



Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

Unificação Assimétrica Módulo Operadores Nilpotentes com Homomorfismo

por

Bruno de Assis Delboni

Orientador: Daniele Nantes Sobrinho

Brasília

2017

Bruno de Assis Delboni

Unificação Assimétrica Módulo Operadores Nilpotentes com Homomorfismo

Dissertação apresentada ao Departamento de
Matemática da Universidade de Brasília,
como parte dos requisitos para a obtenção do
grau de MESTRE em Matemática.

Orientador: Daniele Nantes Sobrinho

Brasília

2017

Ficha catalográfica elaborada automaticamente,
com os dados fornecidos pelo(a) autor(a)

DD344u Delboni, Bruno de Assis
Unificação Assimétrica Módulo Operadores
Nilpotentes com Homomorfismo / Bruno de Assis
Delboni; orientador Daniele Nantes Sobrinho. --
Brasília, 2017.
152 p.

Dissertação (Mestrado - Mestrado em Matemática) --
Universidade de Brasília, 2017.

1. Teoria da Computação. 2. Unificação. 3.
Unificação assimétrica. 4. Teoria equacional ACUN(h).
I. Sobrinho, Daniele Nantes, orient. II. Título.

Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

Unificação Assimétrica Módulo Operadores Nilpotentes com Homomorfismo

por

Bruno de Assis Delboni *

*Dissertação apresentada ao Departamento de Matemática da Universidade
de Brasília, como parte dos requisitos para obtenção do grau de*

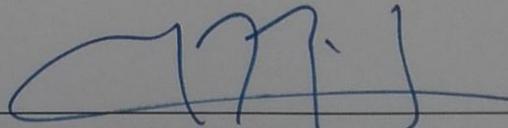
MESTRE EM MATEMÁTICA

Brasília, 06 de março de 2017.

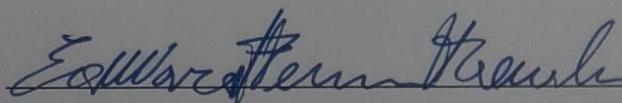
Comissão Examinadora:



Prof. Dra. Daniele Nantes Sobrinho - MAT/UnB (Orientadora)



Prof. Dr. Mauricio Ayala Rincón - MAT/UnB (Membro)



Prof. Dr. Edward Hermann Haeusler - PUC-RIO (Membro)

* O autor foi bolsista do CNPq durante a elaboração desta dissertação.

”Night gathers, and now my watch begins. It shall not end until my death. I shall take no wife, hold no lands, father no children. I shall wear no crowns and win no glory. I shall live and die at my post. I am the sword in the darkness. I am the watcher on the walls. I am the shield that guards the realms of men. I pledge my life and honor to the Night’s Watch, for this night and all the nights to come.”—The Night’s Watch oath

Agradecimentos

Agradeço primeiramente aos meus pais Eliseu Antônio e Bruna Valéria, por todos seus sacrifícios que tiveram para me educar, saibam que todo meu esforço é para orgulhá-los. Aos meus irmãos Arthur Henrique e Luana, que são meus verdadeiros amigos e sempre me apoiaram. A minha tia-mãe Sandra e aos meus primo-irmãos Junior e Morgana. Dedico especialmente este trabalho a minha avó Santa que não tive a honra de conhecê-la e aos meus avós Maria Euzélia e Hegner Francisco.

Agradeço a minha orientadora Daniele Nantes por ter me dado a oportunidade de ser seu orientando, por ter acreditado em minha capacidade mesmo quando eu duvidava, aos ensinamentos que me passaste e principalmente as críticas boas e ruins que me fizeram crescer como aluno e pessoa.

Agradeço aos meus amigos de Brasília e do mestrado, Weninson e Welinton que me apoiaram, a Sara Raíssa por me ajudar e dividir angústias, Salém por sua amizade e pelas nossas conversas, e especialmente ao Rafael e a Nathália que sempre estiveram ao meu lado e que sem eles não teria perseverado.

Agradeço especialmente a Elvira Padua Lovatte por sua inspiração, aos meus amigos da graduação André e Lucas pela sua amizade e suporte, José Eduardo (Mangue), Eneas (Maioral), Thiago (Solão) e Aaron (Yani) por suas amizades sinceras e por me apoiarem constantemente.

E por último mas não menos importante, agradeço a Bélinha por sua amizade e palavras gentis nos momentos que mais precisava, a Aline e Débora por sua amizade e por fazerem parte da minha vida durante boa parte da graduação.

Obrigado a todos que me apoiaram durante minha jornada e claro agradeço a CNPq por seu apoio financeiro à minha carreira acadêmica.

Resumo

Esta dissertação tem como foco o estudo do problema de unificação módulo uma teoria equacional cuja assinatura contém um operador binário \oplus que satisfaz as identidades Associatividade, Comutatividade, Unidade e Nilpotência (ACUN), e que pode ou não conter um operador unário h que satisfaz a identidade de homomorfismo (ACUNh), que é a teoria equacional do operador *XOR*, amplamente utilizado em diversas ferramentas criptográficas, como MAUDE-NPA [10] que utiliza uma encriptação de grupos abelianos, incluindo *XOR* (ou exclusivo), exponenciação e encriptação homomórfica. Primeiro apresentaremos alguns critérios para existência de soluções para problemas de ACUN(h)-unificação *elementar com constantes* que consiste em associar o problema de unificação à um sistema de equações lineares cujos coeficientes são elementos de \mathbb{Z}_2 ou $\mathbb{Z}_2[h]$, dependendo se o homomorfismo é ou não considerado. Segundo, apresentaremos um algoritmo para resolver problemas de ACUN(h)-unificação geral que retorna sempre um conjunto completo de unificadores. Finalmente, apresentaremos o estudo de um novo paradigma de unificação, a dizer, *unificação assimétrica*, que consiste de obter unificadores de um problema Γ de unificação com a propriedade de preservar formas normais do lado direito de cada equação de Γ com relação a um sistema de reescrita *convergente e coerente* módulo uma teoria equacional E . No caso particular da teoria equacional ACUN construiremos um algoritmo de conversão de ACUN-unificadores para ACUN-unificadores assimétricos.

Palavras-chave: Unificação, unificação assimétrica, teoria equacional ACUN(h)

Abstract

This dissertation focuses on the study of unification problems modulo an equational theory whose signature contains a binary operator \oplus , which satisfies the identities of *Associativity*, *Commutativity*, *Unity* and *Nilpotence* (ACUN), and which may or not contain a unary operator h satisfying the homomorphism identity (ACUNh), which is the equational theory for the operator XOR, Widely used on many cryptographic tools, like MAUDE [10], which uses group encryption, including XOR (exclusive or), exponentiation and homomorphic encryption. First we will present some criteria to the existence of solutions for *elementary with constants* ACUN(h)-unification problems which consist of associating a unification problem to a linear equation system whose coefficients are elements of \mathbb{Z}_2 or $\mathbb{Z}_2[h]$, depending one we are considering homomorphism or not. Second, we will present an algorithm to solve *general* ACUNh-unification problems which always returns a complete set of most general unifiers. Finally, we will present the study of a new unification paradigm, to say so, *asymmetric unification*, which consist of obtaining unifiers from the unification problem Γ , with the property of preserving the normal form from of the right hand side of each equation in Γ , considering a convergent and coherent rewriting system. In the particular case of the equational theory ACUN, we will also present an algorithm which takes as input ACUN-unifiers and outputs ACUN-asymmetric unifiers.

Keywords: Unification, asymmetric unification, ACUN(h) equational theory

Sumário

1	Preliminares	17
1.1	Termos, Substituições e Identidades	17
1.2	Álgebras, Homomorfismos e Congruências	23
1.3	Classes Equacionais	25
1.4	Sistemas de Reescrita de Termos e Unificação	26
1.4.1	Reescrita Módulo Teorias Equacionais	27
1.4.2	Unificação Módulo Teorias Equacionais	28
2	Unificação Módulo ACUN	33
2.1	Conceitos Básicos	34
2.2	Padronização	35
2.3	ACUN-unificação Elementar com Constantes	37
2.3.1	ACUNh-unificação Elementar com constantes	44
2.4	Unificação Geral ACUN(h)	52
3	Um algoritmo eficiente para ACUNh-unificação	56
3.1	Purificação	56
3.1.1	Terminação e correção de [Purif]	66
3.1.2	Confluência da purificação	71
3.1.3	Algoritmo Purif	79
3.2	\mathcal{J}_{XORh} : um algoritmo para ACUNh-unificação	80
3.2.1	Terminação de \mathcal{J}_{XORh}	89

3.2.2	Correção de \mathcal{J}_{XORh}	92
3.2.3	Completude de \mathcal{J}_{XORh}	99
4	Unificação Assimétrica	112
4.1	Preliminares	113
4.2	Unificação assimétrica módulo ACUN	115
4.3	Um algoritmo para ACUN–unificação assimétrica	121
4.3.1	Regras de \mathcal{J}_{AXO}	122
5	Correção e Completude de \mathcal{J}_{AXO}	132
5.1	Idempotência das Soluções e Regularidade dos Estados Válidos de \mathcal{J}_{AXO}	132
5.2	Correção e Completude	140

Introdução

Este trabalho aborda técnicas para resolver o problema de decidir se dois termos, digamos s e t , são *unificáveis*, isto é, se existe uma substituição σ tal que $s\sigma = t\sigma$. Em particular, vamos tratar do caso em que a assinatura de termos contém símbolos de função com as propriedades algébricas: Associatividade, Comutatividade, Unidade, Nilpotência e homomorfismo (ACUNh).

