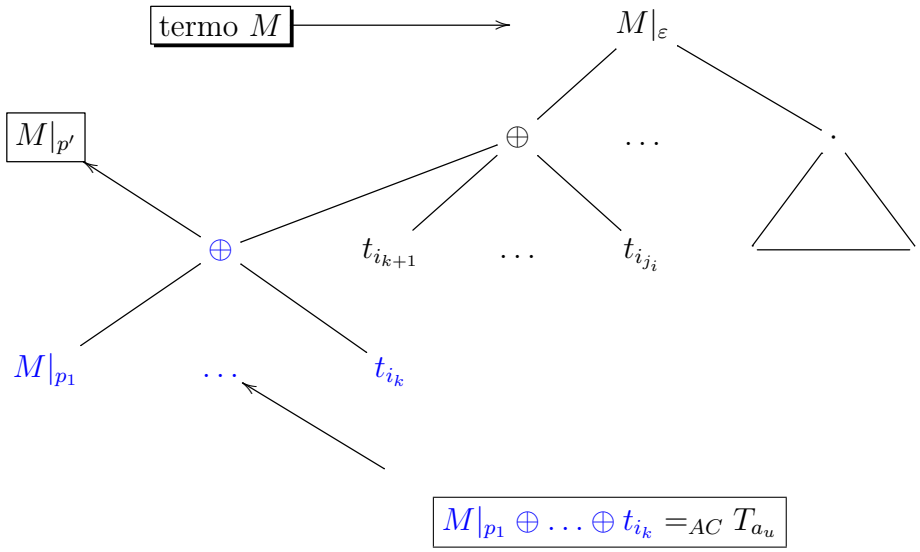
para $1 \leq j \leq r_k$,$1 \leq k \leq z$ e t_k^j não encabeçado com $\oplus$.

Existe um número exponencial de combinações de termos de $sat(\Gamma)$, mesmo quando se inicia de termos de tamanho maximal. Suponha que existam posições p e p' de M tais que $M|_p == T_{kj}$ e $M|_{p'} == T_{kj'}$, para j, j' e k. Observe que T_{kj} $T_{kj'}$ tem os mesmos tamanhos. Então, é preciso adivinhar qual deletar primeiro (Passo 2). Recursivamente, aplicando-se o mesmo raciocínio, podem existir posições q e q' do termo resultante de M' (obtido após deletar $M|p$ ou $M|p'$) tais que $M'|_q = T_{mi}$ e $M'|_{q'} = T_{mi'}$, e novamente é preciso adivinhar qual termo deletar primeiro. No fim do procedimento, pode-se obter uma saída NÃO, isto é, "M não pode ser escrito como $C[T_1, \ldots, T_k]$" , porém, se uma outra combinação de termos fosse escolhida ao decorrer do procedimento, uma saída SIM, poderia ter sido obtida. A complexidade de checar todas as possibilidades é exponencial. Portanto, a afirmação feita no passo 2 do procedimento proposto em [1] - **este laço pode ser feito em tempo** $|M||\phi|^2$- não é verdadeira.

Considere a seguinte ilustração do contra-exemplo:

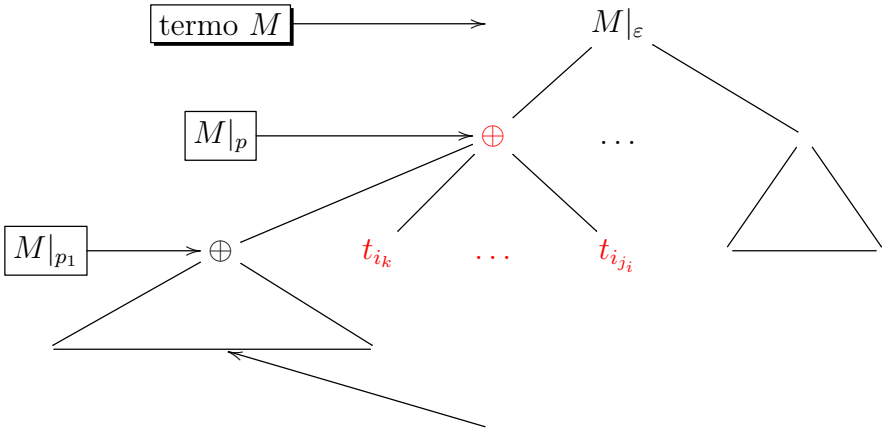


Utilizando as propriedades de associatividade e comutatividade, obtém-se a seguinte configuração de M:



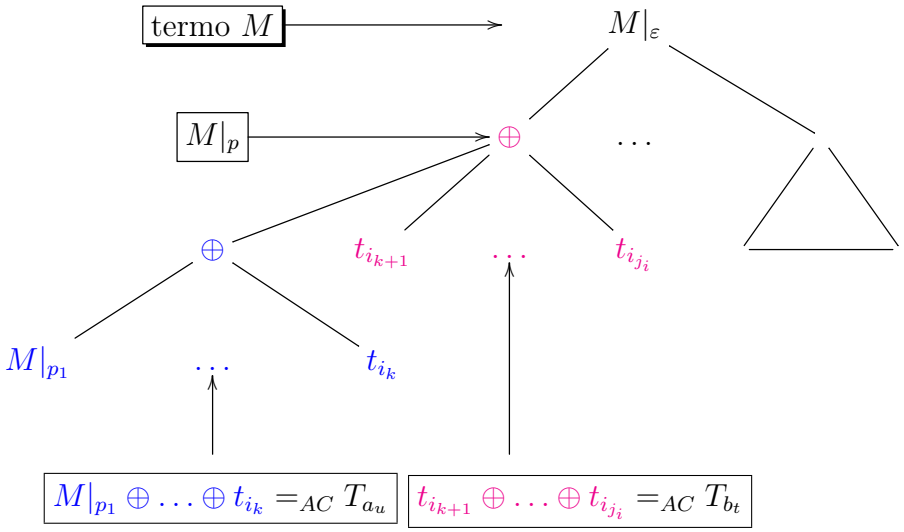
Qual deletar primeiro?

Suponha que a posição escolhida de M seja p, pode-se ter a seguinte situação:



Não existe um termo em $sat(\Gamma)$
que casa módulo AC com $M|_{p_1}$

Se, por outro lado, a posição p' de M tivesse sido escolhida, a seguinte situação poderia ocorrer:



- Observe que T_{a_j} e T_{a_u} tem os mesmos tamanhos. Então, é preciso "adivinhar" qual deletar primeiro, e isto induz o não-determinismo.
- A complexidade de checar todas as possibilidades é exponencial. Portanto, a afirmação feita no passo 2 do procedimento proposto em [1] - **este laço pode ser feito em tempo** $|M||\phi|^2$- não é verdadeira.

Exemplo 2.1. *Considere o seguinte conjunto* $sat(\Gamma)$*:*

$$sat(\Gamma) = \left\{ \begin{array}{l} n_1 \oplus n_{10} \oplus n_9 \oplus n_7 \oplus n_8 \ , \ n_2 \oplus n_6 \oplus n_4 \oplus n_9 \oplus n_7 \ , \\ n_2 \oplus n_3 \oplus n_5 \oplus n_7 \oplus n_8 \ , \ n_2 \oplus n_3 \oplus n_5 \oplus n_6 \oplus n_9 \ , \\ n_4 \oplus n_3 \oplus n_9 \oplus n_6 \oplus n_1 \ , \ n_1 \oplus n_4 \oplus n_2 \oplus n_9 \ , \\ n_1 \oplus n_3 \oplus n_5 \oplus n_6 \ , \ n_1 \oplus n_4 \oplus n_2 \oplus n_9 \ , \\ n_2 \oplus n_7 \oplus n_4 \oplus n_3 \ , \ n_3 \oplus n_{10} \oplus n_8 \oplus n_7, \\ n_5 \oplus n_7 \oplus n_3 \ , \ n_7 \oplus n_6 \oplus n_5 \ , \ n_1 \oplus n_2 \oplus n_3, \\ n_1 \oplus n_4 \ , \ n_7 \oplus n_4 \ , \ n_2 \oplus n_5 \ , \ n_7 \end{array} \right\}$$

e seja $M = n_1 \oplus n_7 \oplus n_5 \oplus n_4 \oplus n_6 \oplus n_3 \oplus n_2 \oplus n_9$ *um termo básico e na forma normal.*

O objetivo é encontrar termos $T_1, \ldots, T_k \in sat(\Gamma)$ *e um contexto* C *tal que* $M == C[T_1, \ldots, T_k]$.

1. *Iniciando com* $T_1 = n_1 \oplus n_{10} \oplus n_9 \oplus n_7 \oplus n_8$ *pode-se verificar que não existe um subtermo em* M *que é igual a* T_1*. Portanto, a resposta é NÃO.*

2. *Vá para o próximo termo* $T_2 = n_2 \oplus n_6 \oplus n_4 \oplus n_9 \oplus n_7$.

   Observe que o termo $M_1 = \mathbf{n_2} \oplus \mathbf{n_6} \oplus \mathbf{n_4} \oplus \mathbf{n_9} \oplus \mathbf{n_7} \oplus n_1 \oplus n_5 \oplus n_3 \in M\downarrow$. *Seguindo o procedimento, delete* T_2 *de* M_1 *obtendo* $M_1 = \Box \oplus n_1 \oplus n_5 \oplus n_3$ *e repita o procedimento novamente para* $M_1' = n_1 \oplus n_5 \oplus n_3$. *Não existe termo em* $sat(\Gamma)$ *que casa com a parte restante de* M_1'. *A resposta é NÃO.*

3. *Vá para o próximo termo* $T_3 = n_2 \oplus n_3 \oplus n_5 \oplus n_7 \oplus n_8$, *pode-se verificar que não existe subtermo em* M *que é igual a* T_3. *Portanto, a resposta é NÃO.*

4. *Vá para o próximo termo* $T_4 = n_2 \oplus n_3 \oplus n_5 \oplus n_6 \oplus n_9$.

   Observe que o termo $M_2 = \mathbf{n_2} \oplus \mathbf{n_3} \oplus \mathbf{n_5} \oplus \mathbf{n_6} \oplus \mathbf{n_9} \oplus n_1 \oplus n_7 \oplus n_4 \in M\downarrow$. *Seguindo o procedimento, delete* T_4 *de* M_2 *obtendo o termo* $M_2 = \Box \oplus n_1 \oplus n_7 \oplus n_4$ *e repita o procedimento novamente para* $M_2' = n_1 \oplus n_7 \oplus n_4$. *Seguindo este raciocínio, conclui-se que a escolha de termos importa. Na sequência, se o termo escolhido inicialmente fosse* $T_5 = n_1 \oplus n_4$ *seguido por* $T_6 = n_7$, *uma resposta positiva seria obtida.*

Afim de garantir que a metodologia proposta seja correta, várias mudanças são necessárias:

1. Uma nova definição de *teorias localmente estáveis* para a qual a prova do Caso 1(b) do Lema 11 em [1] possa ser completada (Definição 2.2).

2. Uma restrição no tipo de contextos, para que a afirmação 2 (b) da demonstração do Lema 11 em [1] seja verdadeira.

3. Um lema de minimização de E-contextos (Lema 2.1), este resultado foi considerado em [1], porém seu enunciado era impreciso e feito no decorrer de uma demonstração.

4. Uma proposição de classificação das ocorrências de instâncias de variáveis de regras que são aplicáveis em termos que podem ser construídos a partir dos termos de $sat(\Gamma)$ (Proposição 2.1).

5. Um novo algoritmo de decisão para a decidibilidade da relação de dedução para uma subclasse de teorias AC: as N-localmente estáveis normais.

6. Um algoritmo de decisão polinomial para a decidibilidade da relação de dedução para uma subclasse de teorias localmente estáveis normais : as teorias I-localmente estáveis.

7. Aplicação dos resultados para teorias de Grupos Abelianos finitos.

2.3 Teorias Localmente Estáveis Normais

Na sequência associa-se com cada conjunto Γ de mensagens, o conjunto dos subtermos que podem ser deduzidos a partir de Γ apenas pela aplicação de contextos "pequenos", e

depois o resultado pode ser levantado para contextos de tamanho arbitrário. O conceito de pequeno é arbitrário — na definição abaixo, limita-se o tamanho de um E-contexto C pelo tamanho da teoria equacional induzida por E, denotada por c_E (Definição 1.34), e o tamanho de C' por $p(c_E)$, onde p é uma função polinomial, mas outros limitantes podem ser adequados. Observe que limitando o tamanho de um E-contexto por c_E faz o contexto grande o suficiente para ser uma instância de qualquer uma das regras do SRT $\mathcal{R}$ associado a E.

Definição 2.2 (N-Localmente Estável *cf.* Definição 6 em [1])**.** *Uma teoria equacional AC-convergente E é* localmente estável normal *se, para um conjunto finito $\Gamma = \{M_1, \ldots, M_n\}$, onde os termos $M_1, \ldots, M_n$ são básicos e estão na forma normal, existe um conjunto finito e computável $sat(\Gamma)$ tal que*

1. *$M_1, \ldots, M_n \in sat(\Gamma)$;*
2. *se $M_1, \ldots, M_k \in sat(\Gamma)$ e $f(M_1, \ldots, M_k) \in st_{\oplus}(sat(\Gamma))$ então $f(M_1, \ldots, M_k) \in sat(\Gamma)$, para $f \in \Sigma_E$;*
3. *se $C[S_1, \ldots, S_l] \xrightarrow{h} M$, onde C é um E-contexto normal tal que $|C| \leq c_E$, $fn(C) \cap \tilde{n} = \emptyset$ e onde $S_1, \ldots, S_l \in sum_{\oplus}(sat(\Gamma), \tilde{n})$, para $\oplus$ um símbolo AC, então existe um E-contexto normal C', um termo M', um polinômio p, e termos $S'_1, \ldots, S'_k \in sum_{\oplus}(sat(\Gamma), \tilde{n})$, tais que $|C'| \leq p(c_E)$, $fn(C') \cap \tilde{n} = \emptyset$ e $M \xrightarrow{*}_{\mathcal{R} \cup AC} M' =_{AC} C'[S'_1, \ldots, S'_k]$;*
4. *se $M \in sat(\Gamma)$ então $M\!\downarrow \in sat(\Gamma)$.*
5. *se $M \in sat(\Gamma)$ então $\Gamma \vdash M$.*

Observe que o conjunto $sat(\Gamma)$ pode não ser único. Qualquer conjunto $sat(\Gamma)$ satisfazendo as cinco condições acima é adequando para os resultados.

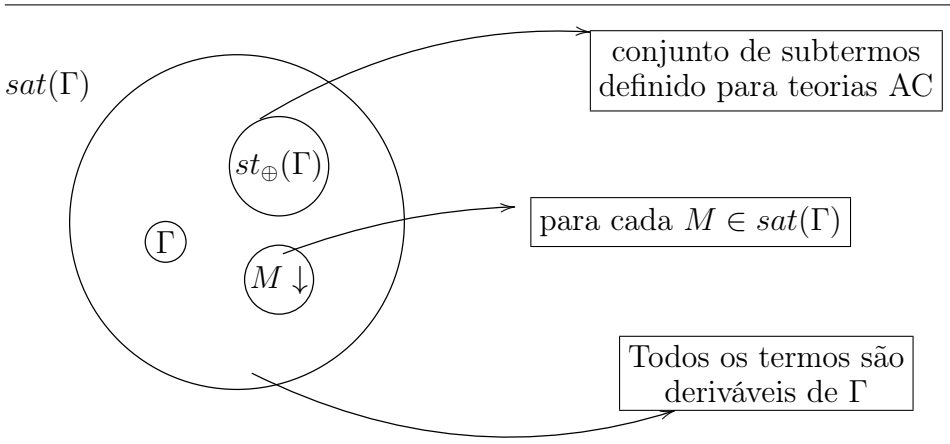


Figura 2.3: Conjunto $sat(\Gamma)$ para teorias **N**-localmente Estáveis

Diferentemente de [1] o conjunto $sat(\Gamma)$ não será fechado módulo associatividade e comutatividade. Isto faria $|sat(\Gamma)|$ exponencial em $|\Gamma|$ sempre que sua assinatura Σ_E

contém símbolos de função associativos e comutativos. Ao invés disso, a propriedade de associatividade e comutatividade será tratada no Lema 3.1.

Observação 2.5. *A adição da regra 4 na Definição 2.2 em relação à Definição 6 de [1] é necessária para provar o Lema 2.3, que é a versão do resultado de "levantamento" (Lema 11 em [1]). O conceito de contextos normais também é essencial para a demonstração deste lema*[1].

Observação 2.6. *A regra 2 da Definição 2.2 é baseada em uma função de subtermos $st_{\oplus}$ módulo AC, que mapeia um conjunto de subtermos em um conjunto de subtermos, onde $\oplus$ é um símbolo de função AC. Além disso, $st_{\oplus}$ depende da teoria equacional considerada.*

Com o objetivo de alcançar o resultado de estabilidade global, alguns resultados técnicos serão necessários.

O Lema 2.1 mostra que o estudo em termos genéricos da forma $C[T_1, \ldots, T_k]$, onde C é um E-contexto arbitrário e $T_1, \ldots, T_k \in sat(\Gamma)$ pode ser restrito para o estudo de E-contextos minimais utilizando uma técnica de transformação de contextos.

Lema 2.1 (Minimização de contextos)**.** *Sejam E uma teoria $\mathbf{N}$-localmente estável, C um E-contexto normal e $T_1, \ldots, T_k \in sat(\Gamma)$. Se existir uma posição p de C tal que $C|_p \neq \Box$ e existe uma posição q (não-vazia) com $C|_{pq} = \Box$ em C e $C[T_1, \ldots, T_k]|_p \in sat(\Gamma)$, então $C' \stackrel{def}{=} C[p \leftarrow \Box]$ é um contexto normal com $|C'| < |C|$.*

Demonstração. A prova segue pela busca de uma posição maximal $p \in \mathcal{P}os(C)$, da representação de árvore de C, tal que $C[T_1, \ldots, T_k]|_p \stackrel{def}{=} A$ e $A \in sat(\Gamma)$. Considera-se um novo E-contexto C' que será construído pela substituição do subcontexto $C|_p$ por um buraco $\Box$ que será instanciado por A. Isto é,

$$C[T_1, \ldots, T_k] == C'[T_{i_1}, \ldots, \underbrace{A}_{\text{posição } p}, \ldots, T_{i_r}]$$

onde $T_{i_1}, \ldots, T_{i_r} \in \{T_1, \ldots, T_k\}$ e C' é um E-contexto estritamente menor que C. $\Box$

A seguir, ilustra-se o processo de minimização de contextos.
Suponha que $C_1[T_1, \ldots, T_n] \in sat(\Gamma)$:
Então o contexto C será substituído pelo contexto C' da seguinte maneira:

Observação 2.7. *Se existir outra posição p' em C' com as hipóteses do Lema 2.1 poder-se-á transformar novamente. Observe que, como p é maximal, tem-se que $p||p'$. Iterando dessa forma (ou realizando transformações em paralelo), obtém-se um E-contexto minimal para C e $T_1, \ldots, T_k$.*

O seguinte lema caracteriza estruturalmente um E-contexto cujos buracos foram instanciados com termos de $sat(\Gamma)$ e que possui uma posição tal que o seu subtermo, nesta posição, é um termo redutível via uma regra do sistema de reescrita de termos associado à teoria equacional E que é **N**-localmente estável.

[1] Com estas condições adicionais, o Lema 11 em [1] pode também ser provado. Este fato foi confirmado via comunicação pessoal com o autor principal do artigo.

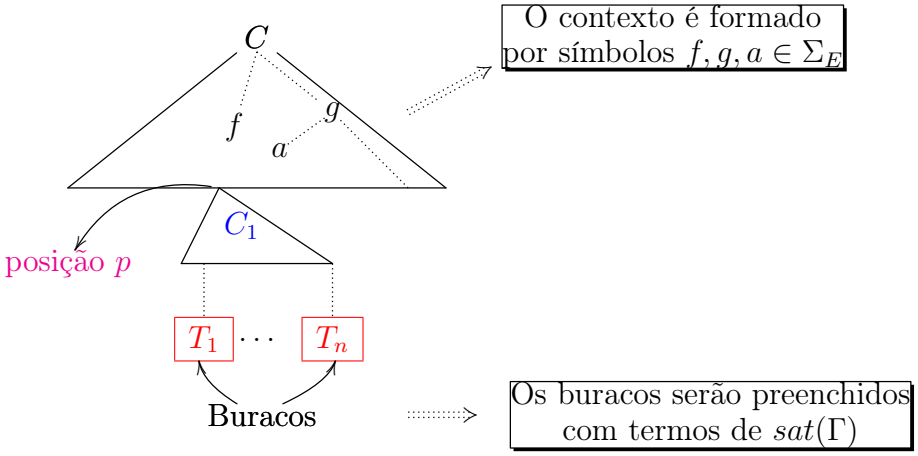


Figura 2.4: Minimização de Contextos, termo $C_1[T_1, \ldots, T_n] \in sat(\Gamma)$

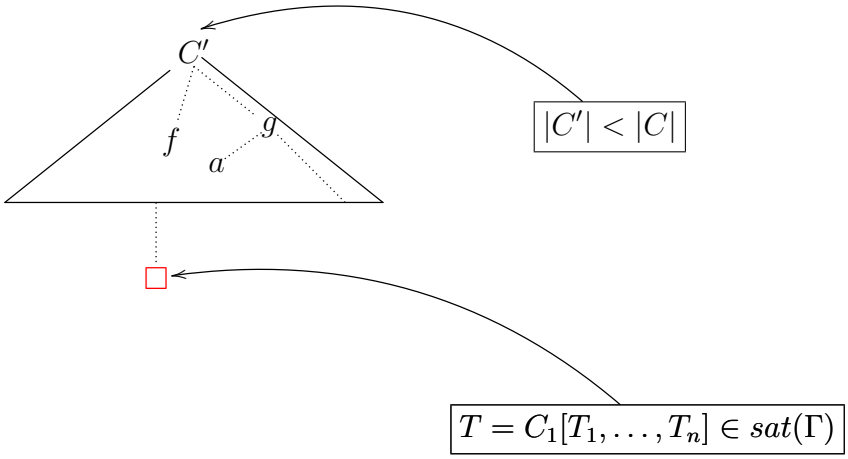


Figura 2.5: Minimização de contextos, o novo contexto C'

Lema 2.2 (Caracterização Estrutural de Redexes)**.** *Seja E uma teoria* **N***-localmente estável. Sejam C um E-contexto normal e $T_1, \ldots, T_k \in sat(\Gamma)$ tais que $C[T_1, \ldots, T_k] \to T$ via regra $M_0 \to N_0 \in \mathcal{R}_E$. Então, o termo $C[T_1, \ldots, T_k]$ pode ser escrito da seguinte forma:*

$$C[T_1, \ldots, T_k] =_{AC} C^*[T_{j_1}, \ldots, T_{j_s}, \underbrace{M'' \oplus M' \oplus \bigoplus_{i=1}^{r} C'_i[T_{i_1}, \ldots, T_{i_{r_i}}]}_{\text{posição } q}, T_{j_{s+1}} \ldots, T_{j_w}] \quad (2.1)$$

onde C'_i e C^* são E-contextos para $1 \leq i \leq r$ e algum $r \in \mathbb{N}$ e alguma posição q de $C[T_1, \ldots, T_k]$. Tem-se que $M' = M'_1 \oplus \ldots \oplus M'_t$ para algum $t \in \mathbb{N}$, $M'' = M''_1 \oplus \ldots \oplus M''_l$ para algum $l \in \mathbb{N}$ ($t \leq l$) tais que $M'_u \oplus M''_u \in sat(\Gamma)$, para $1 \leq u \leq l$. Para $1 \leq i \leq r$ tem-se que $C'_i|_\varepsilon \neq \oplus$ e $T_{j_1}, \ldots, T_{j_w}, T_{i_1}, \ldots, T_{i_{r_i}} \in \{T_1, \ldots, T_k\}$. Além disso,

$$M' \oplus \bigoplus_{i=1}^{r'} C'_i[T_{i_1}, \ldots, T_{i_{r_i}}] =_{AC} M_0\theta$$

para algum $r' \in \mathbb{N}$ e alguma substituição θ.