Dentre as aplicações de unificação estão: o processo de ligação de variáveis na execução de programas lógicos, utilizado, por exemplo, em *provadores* automáticos de teoremas; *reescrita de termos*, que modelam computação *passo-a-passo*; análise de segurança de protocolos criptográficos, entre outros.

Em meados de 1980, Dolev e Yao, no trabalho [8] iniciam o uso de métodos formais para analisar protocolos de criptografia a fim de detectar vulnerabilidades, os autores supõem que as mensagens são elementos de uma *álgebra livre*, isto é, o intruso malicioso apenas considera funções abstratas, no qual suas propriedades intrínsecas não são levadas em consideração.

Nesse modelo [8], duas mensagens são ditas iguais se são representadas pelo mesmo termo, neste caso, durante uma busca de possíveis ataques, o termo que representa a mensagem esperada é *comparada* com o termo que representa a mensagem enviada.

Porém esta abordagem ignora o fato de que possa existir alguma propriedade algébrica sobre os termos que representam as mensagens, permitindo assim que intrusos maliciosos possam obter alguma informação da mensagem sem a necessidade de possuir a chave. Para resolver esse problema, são utilizadas abordagens modernas de análise de protocolos de criptografia utilizando métodos mais flexíveis, que levam essas propriedades algébricas em consideração [7].

Surge então o interesse em resolver problemas de *unificação com propriedades algébricas* de uma teoria E , ao invés de apenas a unificação sintática, para de detectar um possível ataque. Para tal, faz-se

uma busca sobre os procedimentos do protocolo, encontrando possíveis vulnerabilidades via unificação dos termos, porém esse espaço de busca pode ter um tamanho arbitrário e/ou até infinito, então encontrar um algoritmo de unificação que diminui o espaço de busca de vulnerabilidades consideravelmente é essencial para a análise de protocolos de criptografia.

A partir da necessidade do desenvolvimento de técnicas mais eficientes para solubilidade da unificação equacional, apresentaremos, neste trabalho os métodos desenvolvidos para a teoria equacional cujos modelos são grupos Abelianos de expoente 2 [11, 16, 18]. Mais especificamente, os objetivos são:

1. Fazer um levantamento histórico das técnicas existentes para solubilidade do problema da unificação módulo a teoria equacional que envolve operadores Associativos, Comutativos, Unidade, Nilpotência (ACUN) e possivelmente uma função h com propriedade de homomorfismo.
2. Apresentar o método de unificação módulo ACUN(h) proposto por Liu [18], bem como o problema de *unificação assimétrico*, que faz uma restrição sobre as soluções de um problema de unificação tradicional.

Vamos seguir a abordagem proposta por Guo, Narendran e Wolfran em [11], para problemas de ACUN(h)-unificação elementar com constantes: a cada problema Γ de ACUN(h)-unificação é associado um conjunto de sistemas de equações lineares com coeficientes no corpo booleano \mathbb{Z}_2 , no caso da teoria equacional ACUN, e para ACUN h , com coeficientes em $\mathbb{Z}_2[h]$, o anel de polinômios sobre o corpo booleano \mathbb{Z}_2 com incógnita h . Um critério para existência de unificador para Γ fica então relacionado com existência de soluções para cada sistema de equações lineares, donde segue que a complexidade para computar uma solução para Γ é polinomial.

Porém, quando são considerados símbolos de função não interpretados na teoria equacional ACUN(h), Schulz em seu artigo [16] mostra que decidir se Γ é unificável é NP-difícil. Seguindo o método proposto por Liu em [18], vamos apresentar um algoritmo mais eficiente para computar um conjunto completo de ACUN(h)-unificadores para um problema de unificação Γ geral, isto é, cuja assinatura contém símbolos de função não interpretados.

Observa-se que muitos métodos de análise de protocolos adotam técnicas para automaticamente detectar estados inalcançáveis ou redundantes, assim aperfeiçoando a busca por possíveis invasores, como é o caso do Maude-NPA [10].

São técnicas muito úteis em aumentar a eficiência da análise de protocolos de criptografia. No entanto estas técnicas são incompatíveis com os métodos de unificação usuais.

Para solucionar esse problema Liu *et. al.* [9] propõem um novo paradigma de unificação, chamado *unificação assimétrica*, que consiste em:

- Decompor a teoria equacional E' em um par (\mathcal{R}, E) , onde \mathcal{R} é um sistema de reescrita convergente módulo E tal que $\rightarrow_{\mathcal{R}, E}$ é E -coerente, intuitivamente esse sistema de reescrita reduz representantes de uma mesma classe de equivalência módulo E para representantes de uma classe de equivalência módulo E .
- Obter um conjunto de E -unificadores de Γ , chamados *E -unificadores assimétricos*, que possui a propriedade de que para cada equação $s \stackrel{?}{=} t \in \Gamma$, os unificadores assimétricos preservam a forma normal do lado direito da equação com relação a relação de reescrita $\rightarrow_{\mathcal{R}, E}$, isto é, δ é dito E -unificador assimétrico de Γ se para cada $s \stackrel{?}{=} t \in \Gamma$, $(s \downarrow_{\mathcal{R}, E})\delta \downarrow_{\mathcal{R}, E} =_E (t \downarrow_{\mathcal{R}, E})\delta$.

Por fim, apresentaremos o procedimento proposto por Liu [18] que desenvolve um algoritmo (\mathcal{J}_{AXO}) que converte um conjunto completo de ACUN-unificadores de um problema Γ em um conjunto completo de ACUN-unificadores assimétricos de Γ .

Trabalhos Relacionados. Para o problema geral de unificação módulo $ACUNh$ os autores de [6] e [15] apresentam um algoritmo de unificação sobre a teoria equacional dos *Grupos Abelianos* com homomorfismo (AGh) que consiste em decompor o problema em uma unificação elementar com constantes sobre a teoria equacional (AGh) e um problema de unificação sintática. Porém de acordo com Liu [18], o algoritmos propostos em [6] e [15] resultam em um conjunto completo de unificadores redundante, isto é, o conjunto completo obtido não é minimal e possui uma quantidade expressiva de soluções comparáveis entre si, impossibilitando uma busca eficiente. Em contra partida, Ziqhiang propõe abordagens diferentes para unificação módulos $ACUNh$ e AGh , afirmando que gera um conjunto completo de unificadores minimal ou contendo uma quantidade inexpressiva de soluções que são comparáveis, tornando assim a busca mais eficiente.

Schulz [16] apresenta uma série de resultados discutindo a complexidade de decidir se um problema de unificação módulo uma teoria equacional regular E contendo as regras A (Associatividade),

C(Comutatividade) e AC ou ACUN(h), provando que quando existem símbolos de função não interpretados pelas teorias equacionais E e $ACUN(h)$ então o problema é NP-difícil. Enquanto Guo, Narendran e Wolfram em [11] provam que considerando apenas os problemas elementares com constantes a complexidade se torna polinomial.

Contribuições.

Neste trabalho apresentaremos com detalhes os métodos propostos por Guo, Narendran e Wolfram [11] e Liu [18]. Alguns resultados são enunciados ou admitidos nesses trabalhos sem apresentar demonstrações, mais especificamente:

- Na Seção 1.4, provamos resultados relacionados a propriedade de E -coerência (Teorema 1.1), transitividade de E -extensões conservativas (Proposição 1.5) e também sobre conjuntos completos de E -unificadores de E -extensões conservativas (Proposição 1.6).
- No Capítulo 2 demonstramos os teoremas sobre os processos de padronização (Proposição 2.1) e normalização (Proposição 2.2) de problemas de ACUN(h)-unificação; que teoria equacional $ACUN(h)$ tem uma decomposição; o Teorema 2.6 que associa cada problema elementar com constantes a um conjunto de sistemas de equações lineares com coeficientes em $\mathbb{Z}_2[h]$, [11].
- No Capítulo 3, desenvolvemos as propriedades de *terminação* e *correção* da regra de *purificação*, enunciadas em [18], que se baseia em transformar problemas de ACUN(h)-unificação em problemas ditos "puros", que são problemas cujas equações são do tipo $S =^? 0$ com S sendo uma "soma" de termos t cuja $raíz(t) \neq \oplus$ e que não ocorre símbolos de função \oplus, h fora da posição raiz. Esta regra ganhou um foco especial neste trabalho, devido a sua importância na solução de problemas de $ACUN(h)$ -unificação.
- Nos Capítulos 4 e 5, propusemos uma abordagem semelhante à de Liu [18] para a demonstração de *correção* e *completude* do algoritmo \mathcal{J}_{AXO} para $ACUN$ -unificação assimétrica. Flexibilizamos a definição de *violação*, isto é, o par (v, t) é uma *violação* de σ quando $v\sigma \downarrow_{\mathcal{R}, \mathcal{E}} \oplus t\sigma \downarrow_{\mathcal{R}, \mathcal{E}}$ é irreduzível com relação a $\rightarrow_{\mathcal{R}, \mathcal{E}}$, então admitimos que pares de restrição triviais $(0, w), (v, 0)$ não são violações. Além disso, criamos a relação de α -pertinência no conjunto de soluções \mathcal{Inst} e

um critério para α -pertinência, que foi amplamente utilizado para provar que basta considerar apenas os unificadores assimétricos idempotentes para computar um conjunto completo de $ACUN$ -unificadores assimétricos e que as soluções não se perdem na execução do algoritmo \mathcal{J}_{AXO} .

Organização.

Capítulo 1: Preliminares

Conceitos e definições básicas são introduzidos. As seções iniciais são referentes à teoria da reescrita e unificação, os principais conceitos e notações segue àquelas introduzidas por F. Baader e T. Nipkow em [4]. A Seção 1.4 introduz conceitos de reescrita módulo uma teoria equacional E , E -extensões conservativas, E -coerência, e os resultados sobre esses temas.

Capítulo 2: Unificação Módulo $ACUN$

Apresentaremos uma abordagem para resolução do problema da unificação módulo as teorias equacionais $ACUN(h)$, que são o foco deste trabalho. Na seção 2.1 estão as definições específicas sobre as teorias equacionais $ACUN(h)$ e seus respectivos sistemas de reescrita \mathcal{R}_\oplus e $\mathcal{R}_{\oplus h}$.

Na Seção 2.3 um método para resolver o problema de $ACUN(h)$ -unificação *elementar com constantes* proposto em [11], provando que para problemas elementares com constantes a complexidade de decidir a solubilidade é polinomial. Na seção 2.4 exibiremos a abordagem proposta por Schulz [16], para mostrar que para as teorias equacionais $ACUN(h)$ e para uma teoria equacional E *regular*, que possuem as identidades A , C ou AC , os problemas de unificação gerais são NP -difíceis.

Capítulo 3: Um algoritmo eficiente para $ACUNh$ - unificação

Apresentaremos o método proposto por Liu [18] para a solubilidade de $ACUN(h)$ -unificação considerando símbolos de função arbitrários.

Na seção 3.1 apresentaremos a regra de inferência *purificação*, que transforma um problema Γ de $ACUN(h)$ -unificação em um problema *purificado* Γ' que é uma $ACUNh$ -extensão conservativa de Γ . Além disso, provamos que a regra de purificação é correta e terminante, estas demonstrações foram omitidas em [18].

Na seção 3.2 apresentaremos o algoritmo para $ACUN(h)$ -unificação que é *correto, completo e terminante*, proposto em [18]. Mostraremos também que todo problema de $ACUN(h)$ -unificação tem um conjunto completo de $ACUN(h)$ -unificadores finito e para problemas elementares com constantes é unitário.

Capítulo 4: Unificação Assimétrica

Apresentaremos o conceito de *E-unificação assimétrica*, proposto inicialmente por Liu [18]. Na Seção 4.3.1, apresentamos o algoritmo \mathcal{J}_{AXO} , que converte um conjunto completo de $ACUN$ -unificadores padrões em um conjunto completo de $ACUN$ -unificadores assimétricos. Apresentamos provas detalhadas e exemplos que ilustram a aplicação dos resultados.

Capítulo 5: Correção e Completude de \mathcal{J}_{AXO}

Apresentamos uma demonstração da correção e completude de \mathcal{J}_{AXO} diferente da proposta em [18]. Para isto, criamos um critério de pertinência no conjunto das soluções que independe da escolha das variáveis, isto é, definimos α -pertinência para substituições, pois aproveitamos que em cada passo o algoritmo preserva idempotência em substituições.

A demonstração da correção e completude, dependem das propriedades de regularidade dos estados e idempotência, das regras de \mathcal{J}_{AXO} .

Capítulo 1

Preliminares

Neste capítulo estão os pré-requisitos. Serão abordadas as definições básicas sobre reescrita, unificação, assim como as definições para o algoritmo de solubilidade de uma teoria equacional. Veja mais detalhes em [4].

1.1 Termos, Substituições e Identidades

Definição 1.1 (Assinatura). *Uma assinatura Σ é um conjunto cujos elementos são chamados de símbolos de função e cada $f \in \Sigma$ está associado a um número natural n , a aridade de f . Dizemos que f é um símbolo de função n -ária de Σ , equivalentemente $f \in \Sigma^{(n)}$, quando $f \in \Sigma$ e n é a aridade de f , em particular os elementos de $\Sigma^{(0)}$ são chamados de símbolos constantes.*

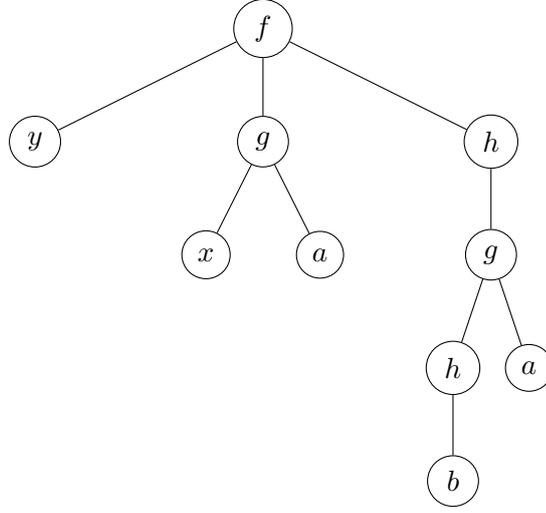
Definição 1.2 (Σ -Termo). *Sejam Σ uma assinatura e \mathcal{V} um conjunto infinito enumerável de variáveis disjunto de Σ . O conjunto $T(\Sigma, \mathcal{V})$ de todos os Σ -Termos sobre \mathcal{V} , é definido de forma indutiva:*

- $\mathcal{V} \subseteq T(\Sigma, \mathcal{V})$, i.e., toda variável é um termo
- Para todo $n \in \mathbb{N}$, $f \in \Sigma^{(n)}$ e $t_1, \dots, t_n \in T(\Sigma, \mathcal{V})$, têm-se que $f(t_1, \dots, t_n) \in T(\Sigma, \mathcal{V})$.

Denotaremos $\Sigma(t)$ como o multiconjunto de todos os símbolos de função ocorrendo no termo t .

Exemplo 1.1. *Sejam os símbolos de função $a, b \in \Sigma^{(0)}$, $f \in \Sigma^{(3)}$, $g \in \Sigma^{(2)}$, $h \in \Sigma^{(1)}$ e as variáveis $x, y \in \mathcal{V}$ então $t := f(x, g(x, a), h(g(h(b), a)))$ é um termo, e $\Sigma(t) = \{\{f, a, a, h, h, b, g, g\}\}$ é o*

multiconjunto de símbolos de função do termo t . Podemos representar o termo t como uma árvore, como abaixo:



(1.1)

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

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

- Se $s \in \mathcal{V} \cup \Sigma^{(0)}$, então $\mathcal{P}os(s) := \{\varepsilon\}$, onde ε denota a palavra vazia.
- Se $s = f(s_1, \dots, s_n)$, então

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

A posição ε é chamada posição raiz do termo s , e o símbolo de função ou de variável nesta posição é chamado de símbolo raiz de s , denotado por $raiz(s)$.

2. definimos a relação \leq sobre $\mathcal{P}os(t)$, da seguinte forma:

$$p \leq q \text{ se, e somente se, existe } l \text{ tal que } q = pl.$$

Quando $p \leq q$ dizemos que p é prefixo de q e quando $p \not\leq q$ e $q \not\leq p$ dizemos que p é paralela a q , denotado por $p \parallel q$

3. Defini-se indutivamente $len(\varepsilon) = 0$ e $len(ip) = 1 + len(p)$

4. O tamanho de um termo s é definido por $|s| := |\mathcal{Pos}(s)|$, isto é, $|s|$ é a cardinalidade de $\mathcal{Pos}(s)$ e a profundidade de um termo s é definido por: $\|s\| = \max\{len(p) \mid p \in \mathcal{Pos}(s)\}$.

Definição 1.4 (Σ -identidade). Seja Σ uma assinatura e \mathcal{V} um conjunto de variáveis. Uma Σ -identidade (ou Σ -equação) é um par $(s, t) \in T(\Sigma, \mathcal{V}) \times T(\Sigma, \mathcal{V})$. O lado direito (ld) é dado por t e o lado esquerdo (le) por s .

Notação: $s = t$. Quando a assinatura Σ é clara no contexto, $s = t$ será denotado simplesmente por identidade ou equação.

Definição 1.5 (Subtermos). Sendo s um Σ -termo, definiremos abaixo a noção de subtermo do termo s relacionado com as posições de s .

1. Para $p \in \mathcal{Pos}(s)$, o subtermo de s na posição p , denotado por $s|_p$, é definido por indução no comprimento de p :

$$s|_\varepsilon := s,$$

$$f(s_1, \dots, s_n)|_{iq} := s_i|_q.$$

Note que, para $p = iq$, onde $p, q \in \mathcal{Pos}(s)$ e $i \in \mathbb{N} \setminus \{0\}$, implica que s é da forma $s = f(s_1, \dots, s_n)$, com $i \leq n$.