Demonstração. A prova deste lema segue pela análise da estrutura da regra $M_0 \to N_0$ de $\mathcal{R}_E$ que é aplicável em $C[T_1, \ldots, T_k]$ e a correspondente estrutura que este termo deve ter para que em alguma posição exista um possível subtermo redutível. Considere a representação do lado esquerdo da regra $M_0 \to N_0$ via um E-contexto cujos buracos foram instanciados com as variáveis de $\mathcal{V}ar(M_0)$:

$$M_0 = C_{M_0}[x_1, \ldots, x_{k_0}]$$

onde C_{M_0} é um E-contexto e $x_1, \ldots, x_{k_0} \in \mathcal{V}ar(M_0)$, assuma que as posições das variáveis são respeitadas bem como suas repetições.

Como a regra $M_0 \to N_0$ é aplicável em $C[T_1, \ldots, T_k]$ existe uma posição p tal que

$$C[T_1, \ldots, T_k]|_p =_{AC} C_{M_0}[x_1\theta, \ldots, x_{k_0}\theta].$$

Caso 1. Suponha que $C_{M_0}|_\varepsilon = f$, para algum $f \in \Sigma_E$ tal que $f \neq \oplus$.

Suponha que f seja um símbolo de função n-ário, para algum $n \in \mathbb{N}$. Então,

$$C[T_1, \ldots, T_k]|_p = f(C_1[T_{1_1}, \ldots, T_{1_{r_1}}], \ldots, C_n[T_{n_1}, \ldots, T_{n_{r_n}}])$$

onde $C_1, \ldots, C_n$ são E-contextos, $p \in \mathcal{P}os(C)$ e $T_{1_1}, \ldots, T_{1_{r_1}}, \ldots, T_{n_1}, \ldots, T_{n_{r_n}} \in \{T_1, \ldots, T_k\}$. Para facilitar a notação, escreva:

$$f(C_1[T_{1_1}, \ldots, T_{1_{r_1}}], \ldots, C_n[T_{n_1}, \ldots, T_{n_{r_n}}]) = C_p[T_{1_1}, \ldots, T_{1_{r_1}}, \ldots, T_{n_1}, \ldots, T_{n_{r_n}}]$$

Logo,

$$C[T_1, \ldots, T_k] =_{AC} C^*[\ldots, \underbrace{C_p[T_{1_1}, \ldots, T_{1_{r_1}}, \ldots, T_{n_1}, \ldots, T_{n_{r_n}}]}_{\text{posição } p}, \ldots].$$

E o resultado segue para $r = 1$ e termos M' e M'' vazios em (2.1).

Caso 2. Suponha que $C_{M_0}|_\varepsilon = \oplus$.

Prova-se por indução no número de ocorrências de $\oplus$ em C_{M_0} que $C[T_1, \ldots, T_k]|_p$ tem uma das seguintes formas:

(a) ou $C[T_1, \ldots, T_k]|_p = C'_1[T_{1_1}, \ldots, T_{1_{r_1}}] \oplus C'_2[T_{2_1}, \ldots, T_{2_{r_2}}]$ para E-contextos C'_1 e C'_2 e termos $T_{i_1}, \ldots, T_{i_{r_i}} \in \{T_1, \ldots, T_k\}$.

(b) $C[T_1, \ldots, T_k]|_p = R \oplus C'_1[T_{1_1}, \ldots, T_{1_{r_1}}]$ com $R = M'_1 \oplus \ldots \oplus M'_t$ e M'_j são subtermos dos termos $\{T_1, \ldots, T_k\}$ de $sat(\Gamma)$ $(1 \leq j \leq t)$.

Base da Indução. Suponha que exista apenas uma ocorrência de $\oplus$ em C_{M_0}.

Então, $C_{M_0} = C_{M_{01}}[x_1, \ldots, x_m] \oplus C_{M_{02}}[x_{m+1}, \ldots, x_{k_0}]$.

Logo, $C[T_1, \ldots, T_k]|_p = C'_1[T_{1_1}, \ldots, T_{1_{r_1}}] \oplus C'_2[T_{2_1}, \ldots, T_{2_{r_2}}]$ para E-contextos C'_1 e C'_2 e termos $T_{i_1}, \ldots, T_{i_{r_i}} \in \{T_1, \ldots, T_k\}$.

- $|C'_1| > 1$ e $|C'_2| > 1$

  Observe que como C'_1 e C'_2 são encabeçados por símbolos de função diferente de $\oplus$ então o resultado segue para $r = 2$ e termos M' e M'' vazios em (2.1). Isto é:

$$C[T_1, \ldots, T_k] =_{AC} C^*[\ldots, \underbrace{\bigoplus_{i=1}^{2} C'_i[T_{i_1}, \ldots, T_{i_{r_i}}]}_{\text{posição}-p}, \ldots]$$

  para algum E-contexto C^*. Neste caso $C[T_1, \ldots, T_k]|_p$ está no caso a).

- $C'_1 = \Box$ e $|C'_2| > 1$

  Suponha que exista uma posição $q \in \mathcal{P}os(C[T_1, \ldots, T_k])$ tal que $C[T_1, \ldots, T_k]|_q = T_u \oplus C'_2[T_{2_1}, \ldots, T_{2_{r_2}}]$, para um E-contexto C'_2 tal que $C'_2|_\varepsilon \neq \oplus$ e termos $T_u, T_{2_1}, \ldots, T_{2_{r_2}} \in \{T_1, \ldots, T_k\}$ e $T_u = T'_u \oplus T''_u$.

$$\begin{aligned} C[T_1, \ldots, T_k]|_q &= T_u \oplus C'_2[T_{2_1}, \ldots, T_{2_{r_2}}] \\ &= (T'_u \oplus T''_u) \oplus C'_2[T_{2_1}, \ldots, T_{2_{r_2}}] \\ &=_{AC} T''_u \oplus \underbrace{T'_u \oplus C'_2[T_{2_1}, \ldots, T_{2_{r_2}}]}_{=_{AC} M_0\theta} \end{aligned} \tag{2.2}$$

  Neste caso $C[T_1, \ldots, T_k]|_p$ está no caso b) para uma posição $p \in \mathcal{P}os(C[T_1, \ldots, T_k])$ tal que $C[T_1, \ldots, T_k]|_p = T'_u \oplus C'_2[T_{2_1}, \ldots, T_{2_{r_2}}]$.

Passo Indutivo. Suponha que existam n ocorrências de $\oplus$ em C_{M_0}.

Então, $C_{M_0} = C_{M_{01}}[x_1, \ldots, x_m] \oplus C_{M_{02}}[x_{m+1}, \ldots, x_{k_0}]$ para E-contextos C'_1 e C'_2 que possuem um número de ocorrências de $\oplus$ menor que n.

Considere o caso em que existam termos $T_{v_1}, \ldots, T_{v_s} \in \{T_1, \ldots, T_k\}$ para algum $v_s \in \mathbb{N}$, tais que $T_{v_h} = M'_{v_h} \oplus M''_{v_h}$, onde $1 \leq h \leq s$.

$$\begin{aligned} C[T_1, \ldots, T_k]|_p &= T_{v_1} \oplus \ldots \oplus T_{v_h} \oplus C'_1[T_{1_1}, \ldots, T_{1_{r_1}}] \\ &=_{AC} (M''_{v_1} \oplus \ldots \oplus M''_{v_h}) \oplus \underbrace{(M'_{v_1} \oplus \ldots \oplus M'_{v_h}) \oplus C'_1[T_{1_1}, \ldots, T_{1_{r_1}}]}_{=_{AC} M_0\theta} \end{aligned}$$

Se $C'_1|_\varepsilon$ não é encabeçado por $\oplus$ então o resultado segue para $r = 1$, e termos $M' = M'_{v_1} \oplus \ldots \oplus M'_{v_h}$ e $M'' = M''_{v_1} \oplus \ldots \oplus M''_{v_h}$.

Se, por outro lado, $C'_1|_\varepsilon = \oplus$, aplica-se a hipótese de indução em $C'_1[T_{1_1}, \ldots, T_{1_{r_1}}]$.

□

A seguinte proposição propõe uma classificação estrutural das instâncias das variáveis do lado esquerdo de uma regra $M_0 \to N_0$ que ocorrem no termo $C[T_1, \ldots, T_k]$ que é redutível por esta regra.

Proposição 2.2 (Classificação)**.** *Seja E uma teoria $\boldsymbol{N}$-localmente estável. Suponha que $C[T_1,\ldots,T_k] \to_{AC} T$ via uma aplicação de uma regra $M_0 \to N_0 \in \mathcal{R}_E$, para um E-contexto C e termos $T_1,\ldots,T_k \in sat(\Gamma)$ que satisfazem o Lema 2.1 .*

Então, existe um subtermo A de $C[T_1,\ldots,T_k]$ tal que

$$A \stackrel{def}{=} M' \oplus \bigoplus_{i=1}^{r'} C'_i[T_{i_1},\ldots,T_{i_{s_i}}] =_{AC} M_0\theta \qquad (\text{ para algum } r' \in \mathbb{N}, 1 \leq r' \leq r)$$

onde $C'_i|_\varepsilon \neq \oplus$ e $T_{i_1},\ldots T_{i_{r_i}} \in \{T_1,\ldots,T_k\}$, para $1 \leq i \leq r'$.
Para cada variável x de M_0, considere as ocorrências de $x\theta$ em A.

1. *ou $x\theta$ ocorre como um subtermo de M'_j para algum $j = 1,\ldots,l$;*
2. *ou $M' =_{AC} x\theta \oplus R$, para algum termo R que será casado com outras instâncias de variáveis em $\mathcal{V}ar(M_0)$;*
3. *ou $x\theta$ ocorre como um subtermo de T_{i_j} para algum i e algum j;*
4. *ou $x\theta =_{AC} C''[T'_1,\ldots,T'_s]$ para algum E-contexto C'' que satisfaz a Proposição 2.1 (isto é, $C'' \neq \Box$) e subtermos $T'_1,\ldots,T'_s$ dos termos $T_1,\ldots,T_k \in sat(\Gamma)$ tais que $C''[T'_1,\ldots,T'_s]$ com é subtermo de $C_i[T_{i_1},\ldots,T_{i_{s_i}}]$, para algum $s \in \mathbb{N}$;*
5. *ou $x\theta =_{AC} R \oplus \bigoplus_{i=1}^{k} C'_i[T_{i_1},\ldots,T_{i_{s_i}}]$ para algum subtermo R (que pode ser vazio) de M' e algum $k \in \mathbb{N}$, tal que $1 \leq k \leq r'$.*

Demonstração. Pelo lema de caracterização estrutural de redexes (Lema 2.2) tem-se que

$$C[T_1,\ldots,T_k] =_{AC} C^*[T_{j_1},\ldots,T_{j_s}, \underbrace{M'' \oplus M' \oplus \bigoplus_{i=1}^{r} C'_i[T_{i_1},\ldots,T_{i_{r_i}}]}_{\text{posição } q}, T_{j_{s+1}}\ldots,T_{j_w}]$$

onde C'_i e C^* são E-contextos para $1 \leq i \leq r$ e algum $r \in \mathbb{N}$ e alguma posição q de $C[T_1,\ldots,T_k]$. Tem-se que $M' = M'_1 \oplus \ldots \oplus M'_t$ para algum $t \in \mathbb{N}$, $M'' = M''_1 \oplus \ldots \oplus M''_l$ para algum $l \in \mathbb{N}$ ($t \leq l$) tais que $M'_u \oplus M''_u \in sat(\Gamma)$, para $1 \leq u \leq l$. Para $1 \leq i \leq r$ tem-se que $C'_i|_\varepsilon \neq \oplus$ e $T_{j_1},\ldots,T_{j_w},T_{i_1},\ldots,T_{i_{r_i}} \in \{T_1,\ldots,T_k\}$.

Suponha que os termos de $sat(\Gamma)$ estejam na forma normal (isto pode ser feito, uma vez que, pela Definição 2.2, para cada $M \in sat(\Gamma)$, tem-se que $M \downarrow \in sat(\Gamma)$.

Suponha também que a regra $M_0 \to N_0$ que é aplicada em A tenha a seguinte forma:

$$C_{M_0}[x_1,\ldots,x_{k_0}] \to C_{N_0}[x_1,\ldots,x_{k'_0}].$$

para E-contextos C_{M_0} e C_{N_0} cujos buracos foram instanciados com as variáveis $x_1 \ldots x_{k_0} \in \mathcal{V}ar(M_0)$ que podem ocorrer mais de uma vez em M_0 (M_0 e N_0 podem não ser lineares), para algum $k_0 \in \mathbb{N}$. Isto é, C_{M_0} é o contexto do termo M_0, no qual os buracos estão nas

posições de variáveis de M_0. Para ter uma instância $M_0\theta$ de M_0 é necessário manter a correspondência dos buracos da mesma variável. Desta forma, considere que

$$A \stackrel{def}{=} M' \oplus \bigoplus_{i=1}^{r'} C'_i[T_{i_1}, \ldots, T_{i_{s_i}}] =_{AC} C_{M_0}[x_1\theta, \ldots, x_{k_0}\theta] \tag{2.3}$$

para alguma substituição θ.

A prova segue por indução no número de ocorrências de $\oplus$ em C_{M_0}.

Base da Indução.

B.I.0) $n = 0$

Neste caso, não existem ocorrências de $\oplus$ em C_{M_0}. Este caso será dividido nos seguintes subcasos:

0.a) $l > 0$ e $r' = 0$

Isto é,

$$A \stackrel{def}{=} M' =_{AC} C_{M_0}[x_1\theta, \ldots, x_{k_0}\theta] \tag{2.4}$$

onde C_{M_0} não contém ocorrências de $\oplus$.

Para cada ocorrência de $x \in \mathcal{V}ar(M_0)$ em A, $x\theta$ ocorre como um subtermo de M'. Os seguintes subcasos devem ser analisados:

- ou $x\theta$ ocorre como um subtermo de M'_i, para algum índice $i = 1, \ldots, l$.
  Pela equação 2.4, tem-se que todo o termo M' deve ser casado com alguma parte de $C_{M_0}[x_1\theta, \ldots, x_{k_0}\theta]$.
  Quando $l > 1$ é necessário que outras variáveis de M_0 quando instanciadas com θ sejam casadas com a parte remanescente de M'. Como, por hipótese, $M' = M_1 \oplus \ldots \oplus M'_l$, seria necessária a ocorrência de pelo menos um $\oplus$ em C_{M_0}. Contradição.
  Quando $l = 1$, tem-se que cada ocorrência de uma variável x de M_0 é uma instância de um subtermo de M'_1. E a redução ocorreria em M'_1. Por hipótese, tem-se que $M'_1 \oplus M''_1 \in sat(\Gamma)$, e portanto, M'_1 está na forma normal. Contradição.
- ou $M' =_{AC} x\theta \oplus R$, para algum termo R.
  Como $M' =_{AC} C_{M_0}[x_1\theta, \ldots, x_{k_0}\theta]$, tem-se que o subtermo R de M' deve ser casado com instâncias de variáveis de M_0 via θ. Porém, se existir pelo menos uma ocorrência de variável $y \in \mathcal{V}ar(M_0)$ tal que $y\theta = R$, tem-se que: $M' = x\theta \oplus y\theta$, e então, C_{M_0} conteria uma instância de $\oplus$. Contradição.

0.b) $l = 0$ e $r' > 0$

Isto é,

$$A \stackrel{def}{=} \bigoplus_{i=1}^{r'} C'_i[T_{i_1}, \ldots, T_{i_{s_i}}] =_{AC} C_{M_0}[x_1\theta, \ldots, x_{k_0}\theta] \tag{2.5}$$

com $C'_i|_\varepsilon \neq \oplus$ e $C'_i \neq \Box$, para todo $i = 1, \ldots, r'$.

Observe que este caso só acontece quando $r' = 1$. Caso contrário, ocorrências de $\oplus$ em C_{M_0} seriam necessárias.

Suponha, então, que $r' = 1$. Então,

$$C[T_{1_1}, \ldots, T_{1_{s_1}}] =_{AC} C_{M_0}[x_1\theta, \ldots, x_{k_0}\theta].$$

Para cada ocorrência de $x \in \mathcal{V}ar(M_0)$ em A, tem-se que:

- ou $x\theta$ ocorre como um subtermo de T_{1_j}, para algum $j = 1, \ldots, s_1$.
- ou $x\theta = C_1''[T_1', \ldots, T_s']$ para algum subtermo $C_1''[T_1', \ldots, T_s']$ de $C_1'[T_{1_1}, \ldots, T_{1_{s_1}}]$.

0.c) $l > 0$ e $r' > 0$

Isto é,

$$A \stackrel{def}{=} M' \oplus \bigoplus_{i=1}^{r'} C_i'[T_{i_1}, \ldots, T_{i_{s_i}}] =_{AC} C_{M_0}[x_1\theta, \ldots, x_{k_0}\theta] \tag{2.6}$$

onde $C_i'|_\varepsilon \neq \oplus$ e $C_i' \neq \Box$, para todo $i = 1, \ldots, r'$.

Neste caso, pelo menos uma ocorrência de $\oplus$ em C_{M_0} é necessária. Este caso não acontece.

B.I.1) $n = 1$ (Este caso não é estritamente necessário, a verificação é feita apenas para induzir a recorrência.)

C_{M_0} contém exatamente uma ocorrência de $\oplus$. Isto é, C_{M_0} pode ser escrito da seguinte forma:

$$C_{M_0}[x_1, \ldots, x_{k_0}] = C^1_{M_0}[C_{M_{01}}[x_1, \ldots, x_u] \oplus C_{M_{02}}[x_{u+1}, \ldots, x_{k_0}]]$$

para E-contextos C^1_{M0}, C_{M_0} e C_{M_0} que não contém ocorrências de $\oplus$ e que podem ser vazios.

1.1 $C^1_{M0} = \Box$, isto é, C_{M_0} é $\oplus$.

Então,

$$C_{M_0}[x_1, \ldots, x_{k_0}] = C_{M_{01}}[x_1, \ldots, x_u] \oplus C_{M_{02}}[x_{u+1}, \ldots, x_{k_0}]$$

E assim,

$$A =_{AC} C_{M_{01}}[x_1\theta, \ldots, x_u\theta] \oplus C_{M_{02}}[x_{u+1}\theta, \ldots, x_{k_0}\theta]$$

Este caso se divide nos seguintes subcasos:

1.1.1) $l > 0$ e $r' = 0$.

Neste caso,

$$A \stackrel{def}{=} M' =_{AC} C_{M_{01}}[x_1\theta, \ldots, x_u\theta] \oplus C_{M_{02}}[x_{u+1}\theta, \ldots, x_{k_0}\theta]$$

Para cada ocorrência de $x \in \mathcal{V}ar(M_0)$ em A, $x\theta$ ocorre como um subtermo de M'.

1.1.2) $l = 0$ e $r' > 0$.

Então,

$$A \stackrel{def}{=} \bigoplus_{i=1}^{r'} C'_i[T_{i_1}, \ldots, T_{i_{s_i}}] =_{AC} C_{M_{01}}[x_1\theta, \ldots, x_u\theta] \oplus C_{M_{02}}[x_{u+1}\theta, \ldots, x_{k_0}\theta].$$

Se $r' = 1$, então $A = C'_1[T_{1_1}, \ldots, T_{1_{s_1}}]$. Por hipótese, $C'_1|_\varepsilon \neq \oplus$, logo não é possível que $A =_{AC} C_{M_{01}}[x_1\theta, \ldots, x_u\theta] \oplus C_{M_{02}}[x_{u+1}\theta, \ldots, x_{k_0}\theta]$, uma vez que o símbolo de função do topo é $\oplus$. Contradição.

Dessa forma, suponha que $r' > 1$ (e, portanto $r > 1$).

Para cada ocorrência de $x \in \mathcal{V}ar(M_0)$ em A, tem-se que:

1.1.2.a) ou $x\theta$ ocorre como um subtermo de T_{i_j}, para algum i e algum j;

1.1.2.b) ou $x\theta =_{AC} C'_{ij}[T_{i_{j_1}}, \ldots, T_{i_{j_s}}]$, tal que $C'_{1j}[T_{1j}, \ldots, T_{1_{j_s}}]$ é um subtermo de $C'_i[T_{i_1}, \ldots, T_{i_{s_i}}]$.

1.1.2.c) ou $x\theta$ ocorre como um termo da forma $x\theta =_{AC} R \oplus \bigoplus_{i=1}^{s'} C'_j[T_{j_1}, \ldots, T_{j_{s_j}}]$ para algum E-contexto C'_j tal que $C'_j|_\varepsilon \neq \oplus$, para algum $s' \in \mathbb{N}$ e algum termo R.

1.1.3) $l > 0$ e $r' > 0$.

$$\begin{aligned} A &\stackrel{def}{=} M' \oplus \bigoplus_{i=1}^{r'} C'_i[T_{i_1}, \ldots, T_{i_{s_i}}] \\ &=_{AC} C_{M_{01}}[x_1\theta, \ldots, x_u\theta] \oplus C_{M_{02}}[x_{u+1}\theta, \ldots, x_{k_0}\theta] \end{aligned}$$

Como $n = 1$, para $r' = 1$ tem-se que

$$A \stackrel{def}{=} M' \oplus C'_1[T_{1_1}, \ldots, T_{1_{s_1}}] =_{AC} C_{M_{01}}[x_1\theta, \ldots, x_u\theta] \oplus C_{M_{02}}[x_{u+1}\theta, \ldots, x_{k_0}\theta]$$

Para cada ocorrência de $x \in \mathcal{V}ar(M_0)$ em A, tem-se que

1.1.3.a) ou $x\theta$ ocorre como um subtermo de M';

1.1.3.b) ou $x\theta$ ocorre como um subtermo de T_{1_j}, para algum j;

1.1.3.c) ou $x\theta =_{AC} C'_{1j}[T_{1j}, \ldots, T_{1_{j_s}}]$, tal que $C'_{1j}[T_{1j}, \ldots, T_{1_{j_s}}]$ é um subtermo de $C'_1[T_{1_1}, \ldots, T_{1_{s_1}}]$.

1.1.3.d) ou $x\theta$ ocorre como um termo da forma $x\theta =_{AC} R \oplus \bigoplus_{i=1}^{s'} C'_j[T_{j_1}, \ldots, T_{j_{s_j}}]$ para algum E-contexto C'_j tal que $C'_j|_\varepsilon \neq \oplus$, para algum $s' \in \mathbb{N}$ e algum termo R.

1.2 $C^1_{M0} \neq \Box$, isto é, $C^1_{M0}|_\varepsilon = f$, para algum $f \neq \oplus$.

Suponha que $C_{M_0}[x_1, \ldots, x_{k_0}] = f(C'_{M_0}[C_{M01}[x_1, \ldots, x_u] \oplus C_{M02}[x_{u+1}, \ldots, x_{k_0}]])$, onde C'_{M_0}, C_{M01} e C_{M01} não possuem ocorrências de $\oplus$.

Este caso só é possível quando $l = 1$ ou $r' = 1$, mas não simultaneamente. A análise é análoga aos casos anteriores.

Passo Indutivo. Suponha que C_{M_0} contenha n ocorrências de $\oplus$. Isto é,

$$C_{M_0}[x_1, \ldots, x_{k_0}] = C'_{M_0}[C_{M01}[x_1, \ldots, x_u] \oplus C_{M02}[x_{u+1}, \ldots, x_{k_0}]]$$

para um E-contexto C'_{M_0} que não possui ocorrências de $\oplus$, e E-contextos C_{M01} e C_{M02} tais que $\#\{\text{ocorrências de } \oplus \text{ em } C_{M01}\} + \#\{\text{ocorrências de } \oplus \text{ em } C_{M02}\} = n - 1$. Este caso será dividido nos seguintes subcasos:

1. $C'_{M_0}|_\varepsilon = f$, $f \neq \oplus$.

   1.1 $l > 0$ e $r' = 0$, isto é, M_0 não é encabeçado por $\oplus$;

   Então,

   $$A \stackrel{def}{=} M' =_{AC} C'_{M_0}[C_{M01}[x_1\theta, \ldots, x_u\theta] \oplus C_{M02}[x_{u+1}\theta, \ldots, x_{k_0}\theta]]$$

   O único caso possível acontece quando $l = 1$ e então a redução ocorreria em M'_1. Porém, $M'_1 \oplus M''_1 \in sat(\Gamma)$ e portanto, M'_1 está na forma normal. Contradição.

   1.2 $l = 0$ e $r' > 0$;

   Então,

   $$A \stackrel{def}{=} \bigoplus_{i=1}^{r'} C'_i[T_{i_1}, \ldots, T_{i_{s_i}}] =_{AC} C'_{M_0}[C_{M01}[x_1\theta, \ldots, x_u\theta] \oplus C_{M02}[x_{u+1}\theta, \ldots, x_{k_0}\theta]]$$

   Como $C'_{M_0}|_\varepsilon \neq \oplus$, o único caso possível acontece quando $r' = 1$. Dessa forma, para cada $x \in \mathcal{V}ar(M_0)$, tem-se que:

   - ou $x\theta$ ocorre como um subtermo de T_{1_j}, para algum índice $j \in \mathbb{N}$.
   - ou $x\theta =_{AC} C'_{1_x}[T_{1_1}, \ldots, T_{1_{s_1}}]$ para algum E-contexto C'_{1_x} tal que $C'_{1_x}[T_{1_1}, \ldots, T_{1_{s_1}}]$ é subtermo de $C'_1[T_{1_1}, \ldots, T_{1_{s_1}}]$.

   E o resultado segue.

   1.3 $l > 0$ e $r' > 0$;

   Neste caso,

   $$\begin{aligned} A &\stackrel{def}{=} M' \oplus \bigoplus_{i=1}^{r'} C'_i[T_{i_1}, \ldots, T_{i_{s_i}}] \\ &=_{AC} C'_{M_0}[C_{M01}[x_1\theta, \ldots, x_u\theta] \oplus C_{M02}[x_{u+1}\theta, \ldots, x_{k_0}\theta]] \end{aligned}$$

   Como $C'_{M_0}|_\varepsilon \neq \oplus$, este caso não é possível.

2. $C'_{M_0} = \Box$, isto é, M_0 é encabeçado por $\oplus$.

   Então,

   $$C_{M_0}[x_1, \ldots, x_{k_0}] = C_{M01}[x_1, \ldots, x_u] \oplus C_{M02}[x_{u+1}, \ldots, x_{k_0}].$$

   Novamente, a análise será dividida nos seguintes subcasos:

2.1) $l > 0$ e $r' = 0$.

Então,

$$A \stackrel{def}{=} M'_1 \oplus \ldots \oplus M'_l =_{AC} C_{M01}[x_1\theta, \ldots, x_u\theta] \oplus C_{M02}[x_{u+1}\theta, \ldots, x_{k_0}\theta].$$

Suponha que a ocorrência de $\oplus$ explícita em C_{M_0} case com uma ocorrência de $\oplus$ de A da seguinte forma:

$$M'_1 \oplus \ldots \oplus M'_k =_{AC} C_{M01}[x_1\theta, \ldots, x_u\theta]$$
$$M'_{k+1} \oplus \ldots \oplus M'_l =_{AC} C_{M02}[x_{u+1}\theta, \ldots, x_{k_0}\theta].$$

com $1 \leq k \leq l$. Como C_{M01} e C_{M02} são E-contextos com um número $< n$ de ocorrências de $\oplus$ em sua composição, o resultado segue por hipótese de indução.

Suponha, agora, que a ocorrência de $\oplus$ explícita em C_{M_0} case com uma ocorrência de $\oplus$ de A da seguinte forma:

$$u_1 \oplus \ldots \oplus u_q =_{AC} C_{M01}[x_1\theta, \ldots, x_u\theta]$$
$$M^*_1 \oplus \ldots \oplus M^*_q \oplus M'_{q+1} \ldots \oplus M'_l =_{AC} C_{M02}[x_{u+1}\theta, \ldots, x_{k_0}\theta].$$

onde $M'_j = u_j \oplus M^*_j$ para $1 \leq j \leq q \leq l$. E o resultado segue por hipótese de indução.

2.2) $l = 0$ e $r' > 0$.

Então

$$A \stackrel{def}{=} \bigoplus_{i=1}^{r'} C'_i[T_{i_1}, \ldots, T_{i_{s_i}}] =_{AC} C_{M_{01}}[x_1\theta, \ldots, x_u\theta] \oplus C_{M_{02}}[x_{u+1}\theta, \ldots, x_{k_0}\theta]$$

Este caso só acontece quando a ocorrência de $\oplus$ explícita em C_{M_0} casa com a j-ésima ocorrência de $\oplus$ em A, para algum $j \in \mathbb{N}$, $1 \leq j \leq r'$. Isto é,

$$\bigoplus_{i=1}^{j} C'_i[T_{i_1}, \ldots, T_{i_{s_i}}] =_{AC} C_{M01}[x_1\theta, \ldots, x_u\theta]$$
$$\bigoplus_{i=j+1}^{r'} C'_i[T_{i_1}, \ldots, T_{i_{s_i}}] =_{AC} C_{M02}[x_{u+1}\theta, \ldots, x_{k_0}\theta]$$

e o resultado segue por hipótese de indução.

2.3) $l > 0$ e $r' > 0$.

Então,

$$A \stackrel{def}{=} M' \oplus \bigoplus_{i=1}^{r'} C'_i[T_{i_1}, \ldots, T_{i_{s_i}}] =_{AC} C_{M_{01}}[x_1\theta, \ldots, x_u\theta] \oplus C_{M_{02}}[x_{u+1}\theta, \ldots, x_{k_0}\theta]$$

As seguintes possibilidades devem ser analisadas:

– $M' =_{AC} C_{M_{01}}[x_1\theta, \ldots, x_u\theta]$ e $\bigoplus_{i=1}^{r'} C'_i[T_{i_1}, \ldots, T_{i_{s_i}}] =_{AC} C_{M_{02}}[x_{u+1}\theta, \ldots, x_{k_0}\theta]$.

– $R_1 =_{AC} C_{M_{01}}[x_1\theta, \ldots, x_u\theta]$ e $R_2 \oplus \bigoplus_{i=1}^{r'} C'_i[T_{i_1}, \ldots, T_{i_{s_i}}] =_{AC} C_{M_{02}}[x_{u+1}\theta, \ldots, x_{k_0}\theta]$, para subtermos R_1 e R_2 de M' tais que $M' =_{AC} R_1 \oplus R_2$.

– $R_1 \bigoplus_{i=1}^{m} C'_i[T_{i_1}, \ldots, T_{i_{s_i}}] =_{AC} C_{M_{01}}[x_1\theta, \ldots, x_u\theta]$ e $R_2 \bigoplus_{i=m+1}^{r'} C'_i[T_{i_1}, \ldots, T_{i_{s_i}}] =_{AC} C_{M_{02}}[x_{u+1}\theta, \ldots, x_{k_0}\theta]$ para subtermos R_1 e R_2 de M' tais que $M' =_{AC} R_1 \oplus R_2$ e algum $s \in \mathbb{N}$, com $m \leq r'$.

Em todos os casos o resultado segue por hipótese de indução.

□

Proposição 2.3. *O caso 5 da Proposição 2.2 não pode ocorrer simultaneamente com os casos 1, 2 ou 3 para ocorrências de uma mesma variável x.*

Demonstração. A demonstração é feita através da análise dos casos:

- Se 5 ocorresse simultaneamente com o caso 1 (ou 3) para ocorrências de uma mesma variável x, então

$$x\theta = R \oplus \bigoplus_{i=1}^{k} C'_i[T_{i_1}, \ldots, T_{i_{s_i}}]$$

seria um subtermo de T_i ou M'_i.

Logo, $C'_i[T_{i_1}, \ldots, T_{i_{s_i}}] \in st(M'_i) \subseteq st(M'_i \oplus M''_i) \subseteq st(sat(\Gamma))$, uma vez que $M'_i \oplus M''_i \in sat(\Gamma)$. Portanto, pelo item 2 da Definição 2.2, segue que $C'_i[T_{i_1}, \ldots, T_{i_{s_i}}] = T \in sat(\Gamma)$ contradizendo a hipótese de que o E-contexto C' satisfaz a Proposição 2.1 (i.e., $C'_i| \neq \Box$) para todo $i = 1, \ldots, k$. A análise é similar quando $C'_i[T_{i_1}, \ldots, T_{i_{s_i}}] \in st(T_i)$

- Se o caso 5 ocorre simultaneamente com o caso 2 para ocorrências de uma mesma variável x.

Por um lado,

$$x\theta = R \oplus \bigoplus_{i=1}^{k} C'_i[T_{i_1}, \ldots, T_{i_{s_i}}]$$

para um subtermo R de M'.

Por outro lado,

$$M' = x\theta \oplus R_1.$$

para algum subtermo R_1 de M'.

Então $M' =_{AC} R \oplus C'_i[T_{i_1}, \ldots, T_{i_{s_i}}] \oplus R_1$. Como, para todo $i = 1, \ldots, k$, $C'_i|_\varepsilon \neq \oplus$ e $C'_i \neq \Box$, tem-se que $C'_i[T_{i_1}, \ldots, T_{i_{s_i}}]$ é um subtermo de M'_j, para algum $1 \leq j \leq l$, e a contradição segue similarmente ao caso anterior.

□

Observação 2.8. *Observe o que acontece quando o caso 5 da Proposição 2.2 ocorre simultaneamente com o caso 4 para uma ocorrência de uma mesma variável x tem-se:*

Por um lado,

$$x\theta = R \oplus \bigoplus_{i=1}^{k} C'_i[T_{i_1}, \ldots, T_{i_{s_i}}]$$

para algum subtermo R (que pode ser vazio) de M' e algum $k \in \mathbb{N}$, tal que $1 \leq k \leq r'$. Por outro lado,

$$x\theta =_{AC} C''[T'_1, \ldots, T'_s]$$

para algum E-contexto C'' que satisfaz a Proposição 2.1 (isto é, $C'' \neq \Box$) e subtermos $T'_1, \ldots, T'_s$ dos termos $T_1, \ldots, T_k \in sat(\Gamma)$ tais que $C''[T'_1, \ldots, T'_s]$ é subtermo de $C'_j[T_{j_1}, \ldots, T_{j_{s_j}}]$, para algum $j \in \mathbb{N}$, $1 \leq j \leq r'$. Desta forma,

$$R \oplus \bigoplus_{i=1}^{k} C'_i[T_{i_1}, \ldots, T_{i_{s_i}}] =_{AC} C''[T'_1, \ldots, T'_s] =_{AC} C'_j[T_{j_1}, \ldots, T_{j_{s_j}}]|_q.$$

para alguma posição $q \neq \varepsilon$.

Por hipótese, $T'_1, \ldots, T'_s$ são subtermos dos termos $T_1, \ldots, T_k \in sat(\Gamma)$, a única forma de separar os termos $T_1, \ldots, T_k \in sat(\Gamma)$ em subtermos "independentes" acontece quando este termo for encabeçado por $\oplus$. Isto é, existe pelo menos um termo $T_n = u_n \oplus v_n$ em $sat(\Gamma)$, para algum índice $n \in \mathbb{N}$ e subtermos u_n e v_n tal que o E-contexto C'_j tem a seguinte forma:

$$\begin{aligned} C'_j[T_{j_1}, \ldots, T_n, \ldots, T_{j_{s_j}}] &=_{AC} C''_j[C^*_j[T_{j_1}, \ldots, T_{n-1}, T_{n+1}, \ldots, T_s] \oplus T_n, \ldots, T] \\ &=_{AC} C''_j[C^*_j[T_{j_1}, \ldots, T_{n-1}, T_{n+1}, \ldots, T_s] \oplus (u_n \oplus v_n), \ldots, T_{j_{s_j}}] \\ &=_{AC} C''_j[\underbrace{(C^*_j[T_{j_1}, \ldots, T_{n-1}, T_{n+1}, \ldots, T_s] \oplus u_n)}_{C'_j[T_{j_1}, \ldots, T_{j_{s_j}}]|_q} \oplus v_n, \ldots, T_{j_{s_j}}] \end{aligned}$$

Proposição 2.4. *O caso 4 da Proposição 2.2 não pode ocorrer simultaneamente com os casos 1, 2 ou 3.*

Demonstração. A prova segue pela análise dos casos.

- Quando o caso 4 ocorre simultaneamente com o caso 1 ou 3 para a mesma variável $x \in \mathcal{V}ar(M_0)$ a análise é similar à prova do lema anterior.

- Quando o caso 4 ocorre simultaneamente com o caso 2 a contradição segue do fato de C'' satisfazer a Proposição 2.1.

□

O seguinte lema estende a propriedade de estabilidade local de redução via reescrita de contextos pequenos para contextos de tamanhos arbitrários. Intuitivamente, este resultado mostra que o estudo local de reduções de reescrita em termos que podem ser construídos pelo intruso a partir de um conhecimento prévio é suficiente para a análise do raciocínio equacional no caso geral.

Lema 2.3 (Estabilidade Global *cf.* Lema 11 em [1])**.** *Seja E uma teoria $\boldsymbol{N}$-localmente estável e um conjunto $\Gamma = \{M_1, \ldots, M_n\}$ de termos básicos e na forma normal. Para todo E-contexto C_1, e termos $T_1, \ldots, T_k \in sat(\Gamma)$, tais que $C_1[T_1, \ldots, T_k] \rightarrow_{\mathcal{R} \cup AC} T$, existe um E-contexto C_2, e termos $T'_i \in sat(\Gamma)$, tais que $T \stackrel{*}{\rightarrow}_{\mathcal{R} \cup AC} C_2[T'_1, \ldots, T'_l]$.*

Demonstração. Suponha que $C_1[T_1, \ldots, T_k] \rightarrow_{AC} T$, para um E-contexto normal C_1 e termos $T_1, \ldots, T_k \in sat(\Gamma)$. Observe que, como E é AC-convergente, todo E-contexto pode ser normalizado (Proposição 1.1). Além disso, por hipótese, $C_1[T_1, \ldots, T_k] \rightarrow_{\mathcal{R} \cup AC} T$ e portanto, segue da Proposição 2.2 que:

$$C_1[T_1, \ldots, T_k] = C'[M'' \oplus M' \oplus \bigoplus_{i=1}^{r} C'_i[T_{i_1}, \ldots, T_{i_{s_i}}], T_1, \ldots, T_k],$$

para algum E-contexto C' e algum $r \in \mathbb{N}$. Para cada $i = 1, \ldots, r$, $C'_i|_\epsilon \neq \oplus$, $C'_i \neq \Box$, $T_{i_1}, \ldots, T_{i_{s_i}} \in sat(\Gamma)$, $i_j \in \{1, \ldots, k\}$, os termos M' e M'' são tais que $M' = M'_1 \oplus \ldots \oplus M'_l$, $M'' = M''_1 \oplus \ldots \oplus M''_l$ com $M'_j \oplus M''_j \in sat(\Gamma)$, onde $l \in \mathbb{N}$ e $1 \leq j \leq l$. Então, existe um subtermo A de $C_1[T_1, \ldots, T_k]$ tal que

$$A \stackrel{def}{=} M' \oplus \bigoplus_{i=1}^{r'} C'_i[T_{i_1}, \ldots, T_{i_{s_i}}] \qquad (\text{ para algum } r' \in \mathbb{N}, 1 \leq r' \leq r)$$

é uma instância $M_0\theta$ (módulo AC) do (le) de alguma regra $M_0 \rightarrow N_0 \in \mathcal{R}_E$. Para cada $x \in \mathcal{V}ar(M_0)$ tem-se que $x\theta$ ocorre como nos casos 1, 2, 3, 4 ou 5, para alguma substituição θ.

A prova segue pela análise da redução $C_1[T_1, \ldots, T_k] \rightarrow_{\mathcal{R} \cup AC} T$. Como, pela definição de $sat(\Gamma)$ (Definição 2.2), para cada termo $T \in sat(\Gamma)$ tem-se que $T \downarrow \in sat(\Gamma)$, assume-se, a seguir, que os termos $T_1, \ldots, T_k \in sat(\Gamma)$ estão todos na forma normal. Portanto, a redução não ocorre dentro dos termos T_i, $1 \leq i \leq k$.

Sem perda de generalidade, assuma que as ocorrências das variáveis de M_0 são $x_1, \ldots, x_{k_1}$, $y_1, \ldots, y_{k_2}$, $z_1, \ldots, z_{k_3}$, onde x_i's estão nos casos 1, 2 ou 3, z_r's estão no caso 4 que não ocorrem simultaneamente com o caso 5, e os y_j's estão no caso 5 ou no caso 4 que ocorrem simultaneamente com o caso 5.

Para cada variável y_j, considere as l ocorrências de y_j em A:

$$\begin{aligned} y_j\theta &=_{AC} R_j^1 \oplus \bigoplus_{i=1}^{k} C_{1i}^j[T_{i_1}^1, \ldots, T_{i_{s_i}}^1](\text{ 1}^{\text{o}}\text{ ocorrência}) \\ &=_{AC} R_j^2 \oplus \bigoplus_{i=1}^{k} C_{2i}^j[T_{i_1}^2, \ldots, T_{i_{s_i}}^2](\text{ 2}^{\text{o}}\text{ ocorrência}) \\ &\vdots \\ &=_{AC} R_j^l \oplus \bigoplus_{i=1}^{k} C_{li}^j[T_{i_1}^l, \ldots, T_{i_{s_i}}^l](\text{ l-ésima ocorrência}) \end{aligned} \tag{2.7}$$

onde para cada u, $1 \leq u \leq l$, R_j^u é subtermo de M', e cada E-contexto $C_{u_i}^j$ satisfaz as propriedades da Proposição 2.2. Os superíndices nos termos $T_{i_1}, \ldots, T_{i_{s_i}} \in sat(\Gamma)$ indicam o número da ocorrência que cada um desses termos ocorre.