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

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

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

Proposição 1.1. Sejam r, s e $t \in \mathcal{T}(\Sigma, \mathcal{V})$ então temos as seguintes propriedades para subtermos:

i. se $pq \in \mathcal{Pos}(s)$, então $s|_{pq} = (s|_p)|_q$

ii. Se $q \in \mathcal{Pos}(t)$ e $p \in \mathcal{Pos}(s)$, então

$$(s[t]_p)|_{pq} = t|_q$$

$$(s[t]_p)[r]_{pq} = s[t[r]_q]_p$$

iii. se $pq \in \mathcal{Pos}(s)$, então

$$(s[r]_{pq})|_p = (s|_p)[r]_q$$

$$(t[s]_{pq})[r]_p = t[r]_p$$

iv. Se $p, q \in \mathcal{Pos}(s)$ e $p \parallel q$, então

$$(s[t]_p)|_q = t|_q$$

$$(s[t]_p)[r]_q = (s[r]_q)[t]_p$$

v. Se v é uma variável e $p \in \mathcal{Pos}(S)$ então $\mathcal{Pos}(S[v]_p) \subseteq \mathcal{Pos}(S)$.

Demonstração. Aplica-se uma indução sobre o comprimento das posições. □

Definição 1.6 (Variáveis de um termo). Definimos $\mathcal{Var}(s)$ como o conjunto de variáveis ocorrendo em s , i.e.

$$\mathcal{Var}(s) := \{x \mid x \in \mathcal{V} \text{ e existe } p \in \mathcal{Pos}(s) \text{ tal que } s|_p = x\}.$$

Quando $s|_p$ é uma variável, $p \in \mathcal{Pos}(s)$ é chamada de posição variável. Seja s um termo, quando $\mathcal{Var}(s) = \emptyset$ dizemos que s é um termo básico. Podemos estender a definição de conjunto de variáveis ocorrendo em um termo s , da seguinte forma. Sendo U um conjunto de termos, então definimos o conjunto de variáveis ocorrendo nos termos de U , como se segue: $\mathcal{Var}(U) := \bigcup_{s \in U} \mathcal{Var}(s)$.

Seja (s, t) um par de termos definimos o conjunto das variáveis ocorrendo no par (s, t) por: $\mathcal{Var}(s, t) := \mathcal{Var}(s) \cup \mathcal{Var}(t)$. Sejam $\Gamma_1, \dots, \Gamma_n$ conjuntos de termos ou conjunto de pares de termos, definimos o conjunto das variáveis ocorrendo nos conjuntos $\Gamma_1, \dots, \Gamma_n$ por:

$$\mathcal{Var}(\Gamma_1, \dots, \Gamma_n) := \bigcup_{i \in \{1, \dots, n\}} \mathcal{Var}(\Gamma_i)$$

Definição 1.7 (Substituição). Seja Σ uma assinatura e \mathcal{V} um conjunto infinito enumerável de variáveis. Uma substituição é uma função $\sigma : \mathcal{V} \rightarrow T(\Sigma, \mathcal{V})$, tal que $x\sigma \neq x$ apenas para um número finito de variáveis $x \in \mathcal{V}$. Este conjunto (finito) de variáveis é chamado domínio de σ e é definido por, $\text{Dom}(\sigma) := \{x \in \mathcal{V} \mid x\sigma \neq x\}$.

Uma vez que definimos o domínio da substituição σ definiremos o conjunto das imagens de σ da seguinte forma, $\text{Im}(\sigma) := \{x\sigma \mid x \in \text{Dom}(\sigma)\}$.

Assim seja σ uma substituição, diremos que σ designa x em t , equivalentemente $[x \mapsto t] \in \sigma$ se, e somente se, $x \in \text{Dom}(\sigma)$ e $x\sigma = t$. Então podemos identificar a substituição σ com o conjunto de suas designações da seguinte forma, $\sigma = \{x \mapsto x\sigma \mid x \in \text{Dom}(\sigma)\}$.

Seja $W \subseteq \mathcal{V}$, definimos a substituição $\sigma|_W$, chamada de restrição de σ a W pelo conjunto de designações, $\sigma|_W := \{x \mapsto x\sigma \mid x \in \text{Dom}(\sigma) \cap W\}$ Podemos estender uma substituição σ para a uma aplicação $\hat{\sigma} : T(\Sigma, \mathcal{V}) \rightarrow T(\Sigma, \mathcal{V})$ da seguinte forma:

- $x\hat{\sigma} = x\sigma$, se $x \in \mathcal{V}$.
- $f(s_1, \dots, s_n)\hat{\sigma} := f(s_1\hat{\sigma}, \dots, s_n\hat{\sigma})$.

Por abuso de notação, utilizaremos sempre a extensão da substituição, exceto quando explicitado o contrário. Vamos denotar por $\text{Sub } T(\Sigma, \mathcal{V})$, o conjunto de todas as substituições $\hat{\sigma} : T(\Sigma, \mathcal{V}) \rightarrow T(\Sigma, \mathcal{V})$ e quando a Σ, \mathcal{V} forem omitidas no contexto, denotaremos apenas por Sub .

Definição 1.8 (Composição de Substituições). Sendo σ e θ duas substituições, definimos a substituição composição $\sigma\theta$ como a composição usual das funções σ e θ , isto é, $x(\sigma\theta) = (x\sigma)\theta$ para todo $x \in \mathcal{V}$.

Assim herdando a propriedade associatividade da composição de funções e obtendo $\text{Dom}(\sigma\theta) \subseteq \text{Dom}(\sigma) \cup \text{Dom}(\theta)$, concluindo de fato que a composição de substituições é uma substituição.

Definição 1.9 (Substituição Mais Geral). Sejam Σ uma assinatura, \mathcal{V} um conjunto infinito contável de variáveis. Dizemos que,

- σ é mais geral que θ , denotado por $\sigma \lesssim \theta$, quando $\exists \gamma \in \text{Sub}$, tal que $\theta = \sigma\gamma$.
- σ é equivalente a θ , denotado por $\sigma \approx \theta$, quando $\sigma \lesssim \theta$ e $\theta \lesssim \sigma$.

Definição 1.10 (Renomeamento de Variáveis de um Termo). Sejam $t \in T(\Sigma, \mathcal{V})$ e $\alpha : \mathcal{V} \rightarrow \mathcal{V}$ uma substituição bijetiva. Dizemos que α é um renomeamento das variáveis de t se, e somente se, $\text{Im}(\alpha) \cap (\text{Var}(t) \setminus \text{Dom}(\alpha)) = \emptyset$.

Exemplo 1.2. Seja $f \in \Sigma^{(2)}$, $g \in \Sigma^{(1)}$, $x, y, z \in \mathcal{V}$ variáveis e o termo $t = f(x, g(y))$. Tome α uma substituição definida por $\alpha = \{x \mapsto z, y \mapsto x\}$ Então $t\alpha = f(x, g(y))\alpha = f(x\alpha, g(y\alpha)) = f(z, g(x))$. Note que $\text{Im}(\alpha) = \{x, z\}$, $\text{Dom}(\alpha) = \{x, y\}$ e $\text{Var}(t) = \{x, y\}$.

Portanto $\text{Im}(\alpha) \cap (\text{Var}(t) \setminus \text{Dom}(\alpha)) = \emptyset$, logo α é um renomeamento de variáveis de t . Note que α não é um renomeamento de variáveis de $f(x, g(z))$.

Definição 1.11 (Renomeamento de Variáveis de uma Substituição). *Sejam $\alpha, \sigma : \mathcal{V} \rightarrow T(\Sigma, \mathcal{V})$ substituições. α é dito renomeamento de variáveis de σ se, e somente se, para todo $x \in \text{Dom}(\sigma)$, α é um renomeamento das variáveis de $x\sigma$.*

Proposição 1.2. *Sejam $\alpha, \sigma : \mathcal{V} \rightarrow T(\Sigma, \mathcal{V})$ substituições. Então α é um renomeamento de variáveis de σ se, e somente se,*

1- $\text{Im}(\alpha) \subset \mathcal{V}$ e α é bijetiva.

2- $\text{Im}(\alpha) \cap (\text{Var}(\text{Im}(\sigma)) \setminus \text{Dom}(\alpha)) = \emptyset$.

Demonstração. (\Rightarrow) Tome α renomeamento de variáveis de σ , pela sua definição $\text{Im}(\alpha) \subset \mathcal{V}$ e $|\text{Im}(\alpha)| = |\text{Dom}(\alpha)|$, então basta provar que, $\text{Im}(\alpha) \cap (\text{Var}(\text{Im}(\sigma)) \setminus \text{Dom}(\alpha)) = \emptyset$ Como para todo $x \in \text{Dom}(\alpha)$, α é um renomeamento de $x\sigma$ então: $\text{Im}(\alpha) \cap (\text{Var}(x\sigma) \setminus \text{Dom}(\alpha)) = \emptyset$. Sabendo que para quaisquer conjuntos A, C e qualquer família de conjuntos $\{B_x : x \in \mathcal{I}\}$ temos, $\bigcup_{x \in \mathcal{I}} (A \cap (B_x \setminus C)) = A \cap (\bigcup_{x \in \mathcal{I}} B_x \setminus C)$, em particular, fazendo $A = \text{Im}(\alpha)$, $\{B_x = \text{Var}(x\sigma) : x \in \text{Dom}(\sigma)\}$ e $C = \text{Dom}(\alpha)$, temos pela equação acima,

$$\emptyset = \bigcup_{x \in \text{Dom}(\sigma)} (\text{Im}(\alpha) \cap (\text{Var}(x\sigma) \setminus \text{Dom}(\alpha))) = \text{Im}(\alpha) \cap \left(\bigcup_{x \in \text{Dom}(\sigma)} \text{Var}(x\sigma) \setminus \text{Dom}(\alpha) \right)$$

Como $\text{Var}(\text{Im}(\sigma)) = \bigcup_{x \in \text{Dom}(\sigma)} \text{Var}(x\sigma)$ obtemos, $\text{Im}(\alpha) \cap (\text{Var}(\text{Im}(\sigma)) \setminus \text{Dom}(\sigma)) = \emptyset$. \square

Então um renomeamento de variáveis de uma substituição será denotada apenas por renomeamento de variáveis.

Definição 1.12 (Renomeamento de variáveis livre de $W \subset \mathcal{V}$). *Sejam α, σ duas substituições. Dizemos que α é um de variáveis de σ livre em $W \subset \mathcal{V}$ se, e somente se, α é um renomeamento de variáveis de σ e $\text{Im}(\alpha) \cap W = \emptyset$.*

Definição 1.13 (Renomeamento Inverso). *Seja α um renomeamento de variáveis, denotamos a substituição $\alpha^{-1} = \{y \mapsto x \mid x \mapsto y \in \alpha\}$ como a o renomeamento inverso de α .*

OBS: α^{-1} definido acima é um renomeamento de variáveis e caso $\text{Dom}(\alpha) \cap \text{Im}(\alpha) = \emptyset$ temos $\alpha\alpha^{-1} = \alpha^{-1}$ e $\alpha^{-1}\alpha = \alpha$.

Proposição 1.3. *Seja α um renomeamento de variáveis. Se α é livre em $W \subset \mathcal{V}$ e $\text{Dom}(\alpha) \subseteq W$, então $\alpha\alpha^{-1}|_W = \text{id}_W$.*

Demonstração. Suponha α renomeamento de variáveis livre em $W \subset \mathcal{V}$, então $\text{Im}(\alpha) \cap W = \emptyset$, com $\text{Im}(\alpha) = \text{Dom}(\alpha^{-1})$, implicando que $\text{Dom}(\alpha^{-1}) \cap W = \emptyset$. Assim, por $\alpha\alpha^{-1} = \alpha^{-1}$ temos que $\alpha\alpha^{-1}|_W = \alpha^{-1}|_W = \text{id}_W$. \square

Proposição 1.4. *Seja α um renomeamento de variáveis de uma substituição σ , então para todo $x \in \text{Dom}(\sigma)$, $x\sigma\alpha^{-1} = x\sigma$ e α^{-1} é um renomeamento de variáveis de $\sigma\alpha$.*

Demonstração. (1) Tome $x \in \text{Dom}(\sigma)$ e $w \in \text{Var}(x\sigma)$. Suponha que $w \notin \text{Dom}(\alpha)$, então $w \in \text{Var}(x\sigma) \setminus \text{Dom}(\alpha)$, logo por α ser um renomeamento de variáveis de σ , implica que α é um renomeamento de variáveis de $x\sigma$, então $\text{Im}(\alpha) \cap (\text{Var}(x\sigma) \setminus \text{Dom}(\alpha)) = \emptyset$, portanto $w \notin \text{Im}(\alpha)$, equivalentemente, $w \notin \text{Dom}(\alpha^{-1})$, logo podemos concluir que, $w\alpha\alpha^{-1} = w\alpha^{-1} = w$.

Por outro lado, se $w \in \text{Dom}(\alpha)$, então pela própria definição de renomeamento inverso temos, $w\alpha\alpha^{-1} = w$. Como substituições agem apenas sobre as variáveis, temos que $x\sigma\alpha\alpha^{-1} = x\sigma$.

(2) Tome $x \in \text{Dom}(\sigma\alpha)$ qualquer, vamos provar que $\text{Im}(\alpha^{-1}) \cap (\text{Var}(x\sigma\alpha) \setminus \text{Dom}(\alpha^{-1})) = \emptyset$ e assim conclui-se que α^{-1} é um renomeamento de variáveis $\sigma\alpha$. Suponha $w \in \text{Var}(x\sigma\alpha) \setminus \text{Dom}(\alpha^{-1})$ qualquer, então por $\text{Im}(\alpha) = \text{Dom}(\alpha^{-1})$ temos que $w \notin \text{Im}(\alpha)$, como existe um $v \in \text{Var}(x\sigma)$ onde $v\alpha = w$ e $w \notin \text{Im}(\alpha)$ então $v = w$ e portanto $w\alpha = w$, equivalentemente, $w \notin \text{Dom}(\alpha)$, implicando que $w \notin \text{Im}(\alpha^{-1})$. Assim concluímos que $\text{Im}(\alpha^{-1}) \cap (\text{Var}(x\sigma) \setminus \text{Dom}(\alpha^{-1})) = \emptyset$. \square

Corolário 1.1. *Se $t \in T(\Sigma, \mathcal{V})$ e α é um renomeamento das variáveis de t então $t\alpha\alpha^{-1} = t$*

Demonstração. De fato, basta tomar a substituição $\sigma = \{x \mapsto t\}$ então α é um renomeamento de t , equivalentemente, α é um renomeamento de variáveis de σ e portanto pela proposição anterior temos $x\sigma\alpha\alpha^{-1} = x\sigma$, então $t\alpha\alpha^{-1} = t$. \square

1.2 Álgebras, Homomorfismos e Congruências

Dada uma assinatura Σ , uma álgebra é uma interpretação de todos os símbolos de função em Σ .

Definição 1.14 (Σ -álgebra). *Seja Σ uma assinatura. Uma Σ -álgebra \mathcal{A} consiste de*

- i. um domínio A , e
- ii. para cada $n \in \mathbb{N}$ e cada símbolo de função $f \in \Sigma^{(n)}$, é associado um mapeamento $f^{\mathcal{A}}: A^n \rightarrow A$.

Se a assinatura Σ é clara no contexto ou irrelevante, denotaremos uma Σ -álgebra simplesmente por álgebra.

Definição 1.15 (Σ -homomorfismo). *Seja Σ uma assinatura, e sejam \mathcal{A}, \mathcal{B} Σ -álgebras. Um Σ -homomorfismo $\phi: \mathcal{A} \rightarrow \mathcal{B}$ é um mapeamento de A em B tal que para todo $n \in \mathbb{N}$, $f \in \Sigma^{(n)}$, e $a_1, \dots, a_n \in A$ tem-se que*

$$\phi(f^{\mathcal{A}}(a_1, \dots, a_n)) = f^{\mathcal{B}}(\phi(a_1), \dots, \phi(a_n))$$

Definição 1.16 (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 fechado para Σ -operações, isto é, para todos $n \in \mathbb{N}$, $f \in \Sigma^{(n)}$, e todo $a_1 \equiv b_1, \dots, a_n \equiv b_n$ em A tem-se que*

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

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 para cada $n \in \mathbb{N}$, interpreta os símbolos, $f \in \Sigma^{(n)}$ como

$$f^{\mathcal{A}/\equiv}([a_1]_{\equiv}, \dots, [a_n]_{\equiv}) \equiv [f^{\mathcal{A}}(a_1, \dots, a_n)]_{\equiv}$$

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

Definição 1.17 (Σ -álgebra de termos). *Seja Σ uma assinatura e \mathcal{V} um conjunto de variáveis disjunto de Σ . a Σ -álgebra de termos $\mathcal{T}(\Sigma, \mathcal{V})$ tem como domínio $T(\Sigma, \mathcal{V})$ e para cada $n \in \mathbb{N}$, interpreta os símbolos de função $f \in \Sigma^{(n)}$ da seguinte forma:*

$$\begin{aligned} f^{\mathcal{T}(\Sigma, \mathcal{V})} : T(\Sigma, \mathcal{V})^n &\longrightarrow T(\Sigma, \mathcal{V}) \\ (t_1, \dots, t_n) &\longmapsto f(t_1, \dots, t_n) \end{aligned}$$

1.3 Classes Equacionais

Uma Σ -identidade é um par $s = t$ de termos em $T(\Sigma, \mathcal{V})$, para um conjunto infinito enumerável de variáveis \mathcal{V} . Intuitivamente, uma identidade é “válida” em uma Σ -álgebra \mathcal{A} se para todas as possíveis maneiras de substituir as variáveis em s, t por elementos de A obtemos o mesmo elemento em A . A definição formal abaixo faz uso do fato que um dado mapeamento de variáveis em elementos de A pode ser unicamente estendido a um homomorfismo.