Para cada i, denote por $cl(C_{ui}^j[T_{i_1}^u, \ldots, T_{i_{s_i}}^u])$ a classe de $C_{ui}^j[T_{i_1}^u, \ldots, T_{i_{s_i}}^u]$ módulo AC, e associe com um nome fresco $a_{cl(C_{ui}^j[T_{i_1}^u, \ldots, T_{i_{s_i}}^u])}$ cada classe $cl(C_{ui}^j[T_{i_1}^u, \ldots, T_{i_{s_i}}^u])$, $1 \leq u \leq l$. Desta forma, $a_{cl(C_{ui}^j[T_{i_1}^u, \ldots, T_{i_{s_i}}^u])} = a_{cl(C_{vi}^j[T_{i_1}^v, \ldots, T_{i_{s_i}}^v])}$ sempre que $C_{ui}^j[T_{i_1}^u, \ldots, T_{i_{s_i}}^u]) =_{AC} C_{vi}^j[T_{i_1}^v, \ldots, T_{i_{s_i}}^v])$, para algum $1 \leq v \leq l$.

Em cada equação

$$R_j^u \oplus \bigoplus_{i=1}^{k} C_{ui}^j[T_{i_1}^u, \ldots, T_{i_{s_i}}^u] =_{AC} R_j^v \oplus \bigoplus_{i=1}^{k} C_{vi}^j[T_{i_1}^v, \ldots, T_{i_{s_i}}^v],$$

cada $C_{ui}^j[T_{i_1}^u, \ldots, T_{i_{s_i}}^u]$ deve ser igual módulo AC a um dos $C_{vi}^j[T_{i_1}^v, \ldots, T_{i_{s_i}}^v]$.

Se algum $C_{ui}^j[T_{i_1}^u, \ldots, T_{i_{s_i}}^u]$ fosse igual a algum subtermo de R^v (para algum v), então $C_{ui}^j[T_{i_1}^u, \ldots, T_{i_{s_i}}^u]$ seria um termo de $sat(\Gamma)$, contradizendo a Lema 2.1.

Logo,

$$\begin{aligned} R_j^1 \oplus \bigoplus_{i=1}^{k} a_{cl(C_{1i}^j[T_{i_1}^1, \ldots, T_{i_{s_i}}^1])} &=_{AC} \\ R_j^2 \oplus \bigoplus_{i=1}^{k} a_{cl(C_{2i}^j[T_{i_1}^2, \ldots, T_{i_{s_i}}^2])} &=_{AC} \\ \vdots \\ R_j^l \oplus \bigoplus_{i=1}^{k} a_{cl(C_{li}^j[T_{i_1}^l, \ldots, T_{i_{s_i}}^l])} &\stackrel{def}{=} T_{y_j}. \end{aligned} \tag{2.8}$$

Para cada variável z_t ($1 \leq t \leq k_3$) considere as $m \in \mathbb{N}$ ocorrências de z_t em A:

$$z_t\theta =_{AC} \underbrace{C''_{t_1}[T_1^1, \ldots, T_r^1]}_{1^{\text{o}}\text{ ocorrência}} =_{AC} \ldots =_{AC} \underbrace{C''_{t_m}[T_1^m, \ldots, T_r^m]}_{m-\text{ésima ocorrência}}.$$

Observe que o subíndice $w \in \{1, \ldots, m\}$ representa a ocorrência de z_t em A. Para cada w, o E-contexto C''_{t_w} e os termos $T_1^w, \ldots, T_r^w$ satisfazem as condições do caso 4 da Proposição 2.2. Similarmente ao caso anterior, escreva $cl(C''_{t_w}[T_1^w, \ldots, T_r^w])$ para a classe de $C''_{t_w}[T_1^w, \ldots, T_r^w]$ módulo AC, e associe o nome fresco $b_{cl(C''_t[T_1,\ldots,T_r]))}$ com cada classe.

Logo,

$$z_t\theta =_{AC} b_{cl(C''_t[T_1,\ldots,T_r])}. \tag{2.9}$$

Seja θ' uma substituição tal que:

$$\begin{aligned} x_i\theta' &= x_i\theta \\ y_j\theta' &= T_{y_j} \\ z_t\theta' &= b_{cl(C''_t[T_1,\ldots,T_r])}. \end{aligned}$$

Seja T_2 o termo obtido de $\bigoplus_{i=1}^{r'} C'_i[T_{i_1}, \ldots, T_{i_{s_i}}]$ substituindo cada $C^j_{ui}[T^u_{i_1}, \ldots, T^u_{i_{s_i}}]$ com $a_{cl(C^j_{ui}[T^u_{i_1},\ldots,T^u_{i_{s_i}}])}$ e cada $C''_{t_w}[T_1^w, \ldots, T_r^w]$ com $b_{cl(C''_t[T_1,\ldots,T_r])}$:

$$\begin{aligned} &\bigoplus_{i=1}^{r'} C'_i[T_{i_1}, \ldots, T_{i_{s_i}}] = C'_1[T_{1_1}, \ldots, T_{1_{s_1}}] \oplus \ldots \oplus C'_{r'}[T_{r'_1}, \ldots, T_{r'_{s_{r'}}}] \\ &=_{AC} \bigoplus_{i=1}^{k} C'_i[T_{i_1}, \ldots, T_{i_{s_i}}] \oplus \bigoplus_{u=k+1}^{r'} \underbrace{C'_u[T_{u_1}, \ldots, T_{u_{s_u}}]}_{\text{instances of } y} \\ &=_{AC} \bigoplus_{i=1}^{k} C'_i[T_{i_1}, \ldots, T_{i_{s_i}}] \oplus \bigoplus_{u=m+1}^{s} a_{cl(C'_u[T_{u_1},\ldots,T_{u_{s_u}}])} \\ &= \ldots = C_2[S_1, \ldots, S_n] \oplus S'_a = C_3[S_1, \ldots, S_n, S'_a] == T_2 \end{aligned} \tag{2.10}$$

onde $S_1, \ldots, S_n, S'_a \in sum_{\oplus}(sat(\Gamma), \tilde{n})$ e $|C_3| \leq |C_{M_0}|$.

Por um lado, $A = M' \oplus \bigoplus_{i=1}^{r} C'_i[T_1, \ldots, T_k] =_{AC} M_0\theta$. Por outro lado, $M' \oplus T_2$ é uma instância $M_0\theta'$ de M_0. Portanto,

$$M' \oplus M'' \oplus T_2 \xrightarrow{h} M'' \oplus N_0\theta'$$

onde $M' \oplus M'' =_{AC} \bigoplus_{i=1}^{l} M'_i \oplus M''_i = S'$, para algum $S' \in sum_{\oplus}(sat(\Gamma), \tilde{n})$, uma vez que $M'_i \oplus M''_i \in sat(\Gamma)$, para $1 \leq i \leq l$.

Portanto, $M' \oplus M'' \oplus T_2 =_{AC} S' \oplus C_2[S_1, \ldots, S_n] = C_4[S', S_1, \ldots, S_n] \xrightarrow{h}_{AC} M'' \oplus N_0\theta'$. Observe que, uma vez que C_4 é um E-contexto normal, segue que $|C_4| = |C_{M_0}| \leq c_E$, aplicando a regra 3 da Definição 2.2 segue o resultado.

□

Como consequência segue o seguinte Corolário:

Corolário 2.1. *Seja E uma teoria $\mathbf{N}$-localmente estável. Seja $\Gamma = \{M_1, \ldots, M_n\}$ um conjunto de termos básicos e na forma normal. Para todo E-contexto C_1, termos $M'_1, \ldots, M'_k \in sat(\Gamma)$ e para todo T na forma normal tais que $C_1[M'_1, \ldots, M'_k] \stackrel{*}{\rightarrow}_{\mathcal{R} \cup AC} T$, existe um E-contexto normal C_2 e termos $M''_1, \ldots, M''_l \in sat(\Gamma)$ tais que $T =_{AC} C_2[M''_1, \ldots, M''_l]$.*

Demonstração. Suponha que $C_1[M'_1, \ldots, M'_k] \stackrel{*}{\rightarrow}_{\mathcal{R} \cup AC} T$, onde C_1 é um E-contexto, os termos $M'_1, \ldots, M'_k \in sat(\Gamma)$ e T é um termo na forma normal. Ou $C_1[M'_1, \ldots, M'_k] =_{AC} T$ e o resultado segue; ou existe um termo T_1 tal que $C_1[M'_1, \ldots, M'_k] \rightarrow_{\mathcal{R} \cup AC} T_1 \stackrel{*}{\rightarrow}_{\mathcal{R} \cup AC} T$. Pelo Lema 2.3, existem um E-contexto C_2 e termos $M_{11}, M_{12}, \ldots, M_{1r_1} \in sat(\Gamma)$ tais que $T_1 \stackrel{*}{\rightarrow} C_2[M_{11}, \ldots, M_{1r_1}]$. Por AC-confluência, como T é uma forma normal, $C_2[M_{11}, \ldots, \ldots, M_{1r_1}] \stackrel{*}{\rightarrow}_{\mathcal{R} \cup AC} T$. Uma vez que E é AC-terminante, repete-se este procedimento até que $T =_{AC} C[M''_1, \ldots, M''_l]$ é obtido, para um E-contexto C e termos $M''_1, \ldots, M''_l \in sat(\Gamma)$. □

Na sequência mostra-se que qualquer termo M dedutível de Γ é igual módulo AC a um E-contexto sobre termos em $sat(\Gamma)$. Este Lema é similar à Proposição 16 em [1], aqui verifica-se $=_{AC}$ (igualdade módulo associatividade-comutatividade) ao invés de $==$ (igualdade sintática).

Lema 2.4 (*cf.* Proposição 16 em [1])**.** *Seja E um teoria $\mathbf{N}$-localmente estável. Seja $\Gamma = \{M_1, \ldots, M_n\}$ um conjunto finito de termos básicos na forma normal, e M um termo básico na forma normal. Então $\Gamma \vdash M$ se, e somente se, existe um E-contexto C e termos $M'_1, \ldots, M'_k \in sat(\Gamma)$ tais que $M =_{AC} C[M'_1, \ldots, M'_n]$.*

Demonstração. Se $M =_{AC} C[M'_1, \ldots, M'_k]$ para termos $M'_1, \ldots, M'_k \in sat(\Gamma)$ e um E-contexto C então, pela Definição 2.2, tem-se que $\Gamma \vdash M'_i$ para cada $i \in \{1, \ldots, k\}$. Pela Proposição 2.1, $M_i \approx_E C_i[M_{i1}, \ldots, M_{in_i}]$, para E-contextos C_i e termos $M_{i1}, \ldots, M_{in_i} \in \Gamma$, $1 \leq i \leq k$. Portanto,

$$M \approx_E C[C_1[M_{11}, \ldots, M_{1n_1}], \ldots, C_k[M_{k1}, \ldots, M_{kn_k}]],$$

isto é, existem um E-contexto C^* e termos $M''_1, \ldots, M''_t \in \Gamma$ tais que $M \approx_E C^*[M''_1, \ldots, M''_t]$. Pela Proposição 2.1, $\Gamma \vdash M$.

Reciprocamente, se $\Gamma \vdash M$ então, pela Proposição 2.1, $M \approx_E C[M_1, \ldots, M_1]$ para um E-contexto C e termos $M_1, \ldots, M_k \in \Gamma \subset sat(\Gamma)$. Uma vez que M está na forma normal, $C[M_1, \ldots, M_k] \stackrel{*}{\rightarrow} M$, aplicando o Corolário 2.1, existem um E-contexto C_2 e termos $M'_1, \ldots, M'_k \in sat(\Gamma)$ tais que $M =_{AC} C_2[M'_1, \ldots, M'_k]$ e o resultado segue. □

Como consequência dos resultados anteriores será possível obter a decidibilidade do problema da dedução do intruso para teorias **N**-localmente estáveis. A decidibilidade é obtida via um algoritmo que verifica um caso de casamento módulo AC de ordem superior que será proposto para a demonstração do Lema 3.1 que será enunciado no próximo capítulo. O seguinte lema é, na verdade, um corolário do Lema 3.1.

Lema 2.5. *Seja E um teoria $\mathbf{N}$-localmente estável, $\Gamma = \{M_1, \ldots, M_n\}$ um conjunto finito de termos básicos na forma normal e M um termo básico na forma normal. Então a questão se existe um E-contexto normal C e $T_1, \ldots, T_k \in sat(\Gamma)$ tais que $M =_{AC} C[T_1, \ldots, T_k]$ é decidível em tempo polinomial não determinístico em $|M|$ e $|sat(\Gamma)|$.*

Demonstração. A prova deste lema é consequência do Lema 3.1 e da Observação 3.3. □

Teorema 2.1. *A decidibilidade do* Problema da Dedução do Intruso *está em NP para teorias* **N***-localmente estáveis.*

Demonstração. A prova deste teorema é consequência dos Lemas 2.4 e 2.5. □

No próximo capítulo um limitante polinomial para a decidibilidade do problema da dedução do intruso para um caso restrito de teorias localmente estáveis normais será estudado.

Capítulo 3

Teorias Localmente Estáveis com Inversos

Afim de obter um algoritmo de decisão polinomial para o problema de segurança descrito no capítulo anterior será necessário restringir ainda mais a teoria equacional imersa na capacidade de raciocínio algébrico do intruso. Será necessário considerar a existência de inversos para cada símbolo associativo e comutativo na assinatura da teoria equacional considerada. Define-se então uma nova subclasse de teorias equacionais convergentes módulo associatividade e comutatividade de algum símbolo de função binário: as *teorias localmente estáveis com inversos*. Esta teoria equacional é **N**-localmente estável com a propriedade adicional de ser fechada para aplicação de inversos.

Mais precisamente, este capítulo destina-se a resolver um problema de casamento equacional de ordem superior restrito (Lema 2.1) que foi proposto no Capítulo 3: dada uma teoria equacional $\approx_E$ induzida por um conjunto de identidades E, existe um E-contexto normal C tal que $M =_{AC} C[T_1, \ldots, T_k]$ para termos $T_1, \ldots, T_k \in sat(\Gamma)$?

O algoritmo de decidibilidade que será proposto no Lema 3.1 baseia-se em uma busca na ávore de representação dos termos de $sat(\Gamma)$. Uma parte do algoritmo consiste de um caso restrito do problema do casamento módulo associatividade e comutatividade, o chamado *Casamento AC com Ocorrências Distintas*, que foi introduzido na Seção 1.5.1 do Capítulo 2. Uma outra parte recairá em resolver sistemas de equações Diofantinas lineares sobre $\mathbb{Z}$ e os inversos serão interpretados como *inteiros negativos*. Este algoritmo roda em tempo polinomial (determinístico) para a classe de teorias **I**-localmente estáveis. O mesmo algoritmo pode ser utilizado para decidir o PDI para a classe de teorias **N**-localmente estáveis, a ausência de inversos implica em resolver sistemas de equações Diofantinas lineares sobre $\mathbb{N}$, e neste caso a decidibilidade está em NP..

Para ilustrar o resultado, na Seção 3.2.1, mostra-se que a teoria equacional de Grupos Abelianos de ordem n (dada) é localmente estável com inversos. Para isto, foi necessário definir um sistema de reescrita de termos convergente módulo AC para esta teoria equacional. Vale ressaltar que não foi encontrado disponível na literatura nenhum estudo relacionado a esta teoria equacional particular, dessa forma, pode-se afimar que o sistema de reescrita associado a esta teoria, bem como este exemplo de aplicação são inéditos

e fazem sentido em aplicações de segurança, uma vez que protocolos criptográficos que contém propriedades de grupos Abelianos em suas primitivas criptográficas, fazem uso de grupos finitos. Partes deste capítulo foram publicadas no *7th Workshop on Logical and Semantic Frameworks, with Applications (LSFA 2012)* [6].

3.1 Teorias Localmente Estáveis com Inversos

Seja Σ uma assinatura e $\approx_E$ a teoria equacional induzida por um conjunto E de Σ-identidades. Para os resultados a seguir assuma que E satisfaz a seguinte propriedade:

(*) *E é uma teoria **N**-localmente estável cuja assinatura Σ_E contém, para cada símbolo de função associativo-comutativo $\oplus$, seu correspondente* inverso $i_\oplus$.

Isto é, os seguintes resultados são relacionados à teorias equacionais E que contenham a seguinte equação:

$$x \oplus i_\oplus(x) = e_\oplus \tag{3.1}$$

para cada símbolo de função associativo-comutativo $\oplus$ em Σ_E, onde $i_\oplus$ é o símbolo de função unário que representa o inverso de $\oplus$ e $e_\oplus$ é o elemento neutro correspondente.

Pode-se definir, a partir de um conjunto finito Γ de informações (mensagens), um conjunto saturado de termos que leva em consideração a teoria equacional envolvida na álgebra das mensagens. Este conjunto $sat(\Gamma)$ depende da definição de subtermos st, que pode variar de acordo com a teoria equacional, e também dos inversos $i_\oplus$ associado à cada símbolo associativo e comutativo $\oplus$ contido na assinatura.

Na sequência a expressão ***I**-localmente estável* é uma abreviação para *localmente estável com inversos.*

Definição 3.1 (**I**-Localmente Estável)**.** *Uma teoria equacional AC-convergente E que satisfaz a propriedade (*) é dita ser* I-localmente estável *se, para todo conjunto finito $\Gamma = \{M_1, \ldots, M_n\}$, onde os termos M_i são básicos e na forma normal, existe um conjunto finito e computável $sat(\Gamma)$ tal que*

1. *$\Gamma \subseteq sat(\Gamma)$, $e_\oplus \in sat(\Gamma)$ para cada $\oplus \in \Sigma_E$;*
2. *se $N_1, \ldots, N_k \in sat(\Gamma)$ e $f(N_1, \ldots, N_k) \in st_\oplus(sat(\Gamma))$ então $f(N_1, \ldots, N_k) \in sat(\Gamma)$, para $f \in \Sigma_E$;*
3. *se $C[S_1, \ldots, S_l] \xrightarrow{h} M$, onde C é um E-contexto normal tal que $|C| \leq c_E$, onde $S_1, \ldots, S_l \in sum_\oplus(sat(\Gamma))$, para algum $\oplus$, símbolo AC , então existe um E-contexto normal C', um termo M', uma função polinomial p e termos $S'_1, \ldots, S'_k \in sum_\oplus(sat(\Gamma))$, tais que $|C'| \leq p(c_E)$, e $M \xrightarrow{*}_{\mathcal{R} \cup AC} M' =_{AC} C'[S'_1, \ldots, S'_k]$;*
4. *se $M \in sat(\Gamma)$ então $i_\oplus(M) \downarrow \in sat(\Gamma)$ para cada $\oplus$, símbolo AC em Σ_E.*
5. *se $M \in sat(\Gamma)$ então $M \downarrow \in sat(\Gamma)$.*
6. *se $M \in sat(\Gamma)$ então $\Gamma \vdash M$.*

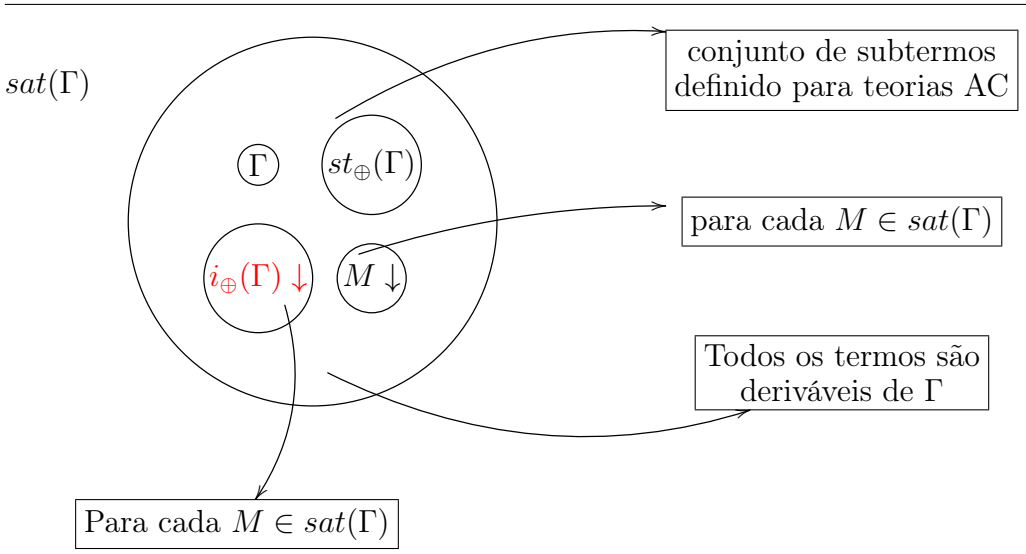


Figura 3.1: Conjunto $sat(\Gamma)$ para teorias **I**-localmente Estáveis

Na sequência provaremos que um caso restrito de AC-casamento de ordem superior ("existe um E-contexto normal C tal que $M =_{AC} C[M_1, \ldots, M_k]$ para $M_1, \ldots, M_k \in sat(\Gamma)$?") pode ser resolvido em tempo polinomial em $sat(\Gamma)|$ e $|M|$. Este problem de AC-casamento é resolvido utilizando o algoritmo CAC-OD (Casamento AC com Ocorrências Distintas) [9], onde cada variável no termo sendo emparelhado ocorre apenas uma vez. Em adição, também será utilizado um algoritmo padrão e de tempo polinomial para resolver sistemas lineares de equações Diofantinas sobre $\mathbb{Z}$ [13, 17, 27, 39].

Para facilitar a descrição do algoritmo abaixo será considerado apenas um símbolo associativo e comutativo $\oplus$ cujo inverso correspondente será denotado por i.

Lema 3.1. *Seja E um teoria **I**-localmente estável, $\Gamma = \{M_1, \ldots, M_n\}$ um conjunto finito de termos básicos na forma normal e M um termo básico na forma normal. Então a questão se existe um E-contexto normal C e $T_1, \ldots, T_k \in sat(\Gamma)$ tais que $M =_{AC} C[T_1, \ldots, T_k]$ é decidível em tempo polinomial em $|M|$ e $|sat(\Gamma)|$.*

Demonstração. Dado Γ, constrói-se o conjunto $sat(\Gamma) = \{T_1, \ldots, T_s\}$, que é finito e computável pela Definição 3.1 (**I**-localmente Estável). Pode-se verificar se $M =^{?}_{AC} C[T_1, \ldots, T_k]$ para algum E-contexto C e termos $T_1, \ldots, T_k \in sat(\Gamma)$ utilizando o Algoritmo 3.