Definição 1.18 (Validade). *Dizemos que uma Σ -identidade $s = t$ vale na Σ -álgebra \mathcal{A} ($\mathcal{A} \models s = t$) se, e somente se, para todo homomorfismo $\phi : T(\Sigma, \mathcal{V}) \rightarrow \mathcal{A}$ tem-se que $\phi(s) = \phi(t)$.*

Definição 1.19 (Modelo). *Seja Σ uma assinatura e E um conjunto de Σ -identidades.*

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

Definição 1.20 (Teoria Equacional). *Seja E um conjunto de Σ -identidades.*

- i. *A identidade $s = t$ é uma consequência semântica de E ($E \models s = t$) sse $s = t$ é válida em todos os modelos de E , isto é, para todo \mathcal{A} , tem-se que $s = t$ é válido em \mathcal{A} .*
- ii. *A relação $\approx_E := \{(s, t) \in T(\Sigma, \mathcal{V})^2 \mid E \models s = t\}$ é chamada de teoria equacional induzida por E .*
- iii. *O conjunto de identidades E é chamado de trivial se, e somente se, $\approx_E = T(\Sigma, \mathcal{V})^2$.*

Definição 1.21 (Congruência módulo E). *Seja E um conjunto de identidades. Denote por Σ_E o conjunto de todos os símbolos de função ocorrendo em E e por $=_E$ a menor congruência em $T(\Sigma, \mathcal{V})$ gerada por E , isto é, a menor relação de equivalência contendo E que é fechada para substituições e compatível com Σ -contexto: para toda substituição σ , para todo termo t e $p \in \text{Pos}(t)$, se $u =_E v$ então $t[u\sigma]_p =_E t[v\sigma]_p$.*

Exemplo 1.3. *A teoria equacional ACUN é dada pelas identidades:*

$$\left\{ \begin{array}{ll} x \oplus (y \oplus z) = (x \oplus y) \oplus z & (\text{Assoc.}) \quad x \oplus 0 = x \quad (\text{Unidade}) \\ x \oplus y = y \oplus x & (\text{Comut.}) \quad x \oplus x = 0 \quad (\text{Nilpotencia}) \end{array} \right.$$

Definição 1.22 (E-unificáveis). *Seja E um conjunto de Σ -identidades. Dois termos s e t são chamados de E-unificáveis se existe uma substituição σ tal que $\sigma =_E t\sigma$. Tal substituição é chamada de E-unificador de s, t .*

Definição 1.23 (Substituição Mais Geral Módulo E). *Sejam Σ uma assinatura, \mathcal{V} um conjunto infinito contável de variáveis, um conjunto E de Σ -identidades, $W \subseteq \mathcal{V}$ e $\sigma, \theta \in \text{SubT}(\Sigma, \mathcal{V})$. Dizemos que,*

- σ é mais geral que θ sobre W módulo E . Denotado por:

$$\sigma|_W \lesssim_E \theta|_W \Leftrightarrow \exists \gamma \text{ substituição. } \theta|_W =_E \sigma\gamma|_W.$$

- σ é equivalente a θ sobre W módulo E . Denotado por,

$$\sigma|_W \approx_E \theta|_W \Leftrightarrow \sigma|_W \lesssim_E \theta|_W \text{ e } \theta|_W \lesssim_E \sigma|_W$$

OBS: Quando $W = \mathcal{V}$ então omitiremos “sobre W ” e “ $|_W$ ” das notações.

1.4 Sistemas de Reescrita de Termos e Unificação

Definição 1.24 (Regra de reescrita). *Sejam Σ uma assinatura, \mathcal{V} um conjunto infinito enumerável de variáveis. Uma regra de reescrita é um par ordenado e orientado $l \rightarrow r$, onde $l, r \in T(\Sigma, \mathcal{V})$, $l \notin \mathcal{V}$ e $\text{Var}(r) \subseteq \text{Var}(l)$. Definimos l como o lado esquerdo (le) e r como o lado direito (ld) de $l \rightarrow r$.*

Definição 1.25 (Sistema de Reescrita de Termos). *Um sistema de reescrita de termos (SRT), é um conjunto R de regras de reescrita.*

Definição 1.26 (Relação de Redução de Termos). *Seja \mathcal{R} um sistema de reescrita de termos, \mathcal{R} define uma relação de redução de termos $\rightarrow_{\mathcal{R}}$ sobre $T(\Sigma, \mathcal{V})$ da seguinte forma:*

$$s \rightarrow_{\mathcal{R}} t \Leftrightarrow \exists l \rightarrow r \in R, p \in \text{Pos}(s), \sigma \in \text{Sub}, \text{tais que } s|_p = l\sigma \text{ e } t = s[r\sigma]_p$$

Então dizemos que o sistema de regras de reescrita R é terminante (confluente) se, e somente se, a relação de redução de termos $\rightarrow_{\mathcal{R}}$ é terminante (confluente).

Definição 1.27 (Relação de Reescrita). *Uma relação \rightarrow sobre $T(\Sigma, \mathcal{V})$ é uma relação de reescrita se, e somente se, \rightarrow é uma relação fechada sobre substituição e compatível sobre Σ -operações.*

Definição 1.28 (Relação de E - Redução). *Seja E um conjunto de Σ -identidades, definimos a relação $\rightarrow_E \subseteq \mathcal{T}(\Sigma, \mathcal{V}) \times \mathcal{T}(\Sigma, \mathcal{V})$ da seguinte forma,*

$$s \rightarrow_E t \Leftrightarrow \exists u = v \in E, p \in \text{Pos}(s), \sigma \in \text{Sub tais que } s|_p = u\sigma \text{ e } t = s[v\sigma]_p$$

Então dizemos que $s =_E t$ se, e somente se, $s \leftrightarrow_E^ t$.*

Observação 1.1. *Seja E um conjunto de Σ identidades, então a dada \approx_E a teoria equacional induzida por E e \rightarrow_E a relação de E -redução, temos pelo Teorema de Birkhof em [4] que $\approx_E = \leftrightarrow_E^*$.*

Definição 1.29 (Problema de Unificação). *Um problema de unificação é um conjunto finito $\Gamma := \{s_1 =^? t_1, \dots, s_n =^? t_n\}$ onde s_i, t_i são termos. Um unificador sintático de Γ , é uma substituição σ tal que para todo $i \in \{1, \dots, n\}$, $s_i\sigma = t_i\sigma$. $\mathcal{U}(\Gamma)$ denota o conjunto de todos os unificadores sintáticos de Γ .*

Uma substituição σ é chamada de unificador sintático mais geral (mgu) de Γ se, e somente se, temos:

- $\sigma \in \mathcal{U}(\Gamma)$
- $\forall \gamma \in \mathcal{U}(\Gamma). \sigma \lesssim \gamma$

Exemplo 1.4. *Seja $\Gamma = \{f(x, g(y)) =^? f(g(y), g(f(a, w)))\}$ um problema de unificação.*

*Note que $\sigma = \{x \mapsto g(f(a, w)), y \mapsto f(a, w)\}$ é um unificador sintático de Γ , basta aplicar σ em ambos os lados da equação de Γ , obtendo $f(g(f(a, w)), g(f(a, w)))$. Essa substituição também é um mgu, obtido pelo algoritmo de unificação sintática, *Unify*, descrito em [4].*

1.4.1 Reescrita Módulo Teorias Equacionais

Métodos de reescrita são amplamente utilizados em muitas áreas da computação e matemática, infelizmente o método de completamento de *Knuth-Bendix* é ineficiente quando adentramos no campo das teorias equacionais, e.g., quando incluímos a *comutatividade* como uma regra de reescrita, destruimos a terminação do sistema de reescrita, causando o método de completamento de *Knuth-Bendix* falhar. Quando se faz necessário de um axioma com tal problema em uma teoria equacional, para mantermos um sistema de reescrita convergente nessa teoria equacional, devemos generalizar alguns conceitos de reescrita, casamento e unificação com respeito à teoria equacional dada.

Definição 1.30 (Relação de Reescrita \mathcal{R}, E). Considere o conjunto \mathcal{R} de regras de reescrita e o conjunto de equações E . A relação de reescrita \mathcal{R}, E , é a relação $\rightarrow_{\mathcal{R}, E}$ definida por:

$$s \rightarrow_{\mathcal{R}, E} t \Leftrightarrow \exists l \rightarrow r \in \mathcal{R}, p \in \text{Pos}(s), \sigma \in \text{Subs}. s|_p =_E l\sigma \text{ e } t = s[r\sigma]_p$$

Definição 1.31 (Relação Reescrita \mathcal{R}/E). Considere o conjunto \mathcal{R} de regras de reescrita e o conjunto de equações E . A relação de reescrita \mathcal{R}/E , é a relação $\rightarrow_{\mathcal{R}/E}$ definida por:

$$\rightarrow_{\mathcal{R}/E} := =_E \circ \rightarrow_{\mathcal{R}} \circ =_E$$

O sistema de reescrita \mathcal{R} é dito convergente módulo E se, e somente se, $\rightarrow_{\mathcal{R}/E}$ é um sistema de reescrita confluyente e terminante sobre $\mathcal{T}(\Sigma, \mathcal{V})/_E$.

Definição 1.32 (Forma normal). Um termo t está na forma normal (w.r.t \mathcal{R}, E) se não existe um termo s tal que $t \rightarrow_{\mathcal{R}, E} s$. Se $t \xrightarrow{*}_{\mathcal{R}, E} s$ e s está na forma normal então s é uma forma normal de t . Quando esta forma normal é única (\mathcal{R} é convergente módulo E), denota-se $(t \downarrow_{\mathcal{R}, E})$.

Observação 1.2. Pelas definições acima, é possível verificar que $\rightarrow_{\mathcal{R}, E} \subseteq \rightarrow_{\mathcal{R}/E}$, então no caso em que $\rightarrow_{\mathcal{R}/E}$ for terminante, implica que $\rightarrow_{\mathcal{R}, E}$ é terminante.

Definição 1.33 (Coerente módulo E). Seja $E' = E'' \dot{\cup} E$ uma teoria equacional onde \mathcal{R} é um sistema de reescrita convergente obtido orientado as identidades de E'' . Dizemos que $\rightarrow := \rightarrow_{\mathcal{R}, E}$ é E -coerente, desde que,

$\forall t_1, t_2, t_3$. se $t_1 \rightarrow_{\mathcal{R}, E} t_2$ e $t_1 =_E t_3$, então existem t_4, t_5 tais que $t_4 =_E t_5$, $t_3 \rightarrow^+ t_5$ e $t_2 \rightarrow^* t_4$.

1.4.2 Unificação Módulo Teorias Equacionais

Seja E um conjunto de Σ -identidades sobre uma assinatura Σ . Denota-se por Σ_E a assinatura de E , isto é, o conjunto de todos os símbolos de função que ocorrem em E .

Definição 1.34 (Problema de E -Unificação). Um problema de E -unificação sobre Σ é um conjunto finito de equações $\Gamma = \{u_1 =_E^? v_1, \dots, u_n =_E^? v_n\}$ entre Σ -termos com variáveis em \mathcal{V} . Um E -Unificador (ou uma E -solução) de Γ é uma substituição σ tal que $u_i\sigma =_E v_i\sigma$ para $i = 1, \dots, n$. O conjunto de todos os E -Unificadores de Γ é denotado por $\mathcal{U}_E(\Gamma)$ e Γ é chamado E -Unificável quando $\mathcal{U}_E(\Gamma) \neq \emptyset$.

Definição 1.35 (Classe dos Problemas de E-Unificação). *Seja Γ um problema de E-unificação sobre a assinatura Σ . Dizemos que:*

- Γ é um problema de E-unificação elementar se, e somente se, $\Sigma = \Sigma_E$.
- Γ é um problema de E-unificação elementar com constantes se, e somente se, $\Sigma \setminus \Sigma_E$ tem apenas símbolos constantes.
- Γ é um problema de E-unificação geral se, e somente se, $\Sigma \setminus \Sigma_E$ tem símbolos de função arbitrários.

Definição 1.36 (Conjunto Completo de E-Unificadores). *Seja Γ um problema de E-unificação. O conjunto completo de E-unificadores de Γ , denotado por $\mathcal{C}_E(\Gamma)$, é um conjunto de todos E-unificadores de Γ tais que*

- $\forall \sigma \in \mathcal{C}_E(\Gamma), \sigma \sigma := \sigma$
- $\forall \theta \in \mathcal{U}_E(\Gamma). \exists \sigma \in \mathcal{C}_E(\Gamma). \sigma|_{\text{var}(\Gamma)} \lesssim_E \theta|_{\text{var}(\Gamma)}$.

Dizemos que $\mathcal{C}_E(\Gamma)$ é minimal, desde que, $\forall \sigma, \theta \in \mathcal{C}_E(\Gamma). \sigma \neq \theta$ então nenhum é mais geral que o outro.

Definição 1.37 (Tipos de E-unificação). *Seja E um conjunto de Σ -identidades, dizemos que E é uma teoria equacional*

- Unitária se, e somente se, todo problema Γ de E-unificação possui um conjunto completo minimal de E-unificadores com cardinalidade ≤ 1 .
- Finitária se, e somente se, todo problema Γ de E-unificação possui um conjunto completo minimal de E-unificadores com cardinalidade finita.
- Infinitária se, e somente se, todo problema Γ de E-unificação possui um conjunto completo minimal e existe um problema Γ' de E-unificação que possui um conjunto completo minimal de E-unificadores que tem cardinalidade infinita.

Definição 1.38 (Decomposição). *Sejam Σ é uma assinatura, $E' = E'' \dot{\cup} E$ um conjunto de Σ -identidades, onde colocando uma orientação em cada identidade de E'' obtemos \mathcal{R} um conjunto de regras de reescrita. Denotamos a tripla (Σ, \mathcal{R}, E) de uma decomposição da teoria equacional (Σ, E') se \mathcal{R} e E possuem as seguintes propriedades:*

- (i) *E é uma teoria equacional que preserva variável, i.e., para cada $s = t \in E$ temos $\mathcal{V}ar(s) = \mathcal{V}ar(t)$.*
- (ii) *E' possui um algoritmo de unificação completo e finitário, i.e., existe um algoritmo de unificação módulo E' que produz um conjunto finito e completo de E' - unificadores.*
- (iii) *\mathcal{R} é convergente módulo E , i.e., a relação $\rightarrow_{\mathcal{R}/E}$ é terminante e confluyente*
- (iv) *$\rightarrow_{\mathcal{R},E}$ é E -coerente.*

Observação 1.3. *Se (Σ, \mathcal{R}, E) é uma decomposição da teoria equacional (Σ, E') , denotaremos abusando da notação $E' := \mathcal{R} \dot{\cup} E$.*

Vamos criar um critério mais simples para garantir que $\rightarrow_{\mathcal{R},E}$ é E -coerente. Seja $E' = E'' \dot{\cup} E$ um conjunto de Σ -identidades, onde E'' possui uma orientação para cada uma de suas equações, obtendo \mathcal{R} um sistema de reescrita convergente módulo E .

Teorema 1.1. *$\rightarrow_{\mathcal{R},E}$ é E -coerente se, e somente se, para todo s, t termos,*

$$s =_E t \Rightarrow s \downarrow_{\mathcal{R},E} =_E t \downarrow_{\mathcal{R},E}$$

Demonstração. Sejam s, t termos tal que $s =_E t$, vamos denotar $\rightarrow := \rightarrow_{\mathcal{R},E}$.

(\Rightarrow): Suponha que \rightarrow seja E -coerente, se s está em sua forma normal módulo E então pela nossa hipótese t está em sua forma normal módulo E e o resultado segue.

Suponha que $s \rightarrow s'$. Pela E -coerência existem, s_1, t_1 tais que

$$\begin{array}{ccc} s & =_E & t \\ \downarrow & & \downarrow^+ \\ s' & \xrightarrow{*} s_1 & =_E t_1 \end{array}$$

Se s' está em sua forma normal então $s' =_E s_1$ e t_1 está em sua forma normal, caso s_1 seja redutível, podemos usar uma indução bem fundada sobre \rightarrow , pois \rightarrow é terminante. E assim segue o resultado.

(\Leftarrow): Seja s' tal que $s \rightarrow s'$, suponha por absurdo que para todos s'', t' termos tais que se $s' \rightarrow^* s''$ e $t \rightarrow t'$ então $s'' \neq_E t'$. Como s é redutível, então pela nossa hipótese, t é redutível, pois caso contrário $s =_E t =_E t \downarrow$ implica que $s =_E s \downarrow$.

Logo $s' \leftarrow s \rightarrow s \downarrow^+$ e $t \rightarrow^+ t'$. Como \rightarrow é confluyente e $s \downarrow$ está em sua forma normal, temos que $s' \rightarrow^* s \downarrow$ e como por hipótese $s =_E t$ implica que $s \downarrow =_E t \downarrow$ temos o seguinte diagrama:

$$\begin{array}{ccc} s & =_E & t \\ \downarrow & & \downarrow^+ \\ s' \xrightarrow{*} s \downarrow & =_E & t \downarrow \end{array}$$

E portanto \rightarrow é E -coerente. □

Definição 1.39 (E -extensão conservativa). *Seja E um conjunto de Σ -identidades e Γ um problema de E -unificação. Dizemos que Γ' é uma E -extensão conservativa de Γ se, e somente se, para cada E -unificador σ de Γ' , σ é um E -unificador de Γ e para cada σ E -unificador de Γ , existe uma substituição γ com as seguintes propriedades*

- $\text{Dom}(\gamma) \subset \text{Var}(\Gamma') \setminus \text{Var}(\Gamma)$
- $\sigma\gamma$ é um E -unificador de Γ'

Quando for claro a teoria equacional E ou não houver ambiguidades, iremos denotar E -extensão conservativa apenas por extensão conservativa.

Provaremos algumas propriedades importantes sobre E -extensões conservativas, dentre elas a transitividade quando as variáveis de Γ são preservadas na E -extensão conservativa.

Proposição 1.5 (Transitividade de E -extensões conservativas). *Sejam Γ_1, Γ_2 e Γ_3 problemas de E -unificação tais que Γ_3 é uma E -extensão conservativa de Γ_2 e Γ_2 é uma E -extensão conservativa de Γ_1 , se $\text{Var}(\Gamma_1) \subseteq \text{Var}(\Gamma_2) \subseteq \text{Var}(\Gamma_3)$ então, Γ_3 é uma E -extensão conservativa de Γ_1 .*

Demonstração. Seja σ um E -unificador de Γ_3 , logo por Γ_3 ser uma E -extensão conservativa de Γ_2 , implica que, σ é um E -unificador de Γ_2 e como Γ_2 é uma E -extensão conservativa de Γ_1 temos que σ é um E -unificador de Γ_1 , assim todo E -unificador de Γ_3 é um E -unificador de Γ_1 .