O Algoritmo 3 abaixo procede da seguinte forma: Para todas as posições p em M encabeçadas por $\oplus$ iniciando pelas posições mais longas em ordem decrescente (posições vistas como sequências) resolva o *sistema linear de equações Diofantinas* (veja o procedimento A abaixo) para $M|_p$ com $sat(\Gamma) \cup S$, onde S é construído incrementalmente a partir de $sat(\Gamma)$, começando com $S = \emptyset$, incluindo todos $M|_p$ que possuirem soluções. Em outras palavras:

A)**Redução para equações Diofantinas lineares.** Primeiro, note que, para cada posição p tal que $M|_p$ é encabeçado com $\oplus$ temos

$$M|_p = \alpha_1 m_1 \oplus \ldots \oplus \alpha_r m_r \, , \, \alpha_j \in \mathbb{N} \tag{3.2}$$

Algoritmo 3 Algoritmo para busca de instâncias de SLDE

1: Seja $\mathcal{P}' = \{p_1, \ldots, p_t\}$ o conjunto de posições de M tais que $M|_p$ é encabeçado com $\oplus$, organizado em ordem decrescente. Para cada $p_j \in \mathcal{P}'$ seja $M|_{p_j}$ um subtermo de M tal que: $M|_{p_j} = n_{j_1} \oplus \ldots \oplus n_{j_{kj}}$ $(j = 1, \ldots, t)$.

2: Recursivamente busque, mas suprimindo passo 1 nesta chamada recursiva, soluções para os argumentos $n_{j_{i_1}}, \ldots, n_{j_{i_l}}$ de $M|_{p_j}$ com $n_{j_{im}} \in \{n_{j_1}, \ldots, n_{j_{k_j}}\}$ com respectivos E-contextos $C_{j_{i_1}}, \ldots, C_{j_{i_l}}$ tais que:

$$n_{j_{i_m}} = C_{j_{i_m}}[T_1, \ldots, T_{s_{i_m}}]$$

onde $T_q \in sat(\Gamma) \cup S$, $q = 1, \ldots, s_{i_m}$.

3: Então verifica-se a solvabilidade do Sistema Linear de Equações Diofantinas gerado a partir de $M|_{p_j}$ e $sat(\Gamma) \cup S \cup \{n_{j_{i_1}}, \ldots, n_{j_{i_{k_l}}}\}$ (veja os procedimentos A e B).

4: Se existir um solução então $S := S \cup \{M|_{p_j}\}$

5: Classifique os termos $sat(\Gamma) \cup S$ por tamanho.

6: Para cada termo $T_i \in sat(\Gamma) \cup S$ (de termos de tamanho maximal para termos de tamanho minimal) verifique:

7: Para cada posição $q \in \mathcal{P}os(M)$ tal que $T_i =_{AC} M|_q$, verifique se o caminho entre T_i e a raiz de M contém um $\oplus$:

- se NÃO, então delete $M|_q$ de M e mova para T_{i+1}.
- se SIM (existe um $\oplus$) então M tem um subtermo N tal que $N = n_1 \oplus \ldots \oplus n_j[T_i] \oplus \ldots \oplus n_k$ e N não pode ser construído a partir de $sat(\Gamma) \cup S$. Portanto, M não pode ser escrito como um E-contexto com termos de $sat(\Gamma)$.

8: Verifique se a parte remanescente de M ainda contém E-aliens. Se este não é o caso, um E-contexto C e termos $M_1, \ldots, M_k \in sat(\Gamma)$ foi encontrado, tal que $M =_{AC} C[M_1, \ldots, M_k]$; caso contrário, tal E-contexto não existe.

onde m_j não é encabeçado por $\oplus$ e $\alpha_j m_j$ conta para $\underbrace{m_j \oplus \ldots \oplus m_j}_{\alpha_j - times}$.

Queremos provar que existem $\beta_1, \ldots, \beta_q \in \mathbb{N}$ tais que

$$\beta_1 T_1 \oplus \ldots \oplus \beta_q T_q =_{AC} M|_p = \alpha_1 m_1 \oplus \ldots \oplus \alpha_r m_r \tag{3.3}$$

Esta AC-igualdade só é possível quando $T_i = \gamma_{1i} m_1 \oplus \ldots \oplus \gamma_{ri} m_r$ para cada i, $1 \leq i \leq q \leq s$, $T_i \in sat(\Gamma) \cup S$ e $\gamma_{j_i} \in \mathbb{N}$.

Isto é, $\beta_1 T_1 \oplus \ldots \oplus \beta_q T_q =_{AC} \alpha_1 m_1 \oplus \ldots \oplus \alpha_r m_r$ se e somente se

$$\begin{aligned}
&\beta_1(\gamma_{1_1} m_1 \oplus \ldots \oplus \gamma_{r_1} m_r) \oplus \\
&\beta_2(\gamma_{1_2} m_1 \oplus \ldots \oplus \gamma_{r_2} m_r) \oplus \\
&\qquad\qquad \vdots \\
&\oplus \beta_q(\gamma_{1_q} m_1 \oplus \ldots \oplus \gamma_{r_q} m_r) = \alpha_1 m_1 \oplus \ldots \oplus \alpha_r m_r
\end{aligned}$$

se, e somente se,

$$\begin{aligned}
&(\gamma_{1_1}\beta_1 \oplus \gamma_{1_2}\beta_2 \ldots \oplus \gamma_{1_q}\beta_q)m_1 \oplus \\
&(\gamma_{2_1}\beta_1 \oplus \gamma_{2_2}\beta_2 \ldots \oplus \gamma_{2_q}\beta_q)m_2 \oplus \\
&\qquad\qquad \vdots \\
&(\gamma_{r_1}\beta_1 \oplus \gamma_{r_2}\beta_2 \ldots \oplus \gamma_{r_q}\beta_q)m_r = \alpha_1 m_1 \oplus \ldots \oplus \alpha_r m_r
\end{aligned}$$

se, e somente se,

$$S = \begin{cases} \gamma_{1_1}\beta_1 \oplus \gamma_{1_2}\beta_2 \ldots \oplus \gamma_{1_q}\beta_q = \alpha_1 \\ \gamma_{2_1}\beta_1 \oplus \gamma_{2_2}\beta_2 \ldots \oplus \gamma_{2_q}\beta_q = \alpha_2 \\ \qquad\qquad \vdots \\ \gamma_{r_1}\beta_1 \oplus \gamma_{r_2}\beta_2 \ldots \oplus \gamma_{r_q}\beta_q = \alpha_r \end{cases} \tag{3.4}$$

onde S é um sistema de equações Diofantinas lineares sobre $\mathbb{Z}$ que pode ser resolvido em tempo polinomial [13, 17, 27, 39].

Observação 3.1. *As equações 3.2 e 3.3 serão interpretadas na aritmética dos inteiros. Se existir um índice j tal que $m_j = i(m'_j)$ e m'_j não é encabeçado por i então $\alpha_j m_j = \alpha_j(i(m'_j))$ e iremos tomá-lo por $(-\alpha_j)m'_j$. Portanto, pode-se tomar $\alpha_j \in \mathbb{Z}$, para todo j. Utilizando o mesmo raciocínio, conclui-se que $\beta_j \in \mathbb{Z}$, para todo $1 \leq j \leq q$ e $\gamma_{j_i} \in \mathbb{Z}$, para todo i e j.*

B) **Selecionando os $T'_j s$ a partir de $sat(\Gamma)$:**
Para cada $T_i \in sat(\Gamma)$, $1 \leq i \leq s$ queremos verificar se $T_i = \gamma_{1_i}m_1 \oplus \ldots \oplus \gamma_{r_i}m_r$.

Algoritmo 4 Algoritmo para selecionar termos de $sat(\Gamma)$

1: Para cada $T_i \in sat(\Gamma)$, $1 \leq i \leq s$, resolva a equação $T_i \oplus x_i =_{AC} \alpha_1 m_1 \oplus \ldots \oplus \alpha_r m_r$ onde x_i é uma variável nova.
2: Uma vez que os $T'_i s$ e M são termos básicos, esta equação pode ser vista como uma instância do problema do casamento CAC-OD, que pode ser resolvido em tempo $\mathcal{O}(|T_i \oplus x_i|.|M|_p|^3)$ [9].
3: Se existir $T_i \in sat(\Gamma)$ tal que $T_i = \gamma^*_{1_i}m_1 \oplus \ldots \oplus \gamma^*_{r_i}m_r \oplus u$, onde u não é vazio, $\gamma^*_{i_j} \in \mathbb{N}$ e o Algoritmo 3 não pode mais ser aplicado, então T_i não será selecionado.

Observe que cada passo do algoritmo pode ser executado em tempo polinomial em $|M|$ e $|sat(\Gamma)|$. Portanto, todo o procedimento é polinomial em $|M|$ e $sat(\Gamma)$. □

Observação 3.2. *Para a prova pode-se adotar uma ordem na qual, por exemplo variáveis são menores que constantes, constantes são menores do que símbolos de função, e símbolos de função também são ordenados, mas outras ordens podem ser utilizadas. Termos são comparados pela ordenação lexicográfica associada construída a partir dessa ordenação nos símbolos.*

Estes resultados dão origem à polinomialidade da decidibilidade da dedução para teorias I-localmente estáveis.

Teorema 3.1. *Seja E um teoria I-localmente estável. Se $\Gamma = \{M_1, \ldots, M_n\}$ é um conjunto de termos básicos e em forma normal e M é um termo básico e em forma normal, então $\Gamma \vdash M$ é decidível em tempo polinomial em $|M|$ e $|sat(\Gamma)|$.*

Demonstração. O resultado segue diretamente dos Lemas 3.1 e 2.4. □

Observação 3.3 (Complexidade da decidibilidade de teorias **N**-localmente estáveis)**.** *Um resultado similar ao Lema 3.1 pode ser enunciado para teorias **N**-localmente estáveis. A ausência de inversos faz com que o problema de resolver se $M =_{AC} C[T_1, \ldots, T_k]$ (para termos $T_1, \ldots, T_k \in sat(\Gamma)$ e um E-contexto C) seja transformável no problema de resolver sistemas de equações lineares Diofantinas sobre os naturais $\mathbb{N}$ que é um problema NP-completo. A NP-completude vem do fato de que decidir a satisfatibilidade de sistemas de equações lineares Diofantinas sobre $\mathbb{N}$ recai em uma restrição do* problema da programação inteira *para os naturais que é NP-completo [39]. Como consequência, segue o seguinte resultado de complexidade para teorias **N**-localmente estáveis, utilizando a indexação do capítulo anterior:*

Teorema 2.1 *A decidibilidade do* Problema da Dedução do Intruso *está em NP para teorias* **N***-localmente estáveis.*

3.2 Grupos Abelianos

Nesta seção, busca-se aplicar os resultados obtidos até agora na teoria equacional de grupos Abelianos. Abadi e Cortier, em [1] afirmam que esta teoria é *localmente estável*. Porém, a presença da função unária para *inverso* e a respectiva identidade que esta satisfaz $(*)$ faz com que esta teoria equacional esteja mais próxima de I-localmente estável. Alguns trabalhos sobre a decidibilidade da dedução do intruso para teoria de grupos Abelianos foram publicados, os trabalhos combinam raciocínio algébrico com técnicas de transformação de prova para o raciocínio dedutivo. Na sequência, analisa-se uma abordagem puramente algébrica do problema da dedução do intruso para a teoria de grupos Abelianos.

Gramática: Seja $\mathcal{N}$ um conjunto infinito enumerável de nomes. Seja $\Sigma_{AG} = \{+, 0, i\}$ uma assinatura tal que $+$ é uma símbolo de função associativo e comutativo, i é um símbolo de função unário chamado *inverso*, e 0 é uma constante, chamado *elemento neutro*.

Seja E_{AG} o conjunto das Σ_{AG}-equações representando a teoria dos Grupos Abelianos:

$$E_{AG} = \left\{ \begin{array}{rcl} x + (y + z) & = & (x + y) + z \\ x + y & = & y + x \\ i(x + y) & = & i(y) + i(x) \end{array} \right. \qquad \begin{array}{rcl} x + 0 & = & x \\ x + i(x) & = & 0 \end{array} \qquad \begin{array}{rcl} i(i(x)) & = & x \\ i(0) & = & 0 \end{array}$$

Sistema de Reescrita de Termos para *AG***:** Defina $\mathcal{R}_{AG}$ pela orientação das equações de E_{AG} da esquerda para direita (excluindo as equações para associatividade e comutatividade).

Lema 3.2. *O SRT $\mathcal{R}_{AG}$ é convergente módulo AC.*

Demonstração. A convergência módulo associatividade e comutatividade pode ser verificada utilizando CiME 2 [20]. □

O seguinte exemplo nos dá algumas ideias para a construção de $sat(\Gamma)$ dado um conjunto finito Γ de termos básicos na forma normal.

Exemplo 3.1. *Seja $\Gamma = \{a+2b+c+d, i(b)+m+n, 2i(c)+i(m)+g, i(n)+2d\}$ um conjunto de mensagens construído a partir de $\Sigma_{AG} \cup G$, onde G é o Grupo Abeliano considerado. Queremos construir o conjunto $sat(\Gamma)$ para Γ que satisfaça as condições da Definição 3.1. Entre outras propriedades, este conjunto $sat(\Gamma)$ tem que satisfazer a Condição 3. Seja $C[\_] := \_ + \_$ um E_{AG}-contexto e $S_1 = a + 2b + c + d, S_2 = i(b) + m + n, S_3 = 2i(c) + i(m) + g \in sum_+(sat(\Gamma), \tilde{n})$.*

$$C[S_1, S_2] = (a + 2b + c + d) + (i(b) + m + n) \xrightarrow{h} a + b + 0 + c + d + m + n = M$$

$$C[S_1, S_3] = (a + 2b + c + d) + (2i(c) + i(m) + g) \xrightarrow{h} a + 2b + d + 0 + i(c) + i(m) + g = N$$

ambas as reduções ocorrem via regra $x+i(x) \to 0$. A definição de $sat(\Gamma)$ tem que garantir que $M \xrightarrow{*} M' =_{AC} C'[S'_1, \ldots, S'_k]$ para $S'_1, \ldots, S'_k \in sum_+(sat(\Gamma), \tilde{n})$ e $N \xrightarrow{*} N' =_{AC} C''[S''_1, \ldots, S''_r]$ para $S''_1, \ldots, S''_r \in sum_+(sat(\Gamma), \tilde{n})$. Adicionar $M \downarrow$ e $N \downarrow$ em $sat(\Gamma)$ ajuda a contornar esta situação.

Definição 3.2 ($sat(\Gamma)$ para E_{AG})**.** *Dado um conjunto $\Gamma = \{M_1, \ldots, M_p\}$ de termos básicos e na forma normal, $sat(\Gamma)$ é o menor conjunto tal que:*

1. *$\Gamma \subseteq sat(\Gamma)$;*
2. *$N_1, \ldots, N_k \in sat(\Gamma)$ e $f(N_1, \ldots, N_k) \in st(sat(\Gamma))$ então $f(N_1, \ldots, N_k) \in sat(\Gamma)$, $f \in \Sigma_{AG}$;*
3. *se $N_i, N_j \in sat(\Gamma)$ e $N_i + N_j \xrightarrow{h} M$ via regra $x + i(x) \to 0$ então $M \downarrow \in sat(\Gamma)$;*
4. *se $N \in sat(\Gamma)$ então $i(N) \downarrow \in sat(\Gamma)$;*

Observação 3.4. *Na Definição 3.2 de $sat(\Gamma)$ para E_{AG} a regra 3 pode gerar um conjunto $sat(\Gamma)$ de tamanho infinito.*

Pode existir uma definição de $sat(\Gamma)$ para E_{AG} satisfazendo todas as exigências de teorias **I**-localmente estáveis. Quando a análise é restrita à Grupos Abelianos de ordem n é possível obter um conjunto finito $sat(\Gamma)$ adicionando algumas regras à Definição 3.2.

3.2.1 Grupos Abelianos de ordem n

Nesta seção será proposta uma teoria equacional para grupos Abelianos de ordem n, cujo sistema de reescrita de termos associado contém 4 regras que dependem da ordem do grupo. Este SRT é completo e foi obtido utilizando uma ferramenta de completamento *à la* Knuth-Bendix, disponível no sistema CiME 3 [21].

Considere a assinatura $\Sigma = \{+, i, 0\}$ para grupos Abelianos, onde $+$ é um símbolo de função binário AC que representa o operador do grupo, i é uma símbolo de função unária que pode ser identificado como a função *inverso* do grupo e 0 é um símbolo constante que pode ser interpretado como o *elemento neutro* do grupo. A teoria equacional E_n que será dada abaixo, faz uso dos axiomas de grupos Abelianos.

E_n: Teoria equacional da teoria de Grupos Abelianos de ordem n

$$E_n = \begin{cases} x + (y + z) = (x + y) + z & x + 0 = x \\ x + y = y + x & x + i(x) = 0 \\ i(x + y) = i(y) + i(x) & i(i(x)) = x \\ n \cdot x = 0 & i(0) = 0 \end{cases}$$

A expressão $n \cdot x$ representa $\underbrace{x + x + \ldots + x}_{n \text{ vezes}}$, para algum $n \in \mathbb{N}$.

$\mathcal{R}_n$: Sistema de Reescrita de Termos para E_n

Não foi encontrado na literatura um SRT para a teoria E_n. A partir dos axiomas de E_n, modela-se o SRT $\mathcal{R}_n$ da seguinte forma:

$$\mathcal{R}_n = \begin{cases} n \cdot x + y \to 0 + y \\ n \cdot x \to 0 \\ i(x) \to (n-1) \cdot x \\ 0 + x \to x \end{cases}$$

A regra $n \cdot x + y \to 0 + y$ é chamada de *regra de extensão*, uma vez que estende a regra $n \cdot x \to 0$, esta regra não é "necessária", mas foi gerada por CiME durante o processo de completamento. Intuitivamente esta regra é utilizada para que a aplicação de $n \cdot x \to 0$ ocorra na posição raiz do termo, dando *prioridade* a esta regra. Os termos que não são eliminados na instância $x\sigma$, ficam acumulados na instância $y\sigma$, para uma substituição σ.

Exemplo 3.2. *Considere a teoria equacional E_3 de grupos Abelianos de ordem 3. Seja $t = (a + b) + ((a + c) + a)$ um termo em um grupo $\mathcal{G}_3$ que é um modelo desta teoria. Tem-se que:*

$$t =_{AC} (a + a + a) + (b + c) = 3a + (b + c) \to_{n \cdot x \to 0} 0 + (b + c).$$

e a regra é aplicada na posiçao 1.

No entanto, se a regra $n \cdot x + y \to 0 + y$ for aplicada, a redução ocorre na posição raiz de $(a + a + a) + (b + c)$ e a parte que sobra é acumulada em y, i.e., $y\sigma = b + c$.

Proposição 3.1. *O sistema de reescrita de termos $\mathcal{R}_n$ é convergente módulo associatividade e comutatividade.*

Demonstração. Dado n, isto pode ser verificado utilizando CiME 3 [21], da seguinte forma:

Para provar a terminação módulo AC, utiliza-se a *ordem de caminhos lexicográficos* induzida sobre a ordenação $i > + > 0$ dos símbolos de Σ. O sistema (CiME 3) verifica que todos os pares críticos são juntáveis. Pelo *Teorema dos pares críticos de Knuth-Bendix* [7], tem-se que $\mathcal{R}_n$ é localmente confluente (módulo AC). Pelo *Lema de Newman* [7] segue que $\mathcal{R}_n$ é confluente (módulo AC) e, portanto, $\mathcal{R}_n$ é convergente módulo AC. □

A seguir, a menos que seja afirmado o contrário, os termos/mensagens são elementos da álgebra de termos $T(\Sigma \cup \mathcal{G} \cup \mathcal{N}, \emptyset)$, onde $\mathcal{G}$ é um grupo Abeliano de ordem n. O conjunto $\mathcal{N}$ representa nomes/constantes livres presentes nas mensagens, bem como termos E-aliens (Definição 1.35).

Para obter um conjunto $sat(\Gamma)$ adequado para a teoria de Grupos Abelianos de ordem n é necessário definir uma noção de subtermos específica:

Definição 3.3 (Subtermos Planos)**.** *Seja t um termo na forma normal. Defina $S(t)$ como o menor conjunto tal que*

- $t \in S(t)$*;*
- *se $i(u) \in S(t)$ então $u \in S(t)$;*
- *se $u_1 + u_2 + \ldots + u_n \in S(t)$ então $u_1, \ldots, u_n \in S(t)$.*

Esta noção de subtermos pode ser estendida para um conjunto T de termos básicos e na forma normal da forma usual: $S(T) := \bigcup_{t \in T} S(t)$.

A partir do conjunto dos subtermos planos de um determinado conjunto Γ de termos (que representa o conhecimento inicial de um intruso), define-se o conjunto das somas que podem ser geradas a p

Definição 3.4 ($SS_+(T)$)**.** *Seja T um conjunto de termos básicos e na forma normal, defina $SS_+(T)$ da seguinte forma,*

$$SS_+(T) := \left\{ (\sum_{s \in M} \alpha_s s) \downarrow | M \subseteq S(T), 1 \leq \alpha_s \leq n \right\}.$$

Lema 3.3. *$|SS_+(T)| \in \mathcal{O}(n^{|S(T)|})$, onde n é a ordem do grupo.*

Demonstração. Primeiramente, observe que existem $2^{|S(T)|}$ possíveis subconjuntos M de $S(T)$. Seja N o maior desses subconjuntos, isto é, $N = \{m_1, \ldots, m_r\}$ tais que $m_i \in S(T)$, para $1 \leq i \leq r$. Dessa forma, no máximo $n^{|N|} \leq n^{|S(T)|}$ possíveis termos são adicionados em $SS_+(T)$:

$$(\alpha_1 \cdot m_1 + \alpha_2 \cdot m_2 + \ldots + \alpha_r \cdot m_r) \downarrow \in SS_+(T)$$

onde $1 \leq \alpha_i \leq n$, para $1 \leq i \leq r$. Como existem $2^{|S(T)|}$ possíveis subtermos, tem-se que no máximo $\leq 2^{|S(T)|}n^{|S(T)|} = (2n)^{|S(T)|}$ são adicionados em $SS_+(T)$. Logo, $|SS_+(T)| \in \mathcal{O}(n^{|S(T)|})$, onde n é a ordem do grupo. □

Definição 3.5 ($sat(\Gamma)$ para E_n)**.** *Dado um conjunto $\Gamma = \{M_1, \ldots, M_p\}$ de termos básicos e na forma normal, $sat(\Gamma)$ é o menor conjunto gerado pelas regras*

1. $\Gamma \subseteq sat(\Gamma)$*;*
2. $N_1, \ldots, N_k \in sat(\Gamma)$ *e* $f(N_1, \ldots, N_k) \in SS_+(sat(\Gamma))$ *então* $f(N_1, \ldots, N_k) \in sat(\Gamma)$*,* $f \in \Sigma_{AG}$*;*
3. *se* $N \in sat(\Gamma)$ *então* $i(N)\downarrow \in sat(\Gamma)$*;*
4. *se* $N_1, \ldots, N_k \in sat(\Gamma)$ *tal que* $N_1 + \ldots + N_k \xrightarrow{h} M$ *via regra* $n \cdot x + y \to 0 + y$ *então* $M\downarrow \in sat(\Gamma)$ *(*$1 < k \leq n$ *).*

Proposição 3.2. *O tamanho de $sat(\Gamma)$ para E_n é exponencial em $|\Gamma|$.*

Demonstração. Seja $\Gamma = \{M_1, M_2, \ldots, M_s\}$ um conjunto de termos básicos e na forma normal e considere o Algoritmo 5 a seguir, para construir o conjunto $sat(\Gamma)$:

Algoritmo 5 Construção de $sat(\Gamma)$ para E_n

INPUT $\Gamma = \{M_1, \ldots, M_p\}$, $sat(\Gamma) = \emptyset$, $i := 0$
$sat_i(\Gamma) \leftarrow \Gamma$
repeat
    if $N_1, \ldots, N_k \in sat_i(\Gamma)$ and $f(N_1, \ldots, N_k) \in SS_+(sat_i(\Gamma))$ **then** $f(N_1, \ldots, N_k) \in Temp$
    end if
    for all $N \in sat_i(\Gamma)$ **do** $Temp \cup \{i(N)\downarrow\}$
    end for
    for $1 < k \leq n$ **do**
        if $N_1 \ldots N_k \in sat_i(\Gamma)$ and $N_1 + \ldots + N_k \xrightarrow{h} M$ via rule $r_1 : n \cdot x + y \to 0 + y$ **then** $Temp \cup \{M\downarrow\}$
        end if
    end for
    $sat_{i+1}(\Gamma) \leftarrow sat_i(\Gamma) \cup Temp$
    $i \leftarrow i + 1$
until $sat_{i-1}(\Gamma) = sat_i(\Gamma)$
$sat(\Gamma) \leftarrow sat_i(\Gamma)$
return $sat(\Gamma)$

O objetivo é provar que $sat(\Gamma)$ é finito e exponencial em $|\Gamma|$. Para isto, mostra-se que todo termo em $sat(\Gamma)$ é um elemento de $SS_+(\Gamma)$. Pelo Lema 3.3, $|SS_+(\Gamma)|$ é exponencial em $|S(\Gamma)|$, que por sua vez é linear em $|\Gamma|$.

A prova é por indução em i, que é a iteração da construção de $sat(\Gamma)$.

Base da Indução. Suponha que $i = 1$.

Seja $M \in sat_1(\Gamma)$, então M foi obtido de uma das seguintes formas:

- $M \in sat_0(\Gamma) = \Gamma$, e o resultado segue trivialmente.
- M foi obtido via passo 4 do algoritmo. Isto é, existem $M_1, \ldots, M_k \in sat_0(\Gamma)$ tal que $N = f(M_1, \ldots, M_k) \in SS_+(\Gamma)$, para $f \in \Sigma_{AG} = \{+, i, 0\}$ e o resultado segue trivialmente.
- M foi obtido via Passo 6 do algoritmo, isto é, existe $M_j \in sat_0(\Gamma)$ e $M = i(M_j)\downarrow$. Então, $M = (n-1)M_j$ com $M_j \in \Gamma \subset SS_+(\Gamma)$, e o resultado segue.
- M foi obtido via Passo 8 do algoritmo, isto é, existem $M_1, \ldots, M_k \in \Gamma$ tais que $M_1 + \ldots + M_k \xrightarrow{h} N$ via regra r_1 e $M = N\downarrow = (M_1 + \ldots + M_k)\downarrow$ e o resultado segue da definição de SS_+.

Passo indutivo. Seja $M \in sat_i(\Gamma)$, $(i > 1)$, então M foi obtido de uma das seguintes formas:

1. M foi obtido via Passo 4 do Algoritmo 2:

   Então existem $M_1, \ldots, M_k \in sat_{i-1}(\Gamma)$ tal que $f(M_1, \ldots, M_k) \in SS_+(sat_{i-1}(\Gamma))$ e $M = f(M_1, \ldots, M_k)$, $f \in \Sigma_{AG} = \{+, i, 0\}$.

   - Se $f = i$ então $k = 1$ e temos $i(M_1) \in SS_+(\Gamma)$. Isto é uma contradição, pois $SS_+(sat_{i-1}(\Gamma))$ só contém formas normais e $i(M_1)$ é um termo redutível.
   - Se $f = +$ então $M = M_1 + \ldots + M_k$.

     Por IH, cada $M_i = \alpha_{i_1} N_{i_1} + \ldots \alpha_{i_s} N_{i_{s_i}} \in SS_+(\Gamma)$, onde $N_{i_j} \in SS_+(\Gamma)$ para $1 \leq i \leq k$ e $1 \leq j \leq s_j$ e segue o resultado.

2. M foi obtido via Passo 6 do Algoritmo 2. Então $M = i(N)\downarrow \in sat_i(\Gamma)$ para algum $N \in sat_{i-1}(\Gamma)$. Por IH, $N = (\alpha_1 M_1 + \ldots + \alpha_r M_r)\downarrow$ onde $M_1, \ldots, M_r \in SS_+(\Gamma)$. Observe que

$$\begin{aligned} i(N)\downarrow &\xrightarrow{h} (n-1)(\alpha_1 M_1 + \ldots + \alpha_r M_r)\downarrow \\ &=_{AC} ((n-1)(\alpha_1)M_1 + \ldots + (n-1)(\alpha_r)M_r)\downarrow \\ &=_{AC} (\beta_1 M_1 + \ldots + \beta_r M_r)\downarrow \end{aligned}$$

   e o resultado segue.

3. M é obtido via passo 8 do Algoritmo. Então existem $M_1, \ldots, M_k \in sat_{i-1}(\Gamma)$ tais que $M_1 + \ldots + M_k \xrightarrow{h} N$ via regra r_1 e $M = N\downarrow$. Por IH, cada $M_j \in sat_{i-1}(\Gamma)$ é tal que $M_j = \alpha_{j_1} M_{j_1} + \ldots + \alpha_{j_s} M_{j_{s_j}}$. Observe que

$$\begin{aligned} M &= (M_1 + \ldots + M_k)\downarrow \\ &=_{AC} ((\alpha_{1_1} M_{1_1} + \ldots + \alpha_{1_s} M_{1_{s_1}})\downarrow + \ldots + (\alpha_{k_1} M_{k_1} + \ldots + \alpha_{k_s} M_{k_{s_k}})\downarrow)\downarrow \\ &=_{AC} ((\alpha_{1_1} M_{1_1} + \ldots + \alpha_{1_s} M_{1_{s_1}}) + \ldots + (\alpha_{k_1} M_{k_1} + \ldots + \alpha_{k_s} M_{k_{s_k}}))\downarrow \\ &=_{AC} (\beta_1 M'_1 + \ldots + \beta_t M'_t)\downarrow \end{aligned}$$

para $M'_1, \ldots, M'_t \in SS_+(\Gamma)$ e $\beta_1, \ldots, \beta_t \in \mathbb{N}$, depois de reorganizar os termos repetidos.

Suponha que $SS_+(\Gamma) = \{M_1, \ldots, M_q\}$. onde $0 \leq \alpha_j \leq n$, $1 \leq j \leq q$ Observe que, no máximo, $(\alpha_1 M_1 + \ldots + \alpha_q M_q) \downarrow$ serão adicionados em $sat(\Gamma)$. Existem n^q possíveis combinações de termos diferentes que podem ser adicionados em $sat(\Gamma)$. Pelo Lema 3.3, $|SS_+(\Gamma)| = q$ é exponencial em $|atomos(\Gamma)|$ que por sua vez é linear em $|\Gamma|$. □

Proposição 3.3. *O conjunto $sat(\Gamma)$ definido para a teoria E_n satisfaz a Condição 3 da Definição 3.1 de **I**-local estabilidade.*

Demonstração. Por indução na estrutura do E_n-contexto, prova-se que:

"se $C[S_1, \ldots, S_l] \xrightarrow{h} M$, onde C é um E_n-contexto normal tal que $|C| \leq c_{E_n}$, e onde $S_1, \ldots, S_l \in sum_+(sat(\Gamma), \tilde{n})$, para $+$ um símbolol AC então existe um E_n-contexto C', um termo M', e termos $S'_1, \ldots, S'_k \in sum_+(sat(\Gamma), \tilde{n})$, tais que $|C'| \leq c_{E_n}$, e $M \xrightarrow{*}_{\mathcal{R} \cup AC} M' =_{AC} C'[S'_1, \ldots, S'_k]$"

Base da Indução. $C[\_] = \_$ é o E_n-contexto vazio.

Segue que $l = 1$ e $C[S_1] = S_1 \xrightarrow{h} M$ onde $S_1 \in sum_+(sat(\Gamma))$, isto é,

$$S_1 = \alpha_1 T_1 + \ldots + \alpha_n T_n + \underbrace{\sum_{j=1}^{r} \beta_j n_j}_{A}, \tag{3.5}$$

para $\alpha_i, \beta_j \in \mathbb{N}^*$, $T_i \in sat(\Gamma)$ e $n_j \notin \tilde{n}$ ($1 \leq i \leq n$ e $1 \leq j \leq r$).

A prova segue pela análise da regra de reescrita de $\mathcal{R}_n$ aplicada em (3.5). Observe que, neste caso, a regra $i(x) \to (n-1)x$ só poderia ser aplicada em algum $T_i \in sat(\Gamma)$, mas por hipótese, os termos de $sat(\Gamma)$ estão na forma normal. Dessa forma, é necessário analisar apenas as aplicações em S_1 das seguintes regras:

1. A regra é $nx + y \to 0 + y$;

   Suponha que existam índices $j_1, j_2, \ldots, j_r \in \{1, \ldots, n\}$ tais que

   $$T_{j_k} = \beta_{j_k} T + u_{j_k} (u_{j_k} \text{ possivelmente vazio.}) \tag{3.6}$$

   para algum termo T, $1 \leq k \leq r$, $1 \leq \beta_{j_k} < n$ e $\beta_{j_1} + \beta_{j_2} + \ldots + \beta_{j_r} = n$.

   Suponha que $\{1, \ldots, n\} - \{j_1, j_2, \ldots, j_r\} = \{a_1, \ldots, a_t\}$. Pode-se reorganizar os

termos de S_1 da seguinte forma:

$$\begin{aligned}
S_1 &= \alpha_1 T_1 + \ldots + \alpha_n T_n + A \\
&=_{AC} \alpha_{j_1} T_{j_1} + \ldots + \alpha_{j_r} T_{j_r} + \underbrace{(\alpha_{a_1} T_{a_1} + \ldots + \alpha_{a_t} T_{a_t})}_{S} + A \\
&=_{AC} (T_{j_1} + \ldots + T_{j_r}) + \sum_{i=1}^{r} (\alpha_{j_i} - 1) T_{j_i} + S + A \\
&=_{AC} (\beta_{j_1} T + u_{j_1} + \ldots + \beta_{j_r} T + u_{j_r}) + \sum_{i=1}^{r} (\alpha_{j_i} - 1) T_{j_i} + S + A \\
&\xrightarrow{h} 0 + (u_{j_1} + \ldots + u_{j_r}) + \sum_{i=1}^{r} (\alpha_{j_i} - 1) T_{j_i} + S + A = M
\end{aligned}$$

Observe que

$$M \xrightarrow{*} (m u_{j_1} + \ldots + m u_{j_r}) \downarrow + \sum_{i=1}^{r} (\alpha_{j_i} - m) T_{j_i} + S + A = M' \tag{3.7}$$

onde $m = min(\alpha_{j_1}, \alpha_{j_2}, \ldots, \alpha_{j_r})$.

Como $T_{j_1}, \ldots, T_{j_r} \in sat(\Gamma)$ e das identidades em (3.6) tem-se que

$$T_{j_1} + \ldots + T_{j_r} \xrightarrow{h} 0 + (u_{j_1} + \ldots + u_{j_r})$$

via aplicacão da regra $nx + y \to 0 + y$. Pelo item 4 da Definição 3.5, segue que $\mathbf{T} = (u_{j_1} + \ldots + u_{j_r}) \downarrow \in sat(\Gamma)$.

Finalmente, de (3.7) tem-se que $M' =_{AC} m\mathbf{T} + \sum_{i=1}^{r} (\alpha_{j_i} - m) T_{j_i} + S + A =_{AC} S' \in sum_+(sat(\Gamma), \tilde{n})$, e o resultado segue para um E_n-contexto vazio.

2. A regra é $nx \to 0$.

   Este resultado é similar ao caso anterior quando u_{j_k} é vazio em (3.6) para todo k, $1 \leq k \leq r$.

3. A regra é $x + 0 \to x$;

   Suponha que $T_i = 0$ para algum índice i em (3.5). O resultado segue diretamente.

Passo Indutivo: Temos que analisar E_n-contextos normais C tais que $1 \leq |C| \leq c_{E_n}$.

Primeiro, observe que E_n-contextos normais não podem ser encabeçados por i. Ou seja, E_n-contextos normais devem ser formados exclusivamente por somas:

$$C[S_1, \ldots, S_k] = S_1 + \ldots + S_k \tag{3.8}$$

onde $S1, \ldots, S_k \in sum_+(sat(\Gamma), \tilde{n})$. Reorganizando os termos repetidos de $sat(\Gamma)$ em (3.8), obtém-se que

$$C[S_1, \ldots, S_k] = S_1 + \ldots + S_k =_{AC} S' \in sum_+(sat(\Gamma), \tilde{n})$$

e o resultado segue pela Base da Indução.

□

Proposição 3.4. *A teoria E_n de Grupos Abelianos de ordem n é I-localmente estável.*

Demonstração. Os casos 1, 2, 4 e 5 da Definição 3.1 são satisfeitos imediatamente pela Definição 3.5. Pela Proposição 3.2 o conjunto $sat(\Gamma)$ gerado é finito. Pela Proposição 3.3 a condição 3 da Definição 3.1 é satisfeita. A condição 6 é satisfeita pois os termos de $sat(\Gamma)$ são obtidos via uma das três regras do Sistema $\mathcal{N}$ (Tabela 2.1). □

Lema 3.4. *Seja E_n a teoria equacional de grupos Abelianos de ordem n, $\Gamma = \{M_1, \ldots, M_n\}$ um conjunto finito de termos básicos e em forma normal e M um termo básico e em forma normal. Então a questão se existe um E_n-contexto normal C e $T_1, \ldots, T_k \in sat(\Gamma)$ tais que $M =_{AC} C[T_1, \ldots, T_k]$ é decidível em tempo polinomial em $|M|$ e $|sat(\Gamma)|$.*

Demonstração. Pela Proposição 3.4, tem-se que E_n é uma teoria **I**-localmente estável, portanto, pelo Lema 3.1 segue o resultado. □

Teorema 3.2. *Seja $\Gamma = \{M_1, \ldots, M_k\}$ um conjunto finito de termos básicos e na forma normal e M um termo básico e na forma normal. O problema da dedução do intruso para E_n é decidível em tempo polinomial em $|M|$ e $|sat(\Gamma)|$.*

Demonstração. Como E_n é uma teoria **I**-localmente estável, o resultado segue pelo Teorema 3.1. □

3.3 Teoria AC-"pura"

Na sequência mostraremos que a complexidade de decidir IDP para teoria AC-"pura" está em NP, concordando com resultados prévios [30].

Considere a assinatura Σ_{AC} que contém apenas símbolos constantes, o símbolo associativo-comutativo $\oplus$ e a teoria equacional E_{AC} contém apenas as equações AC para $\oplus$:

$$E_{AC} = \left\{ \; x \oplus y = y \oplus x \qquad\qquad x \oplus (y \oplus z) = (x \oplus y) \oplus z \; \right\}$$

Neste caso, $\mathcal{R} = \emptyset$ é o SRT convergente módulo AC associado a E_{AC}.

Como no caso de grupos Abelianos, será necessário definir uma noção de subtermos planos adequada para a teoria equacional E_{AC}. A noção de subtermos abaixo considera todas as possibilidades de combinação dos termos módulo associatividade e comutatividade de $\oplus$.

Definição 3.6. *Seja t um termo básico e na forma normal. Defina $St_{AC}(t)$ da seguinte forma:*

1. *$t \in St_{AC}(t)$;*
2. *se $u \in St_{AC}(t)$ e $u =_{AC} v$ então $v \in St_{AC}(t)$.*

Esta noção de subtermos pode ser estendida para um conjunto T de termos básicos e na forma normal da forma usual: $S_{AC}(T) := \bigcup_{t \in T} S_{AC}(t)$.

Definição 3.7. *Seja* $\Gamma = \{M_1, \ldots, M_k\}$ *um conjunto finito de termos básicos na forma normal. Define-se* $sat(\Gamma)$ *para a teoria AC como o menor conjunto tal que*

1. $\Gamma \subseteq sat(\Gamma)$;
2. *se* $N_i, N_j \in sat(\Gamma)$ *e* $N_i \oplus N_j \in St_{AC}(sat(\Gamma))$ *então* $N_i \oplus N_j \in sat(\Gamma)$.

O conjunto $sat(\Gamma)$ é finito uma vez que adicionamos apenas termos cujo tamanho é menor ou igual ao tamanho maximal dos termos em Γ. É fácil ver que o conjunto $sat(\Gamma)$ satisfaz as regras 1,2, e 5 da Definição 2.2, da classe de teorias **N**-localmente estáveis. Uma vez que $\mathcal{R} = \emptyset$ segue que a regra 3 e 4 também são satisfeitas. Portanto, AC é **N**-localmente estável. Logo,

Lema 3.5. E_{AC} *é* ***N****-localmente estável.*

Utilizando o algoritmo proposto no Lema 3.1 tem-se que teorias **N**-localmente estáveis são decidíveis em tempo polinomial não determinístico:

Teorema 3.3. *O Problema da Dedução do Intruso para teorias AC puras está em NP.*

Demonstração. A assinatura da teoria equacional não contém inversos mas o procedimento apresentado no Lema 3.1 pode ser utilizado similarmente, entretanto, tem-se que resolver um sistema de equações lineares Diofantinas S nos naturais $\mathbb{N}$, que é um problema NP-completo [39]. □

O problema de decidir se um sistema não-homogêneo de equações lineares Diofantinas cujos coeficientes tem uma solução em naturais é NP-completo. Este problema é um caso especial de *Problema de Programação Inteira Linear* onde todos os coeficientes a_i, c_i, b, B são inteiros não-negativos, $b = B$ e $a_i = c_i$, $\forall i, 1 \leq i \leq n$:

INSTÂNCIA: Um conjunto finito A de pares $(\overline{a}, b)$, onde $\overline{a} = (a_1, \ldots, a_n)$ é uma n-tupla de inteiros e b é um inteiro, uma n-tupla $\overline{c} = (c_1, \ldots, c_n)$ de inteiros, e um inteiro B.

QUESTÃO: Existe uma n-tupla $\overline{x} = (x_1, \ldots, x_n)$ de inteiros tais que $a_1x_1 + \ldots + a_nx_n \leq b$ para todo $(\overline{a}, b) \in A$ e tal que $c_1x_1 + \ldots + c_nx_n \geq B$?

Este problema é NP-completo [28]. No entanto, existem esforços para desenvolver procedimentos eficientes para encontrar soluções positivas para sistemas de equações lineares Diofantinas. Quando $\Sigma = \{+\}$, isto é, quando a assinatura é reduzida para um símbolo associativo-comutativo, ou possivelmente um símbolo AC mais constantes livres, o problema reduz para combinar soluções positivas minimais de equações Diofantinas lineares [13]. Existem dois métodos conhecidos, um por Huet [29] e outro por Clausen e Fortenbacher [17]. Uma extensão do método de Fortenbacher para resolver diretamente sistemas de equações Diofantinas lineares é apresentado em [13].

Capítulo 4

Problema da Dedução Elementar

Neste capítulo, o objetivo é relacionar a classe de teorias **N**-localmente estáveis e **I**-localmente estáveis com a decidibilidade do *problema da dedução elementar*(PDE) introduzido por A. Tiu, R. Goré e J.Dawson em [41]. Neste trabalho os autores introduzem o *problema da dedução elementar* que é uma versão do problema da dedução do intruso restrito à análise algébrica induzida pela teoria equacional em questão. Apesar de terem desenvolvido um metodologia para tratar este problema, os autores não disponibilizaram nenhuma classe de teorias para as quais o PDE é decidível.

Baseados nos resultados obtidos nos capítulos 2 e 3, tem-se que o a decidibilidade do PDE está em NP para teorias **N**-localmente estáveis e em P para teorias **I**-localmente estáveis. Mais ainda, uma extensão pode ser feita, uma vez que o resultado vale para uma união disjunta de teorias equacionais AC convergentes, onde cada uma possui um símbolo de função AC.

O trabalho [41] baseia-se no fato de que o problema da dedução do intruso é, em geral, formulado via sistemas do tipo dedução natural, e checar a decidibilidade requer um esforço significativo em mostrar que as regras dedutivas são "locais" no sentido introduzido por David McAllester em [33]. Propõe-se, então, utilizando uma tradução tradicional entre sistemas de dedução natural e o cálculo de sequentes, reformular o problema da dedução do intruso como uma busca por prova em um cálculo de sequentes, no qual a localidade é imediata.

Utilizando métodos teóricos básicos, como a permutabilidade de regras e a eliminação de corte, pode-se mostrar que o *problema da dedução do intruso* pode ser reduzido, em tempo polinomial, para o *problema da dedução elementar*, que recai em resolver certas equações que dependem da teoria equacional imersa no protocolo criptográfico em questão.

O trabalho é inicialmente proposto para o estudo do PDI sob a teoria de *assinaturas cegas* e teorias equacionais AC-convergentes arbitrárias. Em [41], prova-se que PDI reduz polinomialmente para PDE, porém a decidibilidade do problema da dedução elementar não é estudada. Como poderá ser visto, estudar a decidibilidade do PDE recai em decidir problemas de unificação de ordem superior módulo uma teoria equacional E. Neste capítulo, será mostrado que tal problema é decidível para as classes de teorias **N**- e **I**-localmente estáveis, que foram introduzidas nos Capítulos 2 e 3.

Este capítulo contém uma seção de preliminares independente, que é necessária para a compreensão dos assuntos tratados aqui. Partes deste capítulo foram publicadas em [6]. As demonstrações referentes aos resultados propostos por A. Tiu, R. Goré e J.Dawson serão apenas enunciados no decorrer do capítulo, para mais detalhes, veja [6, 37, 41].

4.1 Preliminares

Esta seção concentra-se em alguns conceitos básicos de criptografia e algumas noções de termos/subtermos e sistemas dedutivos que serão utilizadas no capítulo. As noções de criptografia são, mais especificamente, aquelas relacionados com *assinaturas digitais*, para mais detalhes, veja [34]. Já as noções de termos e regras dedutivas, foram introduzidas por A. Tiu, R. Goré e J. Dawson em [41].

4.1.1 Assinaturas Cegas

Assinatura cega é uma primitiva criptográfica básica em *e-cash*. Este conceito foi introduzido por David Chaum em [15] para permitir que um banco (ou qualquer um) possa assinar mensagens sem vê-las. A ideia de David Chaum era usar essa propriedade homomórfica de tal forma que Alice possa multiplicar a mensagem original por um fator aleatório (cifrado) que fará a imagem resultante sem significado algum para o Banco. Se o Banco concorda em assinar esta informação com aparência aleatória e enviá-la de volta para Alice, ela será capaz de recuperar a mensagem original com a assinatura do Banco. Formalmente,

Definição 4.1 (Assinatura Digital)**.** *Definições básicas:*

- *Uma* assinatura digital *é uma* string *de dados que associa uma mensagem (na forma digital) com alguma entidade de origem.*
- *Um* algoritmo de geração de assinatura digital *é um método para produzir uma assinatura digital.*
- *Um* algoritmo de verificação de assinatura digital *é um método para verificar que uma assinatura digital é autêntica (isto é, foi de fato criada pela entidade específica).*
- *Um* esquema de assinatura digital *consiste de um algoritmo de geração de assinatura e um algoritmo de verificação associado.*
- *Um* processo de assinatura digital *consiste de um algoritmo (matemático) de geração de asssinatura digital, juntamente com um método para formatar os dados em mensagens que possam ser assinadas.*
- *Um* processo de verificação de assinatura digital *consiste de um algoritmo de verificação, juntamente com um método para recuperar dados a partir da mensagem.*

Esquemas de assinaturas cegas são protocolos de duas partes entre um *remetente* A e um *assinante* B. A ideia é a seguinte: A envia um pedaço de informação para B que B assina e retorna para A. Desta assinatura, A pode calcular a assinatura de B em uma mensagem inicial m da escolha de A. Ao completar o protocolo, B não conhece nem a mensagem m e nem a assinatura associada a ela.

O objetivo de uma assinatura cega é prevenir que um assinante B observe a mensagem que ele assina e a assinatura; portanto, ele é incapaz de associar a mensagem assinada com o remetente A.

Exemplo 4.1 (Aplicações de Assinaturas Cegas)**.** *Esquemas de assinaturas cegas tem aplicações onde o remetente A (o cliente) não quer que o assinante B (o banco) seja capaz de associar posteriormente, uma mensagem m e uma assinatura* $S_B(m)$ *a uma instância específica do protocolo. Isto pode ser importante em aplicações de dinheiro eletrônico onde uma mensagem m pode representar um valor monetário que A pretende gastar. Quando m e* $S_B(m)$ *são apresentados a B para pagamento, B é incapaz de deduzir para que parte o valor assinado foi dado originalmente. Isto permite que A permaneça anônimo e desta forma, padrões de gastos não podem ser monitorados.*

Um protocolo de assinatura cega requer os seguintes componentes:

1. Um mecanismo de assinatura digital para o assinante B. $S_B(x)$ denota a assinatura de B em x.

2. Funções f e g (conhecidas apenas pelo remetente) tais que $g(S_B(f(m))) = S_B(m)$. A função f é chamada de *função de cegamento/ocultação (blinding)*, e g é uma *função de desocultação (unblinding)*, e $f(m)$ é uma *mensagem oculta.*

Sintaxe estendida

Dada uma teoria equacional I-localmente estável E, estende-se a assinatura Σ_E com Σ_C, um conjunto contendo símbolos de função para "construtores" de assinaturas cegas, afim de obter resultados de decidibilidade para a extensão do problema da dedução do intruso para o sistema $\mathcal{N}$ (Tabela 2.1) levando em conta algumas regras para assinaturas cegas.

A assinatura Σ consiste de símbolos de função e é definida pela união de dois conjuntos: $\Sigma = \Sigma_E \cup \Sigma_C$ (com $\Sigma_{\mathsf{E}} \cap \Sigma_C = \emptyset$), onde

$$\Sigma_C = \left\{ \mathsf{pub}(\_), \mathsf{sign}(\_\ ,\_), \mathsf{blind}(\_\ ,\_), \{\_\}_\_ , \langle \_, \_ \rangle \right\}$$

representam os *construtores*, cujas interpretações são:

- $\mathsf{pub}(M)$ dá a chave pública gerada a partir de uma chave privada M;
- $\mathsf{blind}(M, N)$ denota M cifrado com N usando uma encriptação para cegamento;
- $\mathsf{sign}(M, N)$ denota M assinado com uma chave privada N;

- $\{M\}_N$ denota M encriptado com uma chave N utilizando a encriptação simétrica de Dolev-Yao;
- $\langle M, N\rangle$ constrói um par de termos a partir de M e N.

Então a gramática estendida do conjunto de *termos* ou mensagens é dada por

$$M, N \ := a \mid x \mid f(M_1, \ldots, M_n) \mid \mathsf{pub}(M) \mid \mathsf{sign}(M, N) \mid \mathsf{blind}(M, N) \mid \{M\}_N \mid \langle M, N\rangle$$

Definição 4.2 ([41]). *Seja E uma teoria equacional e M um termo em $T(\Sigma_C \cup \Sigma_E, X)$:*

- *M é chamado de E-*alien *quando for encabeçado com $f \in \Sigma_C$ ou M é um nome privado.*
- *M é chamado E-*puro *se ele contém apenas símbolos de Σ_E, nomes e variáveis.*
- *Um subtermo E-alien M de N é dito ser um E-*fator *de N se existe outro subtermo F de N tal que M é um subtermo imediato de F e F é encabeçado por um símbolo $f \in \Sigma_E$*

4.2 Capacidade Dedutiva do Intruso

Dado um conjunto Γ que representa a informação disponível para um intruso, pode-se perguntar se um dado termo básico M pode ser deduzido de Γ utilizando raciocínio equacional baseado na álgebra imersa nas primitivas criptográficas, representada pela teoria equacional E, estendida com a álgebra presente na teoria de assinaturas cegas. Esta relação é representada por $\Gamma \vdash M$ e axiomatizada através do sistema de regras de inferência do tipo dedução natural (Tabela 4.1) introduzido por A.Tiu, R.Goré e J. Dawson em [41] que estende o Sistema $\mathcal{N}$, na Tabela 2.1.

Sistema de Dedução Natural

A técnica comumente utilizada para o estudo da decidibilidade do problema da dedução do intruso consiste em provar que tal sistema de regras tem a propriedade de localidade, introduzida por D.McAllester em [33]. Isto é, seria necessário definir uma noção de subtermos $St(\Gamma)$ adequada para o qual toda prova de $\Gamma \vdash M$ em $\mathcal{N}'$ é tal que todos os nós são rotulados por subtermos de $St(\Gamma \cup \{M\})$. Uma vez que a propriedade de localidade é indecidível [33], os autores propõem uma alternativa metodológica via a tradução para o cálculo de sequentes dado a seguir.

Cálculo de Sequentes para o Intruso

Um sequente $\Gamma \vdash M$ está na forma normal se M e todos os termos em Γ estão na forma normal. A menos que seja afirmado o contrário, assume-se que os sequentes estão na

$$\frac{M \in \Gamma}{\Gamma \vdash M}\,(id) \qquad \frac{\Gamma \vdash \{M\}_K \qquad \Gamma, M \vdash K}{\Gamma \vdash M}\,(e_E) \qquad \frac{\Gamma \vdash M \qquad \Gamma, M \vdash K}{\Gamma \vdash \{M\}_K}\,(e_I)$$

$$\frac{\Gamma \vdash \langle M, N\rangle}{\Gamma \vdash M}\,(p_E) \qquad \frac{\Gamma \vdash \langle M, N\rangle}{\Gamma \vdash N}\,(p_E) \qquad \frac{\Gamma \vdash M \qquad \Gamma \vdash N}{\Gamma \vdash \langle M, N\rangle}\,(p_I)$$

$$\frac{\Gamma \vdash M \qquad \Gamma \vdash K}{\Gamma \vdash \{M\}_K}\,(e_R) \qquad \frac{\Gamma, \{M\}_K \vdash K \qquad \Gamma, \{M\}_K, M, K \vdash N}{\Gamma, \{M\}_K \vdash N}\,(e_L)$$

$$\frac{\Gamma \vdash \mathsf{sign}(M, K) \qquad \Gamma \vdash \mathsf{pub}(K)}{\Gamma \vdash M}\,(\mathsf{sign}_E) \qquad \frac{\Gamma \vdash M \qquad \Gamma \vdash K}{\Gamma \vdash \mathsf{sign}(M, K)}\,(\mathsf{sign}_I)$$

$$\frac{\Gamma \vdash \mathsf{blind}(M, K) \qquad \Gamma \vdash K}{\Gamma \vdash M}\,(\mathsf{blind}_{E1}) \qquad \frac{\Gamma \vdash M \qquad \Gamma \vdash K}{\Gamma \vdash \mathsf{blind}(M, K)}\,(\mathsf{blind}_I)$$

$$\frac{\Gamma \vdash \mathsf{sign}(\mathsf{blind}(M, R), K) \qquad \Gamma \vdash R}{\Gamma \vdash \mathsf{sign}(M, K)}\,(\mathsf{blind}_{E2})$$

$$\frac{\Gamma \vdash M_1 \qquad \ldots \qquad \Gamma \vdash M_n}{\Gamma \vdash f(M_1, \ldots, M_n)}\,(f_I), \text{ onde } f \in \Sigma_E \qquad \frac{\Gamma \vdash N}{\Gamma \vdash M}\approx_E, \text{ onde } M \approx_E N$$

Tabela 4.1: Sistema $\mathcal{N}'$: Dedução Natural para o Intruso

forma normal. O sistema de sequentes para dedução do intruso, sob a teoria equacional E é dado na Tabela 4.2.

Diferentemente das regras de dedução natural, regras de sequentes também permitem a introdução de termos no lado esquerdo do sequente. As regras p_L, e_L,sign_L,blind_{L1} e blind_{L2} são chamadas *regras esquerdas* e as regras p_R, e_R,sign_R,blind_R são chamadas *regras direitas* , com $\langle M, N\rangle$, $\{M\}_K$, $\mathsf{sign}(M, K)$, $\mathsf{blind}(M, K)$, $\mathsf{sign}(\mathsf{blind}((M, R), K)$ como *termo principal*, respectivamente. A regra *acut*, chamada de *corte analítico* é similar à regra de corte (*cut*), exceto que o termo principal A é um E-fator das mensagens do sequente mais abaixo, isto é, o termo eliminado é um subtermo dos termos anteriores. Esta regra é necessária para provar a *admissibilidade* da regra de corte [37, 41].

Proposição 2.7 em [41] *O sequente* $\Gamma \vdash M$ *é derivável no sistema* $\mathcal{N}'$ *se, e somente se,* $\Gamma \downarrow\!\vdash M \downarrow$ *é derivável no sistema* $\mathcal{S}$.

Demonstração. A demonstração desta proposição pode ser encontrada no trabalho [41]. □

Teorema 3.12 em [41] *A regra de corte é admissível para* $\mathcal{S}$.

Demonstração. A demonstração deste teorema pode ser encontrada no trabalho [41]. □

$$\frac{\overset{M\approx_E C[M_1,\ldots,M_k]}{\text{C[ ] um E-contexto},M_1,\ldots,M_k\in\Gamma}}{\Gamma\vdash M}\,(id) \qquad \frac{\Gamma\vdash M \qquad \Gamma,M\vdash T}{\Gamma\vdash T}\,(cut)$$

$$\frac{\Gamma,\langle M,N\rangle,M,N\vdash T}{\Gamma,\langle M,N\rangle\vdash T}\,(p_L) \qquad \frac{\Gamma\vdash M \qquad \Gamma\vdash N}{\Gamma\vdash\langle M,N\rangle}\,(p_R)$$

$$\frac{\Gamma\vdash M \qquad \Gamma\vdash K}{\Gamma\vdash\{M\}_K}\,(e_R) \qquad \frac{\Gamma,\{M\}_K\vdash K \qquad \Gamma,\{M\}_K,M,K\vdash N}{\Gamma,\{M\}_K\vdash N}\,(e_L)$$

$$\frac{\Gamma\vdash M \qquad \Gamma\vdash K}{\Gamma\vdash \mathsf{sign}(M,K)}\,(\mathsf{sign}_R) \qquad \frac{\Gamma\vdash M \qquad \Gamma\vdash K}{\Gamma\vdash \mathsf{blind}(M,K)}\,(\mathsf{blind}_R)$$

$$\frac{\Gamma,\mathsf{sign}(M,K),\,\mathsf{pub}(L),M\vdash N}{\Gamma,\mathsf{sign}(M,K),\,\mathsf{pub}(L)\vdash N}\,(\mathsf{sign}_L),K=_{AC}L$$

$$\frac{\Gamma,\mathsf{blind}(M,K)\vdash K \qquad \Gamma,\mathsf{blind}(M,K),M,K\vdash N}{\Gamma,\mathsf{blind}(M,K)\vdash N}\,(\mathsf{blind}_{L_1})$$

$$\frac{\Gamma,\mathsf{sign}(\mathsf{blind}(M,R),K)\vdash R \qquad \Gamma,\mathsf{sign}(\mathsf{blind}(M,R),K),\mathsf{sign}(M,K),R\vdash N}{\Gamma,\mathsf{sign}(\mathsf{blind}(M,R),K)\vdash N}\,(\mathsf{blind}_{L_2})$$

$$\frac{\Gamma\vdash A \qquad \Gamma,A\vdash M}{\Gamma\vdash M}\,(acut),\ A \text{ é um } E\text{-fator de } \Gamma\cup\{M\}$$

Tabela 4.2: Sistema $\mathcal{S}$: Cálculo de Sequentes para o Intruso

4.3 Problema da Dedução Elementar

Observe que o problema de decidir se $\Gamma \vdash M$ (PDI) para o Sistema $\mathcal{N}$ é equivalente ao problema de decidir se a regra (id) do Sistema $\mathcal{S}$ é aplicável em $\Gamma \vdash M$, isto é, é equivalente ao *problema da dedução elementar*:

Definição 4.3 (Problema da Dedução Elementar)**.** *Dado uma teoria equacional AC-convergente E e um sequente $\Gamma \vdash M$ básico e na forma normal, o* problema da dedução elementar *(PDE) para E, descrito por $\Gamma \Vdash_E M$, é o problema de decidir se a regra (id) é aplicável em $\Gamma \vdash M$(isto é, se existem um E-contexto $C[\ldots]$ e termos $M_1,\ldots,M_k \in \Gamma$ tais que $C[M_1,\ldots,M_k] \approx_E M$).*

Este problema consiste em um problema de unificação de ordem superior módulo uma teoria equacional E, como foi visto, inicialmente, como uma caracterização dos termos dedutíveis do Sistema $\mathcal{N}$ na Proposição 2.1.

Este problema foi introduzido em [41] porém, os autores não disponibilizaram nenhuma teoria equacional para a qual o problema fosse decidível. Utilizando os resultados obtidos no Capítulos 2 e 3, obtém-se que o *problema da dedução elementar* é decidível em tempo

polinomial em $|sat(\Gamma)|$ e $|M|$ para teorias **I**-localmente estáveis e em tempo polinomial não-determinístico para teorias **N**-localmente estáveis.

Teorema 4.1 (Decidibilidade Polinomial Determinística para o PDE)**.** *Seja E uma teoria equacional **I**-localmente estável. Seja $\Gamma \vdash M$ um sequente básico e na forma normal. O* problema da dedução elementar *para teoria E ($\Gamma \Vdash_E M$) é decidível em tempo polinomial em $|sat(\Gamma)|$ e $|M|$.*

Demonstração. Pelo Lema 3.1, o problema se $M =_{AC} C[M_1, \ldots, M_k]$ para um E-contexto C e termos $M_1, \ldots, M_k \in sat(\Gamma)$ é decidível em tempo polinomial em $|sat(\Gamma)|$ e $|M|$. Se $M =_{AC} C[M_1, \ldots, M_k]$ para um E-contexto C e termos $M_1, \ldots, M_k \in sat(\Gamma)$ então existe um E-contexto C' e termos $M'_1, \ldots, M'_n \in \Gamma$ tais que $C'[M'_1, \ldots, M'_n] \xrightarrow{*}_{\mathcal{R} \cup AC} M$. É suficiente notar que para todo $T \in sat(\Gamma)$, T pode ser deduzido dos termos em Γ.

Reciprocamente, se não existir um E-contexto C e termos $M_1, \ldots, M_k \in sat(\Gamma)$ tais que $M =_{AC} C[M_1, \ldots, M_k]$ então, pelo Corolário 2.1, não existem um E-contexto C e termos $M'_1, \ldots, M'_t \in sat(\Gamma)$ tais que $C[M'_1, \ldots, M'_t] \xrightarrow{*} M$. Portanto, não existe um E-contexto C'' e termos $M''_1, \ldots, M''_l \in \Gamma$ tais que $C''[M''_1, \ldots, M''_l] \xrightarrow{*} M$. Logo, o PDE para E é decidível em tempo polinomial em $|sat(\Gamma)|$ e $|M|$. □

Teorema 4.2 (Decidibilidade Polinomial não-determinística para o PDE)**.** *Seja E uma teoria equacional **N**-localmente estável. Seja $\Gamma \vdash M$ um sequente básico e na forma normal. O* problema da dedução elementar *para teoria E ($\Gamma \Vdash_E M$) é decidível em tempo não-determinístico polinomial em $|sat(\Gamma)|$ e $|M|$.*

Demonstração. A demonstração é análoga ao teorema anterior, com exceção da complexidade de tempo, que para teorias **N**-localmente estáveis a decidibilidade é polinomial não-determinística (pelo Lema 2.5). □

A seguinte definição refere-se a transformação do problema de dedução $\Gamma \vdash M$ em um sistema dedutivo $\mathcal{D}$ para um problema equacional de ordem superior (PDE), de forma que a redução de um problema para o outro é polinomial.

Definição 4.4 (Redução Polinomial)**.** *Seja $\Gamma \Vdash_{\mathcal{D}} M$ um problema de dedução, onde $\mathcal{D}$ é um sistema de prova, e seja n o tamanho de $St(\Gamma \cup \{M\})$. Seja E a teoria equacional associada com $\mathcal{D}$. Suponha que o problema da dedução elementar em E tenha complexidade $\mathcal{O}(f(m))$, onde m é o tamanho da entrada. Então o problema $\Gamma \Vdash_{\mathcal{D}} M$ é dito ser* polinomialmente redutível *para o problema da dedução elementar $\Vdash_E$ se ele tiver complexidade $\mathcal{O}(n^k \times f(n))$ para alguma constante k.*

4.3.1 Sistema Dedutivo Linear para o Intruso

Nesta seção o objetivo é mostrar como o PDI pode ser reduzido para um problema de decisão "elementar", que se baseia exclusivamente nas características algébricas do modelo criptográfico em questão.

Primeiramente, propõe-se um sistema dedutivo para o intruso que é livre de corte e gera derivações *normais*.

Definição 4.5. *Uma derivação livre de corte* Π *é dita ser uma* derivação normal *se ela satisfaz as seguintes condições:*

- *nenhuma regra esquerda aparece acima de uma regra direita;*
- *nenhuma regra esquerda aparece imediatamente acima da premissa esquerda de uma regra esquerda ramificada.*

A seguir, denota-se por $\Gamma \Vdash_{\mathcal{R}} M$ o fato de que o sequente $\Gamma \vdash M$ é derivável utilizando apenas regras direitas e (id). Obtém-se um sistema dedutivo mais compacto para a dedução do intruso, chamado Sistema $\mathcal{L}$:

$$\frac{\Gamma \Vdash_{\mathcal{R}} M}{\Gamma \vdash M}\,(r) \qquad \frac{\Gamma, \{M\}_K, M, K \vdash N}{\Gamma, \{M\}_K \vdash N}\,(l_e), \text{ onde } \Gamma, \{M\}_K \Vdash_{\mathcal{R}} K$$

$$\frac{\Gamma, \langle M, N\rangle, M, N \vdash T}{\Gamma, \langle M, N\rangle \vdash T}\,(l_p) \qquad \frac{\Gamma, \mathsf{sign}(M,K),\ \mathsf{pub}(L), M \vdash N}{\Gamma, \mathsf{sign}(M,K),\ \mathsf{pub}(L) \vdash N}\,(\mathsf{sign})K =_{AC} L$$

$$\frac{\Gamma, \mathsf{blind}(M,K), M, K \vdash N}{\Gamma, \mathsf{blind}(M,K) \vdash N}\,(\mathsf{blind}_1), \text{ onde } \Gamma, \mathsf{blind}(M,K) \Vdash_{\mathcal{R}} K$$

$$\frac{\Gamma, \mathsf{sign}(\mathsf{blind}(M,R),K), \mathsf{sign}(M,K), R \vdash N}{\Gamma, \mathsf{sign}(\mathsf{blind}(M,R),K) \vdash N}\,(\mathsf{blind}_2), \text{ onde } \Gamma, \mathsf{sign}(\mathsf{blind}(M,R),K) \Vdash_{\mathcal{R}} R$$

$$\frac{\Gamma \vdash A \qquad \Gamma, A \vdash M}{\Gamma \vdash M}\,(ls), \text{ onde } A \text{ é um } E\text{-fator de } \Gamma \cup \{M\} \text{ e } \Gamma \Vdash_{\mathcal{R}} A$$

Figura 4.1: Sistema $\mathcal{L}$: Sistema de Prova Linear para o Intruso

O seguinte lema garante que os sistemas $\mathcal{S}$ e $\mathcal{L}$ são equivalentes do ponto de vista da relacão de dedução:

Lema 4.1 ([41])**.** *Um sequente* $\Gamma \vdash M$ *é derivável em* $\mathcal{S}$ *se, e somente se,* $\Gamma \vdash M$ *é derivável em* $\mathcal{L}$*.*

O seguinte teorema é válido para teorias equacionais E que contém um único símbolo AC ou é formada pela união finita e disjunta de teorias equacionais $E_1, \ldots, E_n$ cada uma contendo um símbolo AC [41]. Uma extensão deste resultado foi proposta em [37], onde prova-se que a redução polinomial mantém-se mesmo para teorias contendo três símbolos AC adicionadas com equacões para exponenciação e que não podem ser divididas em subteorias equacionais disjuntas.

Teorema 4.3 ($\Vdash_{\mathcal{L}}$ reduz polinomialmente para $\Vdash_E$ [37,41])**.** *O problema de decidir se um sequente* $\Gamma \vdash M$ *no Sistema* $\mathcal{L}$ *é polinomialmente redutível para o problema de decidir o problema da dedução elementar* $\Gamma \Vdash_E M$*.*

Corolário 4.1. *Seja E uma teoria **I**-localmente estável contendo um único símbolo AC ou formada por uma união finita e disjunta de símbolos AC. Sejam Γ um conjunto finito de termos básicos na forma normal e M um termo básico e na forma normal. O* Problema da dedução do Intruso *para a teoria E combinada com assinaturas cegas $\Gamma \vdash_{\mathcal{L}} M$ é decidível em tempo polinomial em $|sat(\Gamma)|$ e $|M|$.*

Demonstração. Como E é uma teoria equacional**I**-localmente estável, pelo Teorema 4.1 segue que $\Gamma \Vdash_E M$ é decidível em tempo polinomial em $|sat(\Gamma)|$ e $|M|$. Como, pelo Teorema anterior, a decidibilidade de $\Gamma \vdash_{\mathcal{L}} M$ reduz polinomialmente para a decidibilidade de $\Gamma \Vdash_E M$, segue o resultado. □

Corolário 4.2. *Seja E uma teoria **N**-localmente estável contendo um único símbolo AC ou formada por uma união finita e disjunta de símbolos AC. Sejam Γ um conjunto finito de termos básicos na forma normal e M um termo básico e na forma normal. O* Problema da dedução do Intruso *para a teoria E combinada com assinaturas cegas $\Gamma \vdash_{\mathcal{L}} M$ é decidível em tempo não-determinístico polinomial em $|sat(\Gamma)|$ e $|M|$.*

Demonstração. Como E é uma teoria equacional **N**-localmente estável, pelo Teorema 4.2 segue que $\Gamma \Vdash_E M$ é decidível em tempo polinomial não-determinístico em $|sat(\Gamma)|$ e $|M|$. Como, pelo Teorema anterior, a decidibilidade de $\Gamma \vdash_{\mathcal{L}} M$ reduz polinomialmente para a decidibilidade de $\Gamma \Vdash_E M$, segue o resultado. □

Conclusão

Este trabalho apresenta uma nova metodologia para decidir o *Problema da Dedução do Intruso* para teorias equacionais associativas e comutativas. Esta metodologia foi inspirada pelo trabalho de M. Abadi e V. Cortier em [1] onde o método é descrito no contexto do *pi-calculus aplicado*. Verificamos que o método de M. Abadi e V. Cortier não se aplica a teorias AC como foi afirmado. Portanto, desenvolvemos novas técnicas para o estudo da decidibilidade do PDI, utilizando reescrita, casamento módulo AC e equações diofantinas, além disso, caracterizamos classes de teorias AC para as quais nosso método pode ser aplicado.

Teorias equacionais associativas e comutativas são, em geral, difíceis de serem tratadas devido ao caráter dinâmico da estrutura de seus termos (e.g. a decidibilidade do problema do AC-casamento e de *AC-unificação com constantes* [7] são NP-completos). A estrutura dos termos se altera módulo AC, e isto dificulta a análise, uma vez que é necessário verificar todas as combinações possíveis.

Em particular, a teoria de grupos Abelianos é relevante para o estudo do problema da dedução do intruso, uma vez que vários protocolos criptográficos fazem uso das suas propriedades algébricas nas primitivas criptográficas. Com base nessa importância, foi feito um levantamento dos trabalhos que trataram de problemas de dedução levando em conta a teoria de grupos Abelianos. Dois trabalhos foram encontrados:

- Em [19] os autores estudaram a decidibilidade do PDI para a teoria equacional de grupos Abelianos. Utilizando uma abordagem de provas normais, os autores provaram que o problema está em NP. No entanto, a demonstração principal do trabalho está imprecisa, alguns casos não tinham sido analisados, o que dificultou a leitura. Uma versão completa da demonstração, com todos os ajustes necessários foi apresentada neste trabalho (Subseção 1.6.1).

- Em [30] os autores estudaram a decibilidade do PDI para algumas teorias AC com homomorfismos. Para isto, propuseram uma generalização da localidade de McAllester [33], e afirmaram que seguindo suas técnicas é possível provar que a decidibilidade do PDI para grupos Abelianos está em P, melhorando o trabalho [19]. Apesar da afirmação, não foi encontrada disponível na literatura nenhuma prova. Afim de provar que o resultado está de fato em P seria necessário definir uma função polinomial de subtermos adequada para a teoria equacional de grupos Abelianos. Porém, seguindo as técnicas propostas pelos autores, mesmo para teoria de grupos

Abelianos com homomorfismo, a função de subtermos encontrada é exponencial. O que torna a decibilidade do problema, seguindo essas técnicas, também exponencial. Pode ser que exista uma definição da função de subtermos tal que o problema esteja na classe P, mas esta é desconhecida.

Ainda em busca de resultados de decidibilidade para o PDI para teorias AC, encontramos o trabalho [41]. Neste trabalho, os autores utilizam técnicas conhecidas de tradução entre sistemas de dedução natural e o cálculo de sequentes e reformulam o PDI como um problema de busca de prova no cálculo de sequentes. Neste contexto, o PDE é introduzido, este problema é uma versão puramente equacional (algébrica) do problema da dedução do intruso. No entanto nenhuma teoria equacional para a qual este problema fosse decidível foi apresentada. Afim de encontrar classes de teorias AC para as quais o problema fosse decidível, o trabalho [1], apresentou-se com propriedades significantes, uma vez que a estrutura do problema em [41] era similar à estrutura dos termos da classe de teorias apresentada em [1].

Com um estudo mais detalhado das técnicas apresentadas em [1], bem como da classe de teorias equacionais apresentada, um contra-exemplo foi encontrado. O algoritmo proposto pelos autores de [1], afirmado ser polinomial, é na verdade, exponencial. Mais ainda, a classe de teorias definida, as chamadas *localmente estáveis*, não satisfazem todas as propriedades que o trabalho afirma possuir, a análise local das reduções de reescrita não se estende para a análise global, o que impede uma previsão dos termos dedutíveis a partir de um conhecimento inicial de um intruso passivo.

Neste trabalho, um novo algoritmo de decisão é proposto. O algoritmo utiliza um procedimento secundário para o problema de casamento AC com ocorrências distintas em combinação com uma redução para o problema da satisfatibilidade de sistemas de equações Diofantinas lineares. O algoritmo roda em tempo polinomial para a classe de teorias **I**-localmente estáveis, que foi definida neste trabalho. E roda em tempo polinomial não determinístico para a classe de teorias **N**-localmente estáveis, também definida neste trabalho.

Para ilustrar os resultados, a teoria de grupos Abelianos foi considerada. Em [1] os autores afirmaram que esta teoria é *localmente estável*, sem apresentar uma demonstração. Uma vez que, com os ajustes necessários, a classe de das teorias *localmente estáveis* se equipara com classe das teorias **N**-localmente estáveis, tentou-se provar que a teoria de grupos Abelianos era um exemplo desta teoria. No entanto, não foi possível definir um conjunto saturado adequado para a teoria de grupos Abelianos: o conjunto com todas as propriedades necessárias seria infinito, e isto contradiz a definição de ser **N**-localmente estável.

Com o objetivo de encontrar um exemplo viável e com aplicações no estudo de protocolos criptográficos, a teoria de grupos Abelianos finitos foi considerada. Não foi possível gerar uma teoria equacional geral, induzida pelas equações de grupos Abelianos e com a hipótese adicional de finitude. A solução encontrada, que foi utilizada neste trabalho, foi definir uma teoria equacional cujos modelos são grupos Abelianos de ordem n dada (no caso considerado, os grupos cíclicos de ordem n). Não foi encontrada na literatura

nenhuma família de sistemas de reescrita convergente para esta teoria. Utilizando a ferramenta de completamento à la Knuth Bendix, do sistema de tratamento equacional via reescrita CiME, obteve-se um sistema de reescrita de termos convergente módulo AC, associado a esta teoria. Demonstrou-se então que esta teoria equacional é **I**-localmente estável, e os resultados de decidibilidade se aplicam.

Verificamos que a decidibilidade do PDE está em P para as teorias **I**-localmente estáveis e em NP para as teorias **N**-localmente estáveis. Como uma extensão, aplicamos os resultados obtidos para o estudo do PDI para teorias **I**-localmente estáveis combinadas com a teoria de assinaturas cegas, e obtemos que a decidibilidade está em P. Já para as teorias **N**-localmente estáveis combinadas com assinaturas cegas, a decidibilidade está em NP.

Como trabalho futuro propõe-se verificar a aplicabilidade da metodologia no estudo de outras teorias equacionais, em particular, para a teoria equacional da exponenciação, que é uma teoria mais complexa composta pelos axiomas de dois grupos Abelianos os axiomas de exponenciação : $x^y \cdot x^z = x^{y+z}$ e $(x^y)^z = x^{yz}$. Esta teoria equacional não pode ser dividida em partes disjuntas. Seria necessário construir um novo conjunto $sat(\Gamma)$ que satisfaça as propriedades equacionais adicionais. Uma outra teoria interessante seria XOR que possui propriedades axiomáticas que parecem adequadas para classificá-la como sendo **N**-localmente estável, no entanto, é necessário definir o conjunto de subtermos módulo AC mais adequado para esta teoria. Caso seja possível definir um conjunto $sat(\Gamma)$ para teoria XOR, a decidibilidade do PDI está em NP, uma vez que o sistema de equações diofantinas gerado recai no problema *Knapsack 0-1*, que é um problema NP-completo.

Baseados nas técnicas desenvolvidas neste trabalho, é também de grande interesse investigar resultados da relação de indistinguibilidade, como foi pretendido em [1]. Para isto, seria necessário traduzir a metodologia para a linguagem do *pi-calculus* e verificar a relação entre a decidibilidade em teorias **N**- ou **I**- localmente estáveis e a relação de *equivalência estática*, isto é, a relação de equivalência entre mensagens que um sistema gera.

Para finalizar, é importante a implementação da metodologia de dedução para aplicações de segurança. Diversos assistentes de prova e sistemas de especificação equacional via reescrita como Maude e CiME podem ser utilizados e integrados para aplicar as técnicas propostas.

Bibliografia

[1] M. Abadi and V. Cortier. Deciding knowledge in security protocols under equational theories. *Theoretical Computer Science*, 367(1-2):2–32, 2006. http://dx.doi.org/10.1016/j.tcs.2006.08.032.

[2] M. Abadi and C. Fournet. Mobile Values, New Names, and Secure Communication. In *Proc. 28th POPL'01*, pages 104–115, 2001. DOI: 10.1145/360204.360213.

[3] M. Abadi and A. Gordon A Calculus for Cryptographic Protocols: The spi Calculus. *Information and Computation* , 148(1): 1–70, 1999. http://dx.doi.org/10.1006/inco.1998.2740.

[4] A. Armando *et al.* The AVISPA Tool for the Automated Validation of Internet Security Protocols and Applications. In *Proc. 17th Computer Aided Verification (CAV'05)*, volume 3576, pages 281–285. Springer-Verlag 2005. DOI: 10.1007/11513988_27.

[5] M. Arnaud, V. Cortier and S. Delaune. Deciding Security for Protocols with Recursive Tests. In *Proc. of CADE*, volume 6803 of *LNCS*, pages 49–63, 2011. DOI:http://dx.doi.org/10.1007/978-3-642-22438-6_6.

[6] M. Ayala-Rincón, M. Fernández and D. Nantes-Sobrinho. Elementary Deduction for Locally Stable Theories with Normal Forms. In *Proc. of 7th Workshop on Logical and Semantic Frameworks, with Applications (LSFA'12)*, volume 113 of *EPTCS*, pages 45–60, 2012. DOI: http://dx.doi.org/10.4204/EPTCS.113.7

[7] F. Baader and T. Nipkow. *Term Rewriting and All That.* CUP, 1998.

[8] M. Baudet, V. Cortier and S. Delaune. YAPA: A Generic Tool for Computing Intruder Knowledge. In *Proc. of RTA'09*, volume 5595 of *LNCS*, pages 148-163. Springer, 2009. arXiv:1005.0737, DOI: 10.1007/978-3-642-02348-4_11.

[9] D. Benanav, D. Kapur, P. Narendran, and L. Wang. Complexity of matching problems. In *Journal of Symbolic Computation*, 3(1/2): 203–216, 1987. DOI: 10.1007/3-540-15976-2_22.

[10] V. Bernat and H. Comon-Lundh. Normal proofs in intruder theories. In *ASIAN*, volume 4435 of *LNCS*, pages 151–166. Springer-Verlag, 2006. DOI: 10.1007/978-3-540-77505-8_12.

[11] M. Berrima, N. B. Rajeb and V. Cortier. Deciding knowledge in security protocols under some e-voting theories. *RAIRO - Theor. Inf. and Applic.*, 45(3), 269–299, 2011. DOI: http://dx.doi.org/10.1051/ita/2011119.

[12] B. Blanchet. An Efficient Cryptographic Protocol Verifier Based on Prolog Rules. In *Proc. CSFW'01*, pages 82–96, IEEE Comp. Soc. , 2001. http://doi.ieeecomputersociety.org/10.1109/CSFW.2001.930138.

[13] A. Boudet, E. Contejean and H. Devie. A new AC Unification Algorithm with an Algorithm for Solving Systems of Linear Diophantine Equations. In *5th. Proc. of LICS*, pages 289–299, 1990. http://dx.doi.org/10.1109/LICS.1990.113755.

[14] B. Bursuc, H. Comon-Lundh, and S. Delaune. Deducibility constraints, equational theory and electronic money. In *Rewriting, Computation and Proof*, volume 4600 of *LNCS*, pages 196–212. Springer-Verlag, 2007. DOI: 10.1007/978-3-540-73147-4_10.

[15] D. Chaum Blind Signatures for Untraceable Payments. *Advances in Cryptology - Proceedings of CRYPTO'82, Lecture Notes in Computer Science*, pages 199–203, Springer-Verlag, 1982. .

[16] Y. Chevalier, R. Küsters, M. Rusinowitch and M. Turuani An NP decision procedure for protocol insecurity with XOR. In *Theorethical Computer Science*, volume 338 (1–3), pages 247–274, 2005. DOI: http://dx.doi.org/10.1016/j.tcs.2005.01.015

[17] M. Clausen and A. Fortenbacher. Efficient Solution of Linear Diophantine Equations. In *Journal of Symbolic Computation*, Volume 8, Issues 1-2, pages 201–216, 1989. http://dx.doi.org/10.1016/S0747-7171(89)80025-2.

[18] H. Comon-Lundh and R. Treinen In *Verification: Theory and Practice, Essays Dedicated to Zohar Manna on the Occasion of His 64th Birthday*, volume 2772 of *LNCS*, pages 225–242. Springer, 2003. DOI: http://dx.doi.org/10.1007/978-3-540-39910-0_10.

[19] H. Comon-Lundh and V. Shmatikov. Intruder Deduction, Constraint Solving and Insecurity Decisions in Presence of Exclusive or. In *LICS*, pages 271–280. IEEE Comp. Soc., 2003. http://doi.ieeecomputersociety.org/10.1109/LICS.2003.1210067.

[20] E. Contejean, C. Marché, B. Monate, and X. Urbain. The CiME rewrite tool (version 2), 2000. Available at http://cime.lri.fr/.

[21] E. Contejean, P. Courtieu, J. Forest, O. Pons and X. Urbain The CiME rewrite tool (version 3), 2011. Available at http://cime.lri.fr.

[22] V. Cortier and S. Delaune. Decidability and Combination Results for Two Notions of Knowledge in Security Protocols *Journal of Automated Reasoning*, 48(4): 441–487, 2012. http://dx.doi.org/10.1007/s10817-010-9208-8.

[23] 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.

[24] S. Delaune. Easy Intruder Deduction Problems with Homomorphisms. *Inf. Process. Lett.*, volume 97(6), pages 213–218, 2006. http://dx.doi.org/10.1016/j.ipl.2005.11.008.

[25] D. Dolev and A. Yao. On the security of public keys protocols. In *Proc. 22nd Annual Symp. on Foundations of Computer Science*, 350–357, 1981. http://doi.ieeecomputersociety.org/10.1109/SFCS.1981.32.

[26] S. Escobar, C. Meadows and J. Meseguer. Maude-NPA: Cryptographic Protocol Analysis Modulo Equational Properties. FOSAD 2007, 1–50, 2007. DOI: 10.1007/978-3-642-03829-7_1.

[27] M. A. Frumkin. Polynomial time Algorithms in the Theory of Linear Diophantine Equations. In *Proc. of Fundamentals of Computation Theory*, volume 56 of *LNCS*, 386–392, Springer-Verlag, 1977. DOI: 10.1007/3-540-08442-8_106.

[28] M. R. Garey and D. S. Johnson. Computers and Intractability: A Guide to the Theory of NP-completeness. W. H. Freeman and Co., 1979.

[29] G. Huet. An Algorithm to Generate the Basis of Solutions to Homogeneous Linear Diophantine equations. *Inf. Process. Lett.*, volume 7(3), pages 144–147, 1978. DOI: http://dx.doi.org/10.1016/0020-0190(78)90078-9.

[30] P. Lafourcade, D. Lugiez and R. Treinen. Intruder Deduction for AC-Like Equational Theories with Homomorphisms In *Proc. of RTA*, volume 3467 of *LNCS*, pages 308–322, Springer-Verlag, 2005. http://dx.doi.org/10.1007/978-3-540-32033-3_23.

[31] P. Lafourcade, D. Lugiez and R. Treinen. Intruder Deduction for AC-Like Equational Theories with Homomorphisms. Reearch Report LSV-04-16, LSV, ENS de Cachan, Nov. 2004. Available at http://www.lsv.ens-cachan.fr/Publis/RAPPORTS_LSV/rapports-year-2004-list.php.

[32] P. Lafourcade. Intruder Deduction for the equational theory of exclusive-or with commutative and distributive encryption. In *Electr. Notes Theor. Comput. Sci.*, volume 171(4): 37–57, 2007. http://dx.doi.org/10.1016/j.entcs.2007.02.054.

[33] D. McAllester. Automatic recognition of tractability in inference relations. *Journal of the ACM*, volume 40, pages 284–303, 1990. DOI: 10.1145/151261.151265.

[34] A. J. Menezes, P. C. van Oorschot and S. A. Vanstone. Handbook of Applied Cryptography, CRC Press LLC.

[35] J. K. Millen and V. Shmatikov. Symbolic protocol analysis with an Abelian group operator or Diffie-Hellman exponentiation. *Journal of Computer Security*, volume 13 (3): pages 515–564, 2005.

[36] V. Shmatikov. Decidable Analysis of Cryptographic Protocols with Products and Modular Exponentiation. In *13th European Symposium on Programming*, volume 2986, pages 355–369, 2004. DOI:10.1007/978-3-540-24725-8_25

[37] D. Sobrinho e M. Ayala-Rincón. Reduction of the Intruder Deduction Problem into Equational Elementary Deduction for Electronic Purse Protocols with Blind Signatures. In *Proc. 17th WoLLIC'10*, volume 6188 of *LNCS*, pages 218–231, Springer-Verlag, 2010. DOI: 10.1007/978-3-642-13824-9_18.

[38] C. Papadimitriou e K. Steiglitz. Combinatoria Optimization: Algorithms and Complexity. Dover Publications, INC.

[39] C. Papadimitriou. Computational Complexity. Addison-Wesley, Inc.

[40] A. Tiu. A trace based simulation for the spi calculus: An extended abstract. In *APLAS*, volume 4807 of *LNCS*, pages 367–382, Springer, 2007. arXiv:0901.2166.

[41] A. Tiu, G. Rajeev and J. Dawson. A proof theoretic analysis of intruder theories. In *Proc. of RTA'09*, volume 5595 of *LNCS*, pages 103–117. Springer-Verlag, 2009. DOI: 10.2168/LMCS-6(3:12)2010.