Por outro lado, tome σ um E -unificador de Γ_1 , então existe θ uma substituição tal que $\sigma\theta$ é um E -unificador de Γ_2 e $\text{Dom}(\theta) \subseteq \text{Var}(\Gamma_2) \setminus \text{Var}(\Gamma_1)$, porém Γ_3 é uma E -extensão conservativa de Γ_2 e

portanto existe uma substituição γ tal que $\sigma\theta\gamma$ é um E -unificador de Γ_3 e $\text{Dom}(\gamma) \subseteq \mathcal{V}\text{ar}(\Gamma_3) \setminus \mathcal{V}\text{ar}(\Gamma_2)$. Note que, $\text{Dom}(\theta\gamma) \subseteq \text{Dom}(\theta) \cup \text{Dom}(\gamma) \subseteq \mathcal{V}\text{ar}(\Gamma_3) \setminus \mathcal{V}\text{ar}(\Gamma_2) \cup \mathcal{V}\text{ar}(\Gamma_2) \setminus \mathcal{V}\text{ar}(\Gamma_1)$ e portanto, $\text{Dom}(\theta\gamma) \subseteq \mathcal{V}\text{ar}(\Gamma_3) \setminus \mathcal{V}\text{ar}(\Gamma_1)$, implicando que Γ_3 é uma E -extensão conservativa de Γ_1 . \square

Outro resultado importante relacionado com E -extensões conservativas, é sobre preservação de conjuntos completos de E -unificadores, isto é, para encontrar um conjunto completo de E -unificadores de um problema Γ de E -unificação, basta encontrar em alguma E -extensão conservativa de Γ .

Proposição 1.6 (Conjuntos completos de E -unificadores de uma E -extensão conservativa). *Sejam Γ um problema de E -unificação. Se Γ' é uma E -extensão conservativa de Γ tal que $\mathcal{V}\text{ar}(\Gamma) \subset \mathcal{V}\text{ar}(\Gamma')$ e $\mathcal{C}_E(\Gamma') \neq \emptyset$ é um conjunto completo de E -unificadores de Γ' , então $\mathcal{C}_E(\Gamma')|_{\mathcal{V}\text{ar}(\Gamma)} := \{\hat{\sigma}|_{\mathcal{V}\text{ar}(\Gamma)} \mid \hat{\sigma} \in \mathcal{C}_E(\Gamma')\}$ é um conjunto completo de E -unificadores de Γ .*

Demonstração. Sejam Γ e Γ' como na hipótese e $\mathcal{C}_E(\Gamma') \neq \emptyset$ um conjunto completo de E -unificadores de Γ' . Logo para cada $\hat{\sigma} \in \mathcal{C}_E(\Gamma')$ tem-se que $\hat{\sigma}$ é um E -unificador de Γ' , e portanto $\hat{\sigma}$ é um E -unificador de Γ , assim $\mathcal{U}_E(\Gamma) \neq \emptyset$.

Seja $\sigma \in \mathcal{U}_E(\Gamma)$ qualquer, assim por Γ' ser uma E -extensão conservativa de Γ , existe uma substituição θ tal que $\text{Dom}(\theta) \subseteq \mathcal{V}\text{ar}(\Gamma') \setminus \mathcal{V}\text{ar}(\Gamma)$ e $\sigma\theta$ é um E -unificador de Γ' , podemos supor sem perda de generalidade que $\text{Dom}(\sigma) \subseteq \mathcal{V}\text{ar}(\Gamma)$, portanto $\text{Dom}(\sigma\theta) \subseteq (\text{Dom}(\sigma) \cup \text{Dom}(\theta)) \subseteq \mathcal{V}\text{ar}(\Gamma')$.

Como $\mathcal{C}_E(\Gamma')$ é um conjunto completo de E -unificadores de Γ' então existem uma substituição γ e $\hat{\sigma} \in \mathcal{C}_E(\Gamma')$ tais que $\sigma\theta|_{\mathcal{V}\text{ar}(\Gamma')} =_E \hat{\sigma}\gamma|_{\mathcal{V}\text{ar}(\Gamma')}$, implicando que, $\sigma\theta =_E \hat{\sigma}\gamma|_{\mathcal{V}\text{ar}(\Gamma')}$.

Afirmação: $\sigma\theta|_{\mathcal{V}\text{ar}(\Gamma)} = \sigma$

Tome $x \in \mathcal{V}\text{ar}(\Gamma)$, podemos supor $\mathcal{V}\text{ar}(\text{Im}(\sigma)) \cap (\mathcal{V}\text{ar}(\Gamma') \setminus \mathcal{V}\text{ar}(\Gamma)) = \emptyset$ pois queremos uma E -extensão qualquer que cumpra as hipóteses, assim podemos trocar as variáveis de $\mathcal{V}\text{ar}(\Gamma') \setminus \mathcal{V}\text{ar}(\Gamma)$ caso seja necessário, pois não altera as hipóteses, portanto $x\sigma\theta = x\sigma$, por outro lado se $x \in \mathcal{V} \setminus \mathcal{V}\text{ar}(\Gamma)$, temos $x\sigma\theta|_{\mathcal{V}\text{ar}(\Gamma)} = x = x\sigma$. Assim $\sigma\theta|_{\mathcal{V}\text{ar}(\Gamma)} = \sigma$.

Note que $[(\hat{\sigma}\gamma)|_{\mathcal{V}\text{ar}(\Gamma')}]|_{\mathcal{V}\text{ar}(\Gamma)} = \hat{\sigma}\gamma|_{\mathcal{V}\text{ar}(\Gamma' \cap \Gamma)} = \hat{\sigma}\gamma|_{\mathcal{V}\text{ar}(\Gamma)}$ pois $\mathcal{V}\text{ar}(\Gamma) \subset \mathcal{V}\text{ar}(\Gamma')$ e como foi provado, $\hat{\sigma}\gamma|_{\mathcal{V}\text{ar}(\Gamma)} = (\hat{\sigma}|_{\mathcal{V}\text{ar}(\Gamma)}\gamma)|_{\mathcal{V}\text{ar}(\Gamma)}$ temos,

$$\sigma|_{\mathcal{V}\text{ar}(\Gamma)} = \sigma = \sigma\theta|_{\mathcal{V}\text{ar}(\Gamma)} =_E (\hat{\sigma}\gamma|_{\mathcal{V}\text{ar}(\Gamma')})|_{\mathcal{V}\text{ar}(\Gamma)} = (\hat{\sigma}|_{\mathcal{V}\text{ar}(\Gamma)}\gamma)|_{\mathcal{V}\text{ar}(\Gamma)}$$

Então por $\hat{\sigma}$ se E -unificador de Γ e idempotente por fazer parte de um conjunto completo de E -unificadores, temos que o conjunto $\mathcal{C}_E(\Gamma')|_{\mathcal{V}\text{ar}(\Gamma)}$ é um conjunto completo de E -unificadores de Γ . \square

Capítulo 2

Unificação Módulo ACUN

Iremos apresentar algoritmo de unificação correto, completo e terminante, para a teoria equacional $ACUNh$ que consiste das seguintes identidades: Associatividade, Comutatividade, Unidade, Nilpotência e homomorfismo.

Para tal definiremos alguns conceitos necessários sobre a teoria $ACUNh$, cujos modelos são os grupos abelianos em que todos os elementos tem ordem 2 e o símbolo de função h é um homomorfismo entre os elementos do grupo.

O tipo do problema de unificação $ACUNh$ varia de acordo com a existência ou não de símbolos de função não-interpretados:

- Quando Γ é um problema de $ACUNh$ -unificação *elementar* ou com *constantes*, o problema de unificação é do tipo unitário e decidível em tempo polinomial, este resultado foi enunciado por Guo, Narendran e Wolfram no artigo [11].
- Quando Γ é um problema de $ACUNh$ -unificação *geral*, isto é, a assinatura considerada contém símbolos de função não-interpretados, o problema de unificação é do tipo finitário. Schulz mostrou no trabalho [16] que o problema de decidir a Solubilidade é NP-difícil.

2.1 Conceitos Básicos

Seja a assinatura $\Sigma = \{\oplus, h, 0\} \dot{\cup} \Sigma'$, onde \oplus é um símbolo de função binário representando a *operação do grupo*, h um símbolo de função unário que representa *homomorfismo* e 0 um símbolo constante que representa a *unidade*. A teoria equacional $ACUNh$ é especificada pelas regras abaixo juntamente com um sistema de reescrita R_{\oplus_h} convergente módulo AC.

Teoria Equacional $ACUNh$:

$$ACUNh = \left\{ \begin{array}{ll} x \oplus (y \oplus z) = (x \oplus y) \oplus z & (\text{Associatividade}) \\ x \oplus y = y \oplus x & (\text{Comutatividade}) \\ x \oplus 0 = x & (\text{Unidade}) \\ x \oplus x = 0 & (\text{Nilpotencia}) \\ h(x) \oplus h(y) = h(x \oplus y) & (\text{Homomorfismo}) \end{array} \right.$$

A teoria equacional $ACUN$ contém as identidades acima, com exceção da identidade para homomorfismo.

\mathcal{R}_{ACUN} : Sistema de Reescrita de Termos para $ACUN$

$$\mathcal{R}_{\oplus} = \left\{ x \oplus 0 \rightarrow x, \quad x \oplus x \rightarrow 0, \quad x \oplus y \oplus x \rightarrow y \right\}$$

\mathcal{R}_{\oplus_h} : Sistema de Reescrita de Termos para $ACUNh$

$$\mathcal{R}_{\oplus_h} = \left\{ \begin{array}{ll} x \oplus 0 \rightarrow x & h(0) \rightarrow 0 \\ x \oplus x \rightarrow 0 & h(x) \oplus h(y) \rightarrow h(x \oplus y) \\ x \oplus y \oplus x \rightarrow y & h(x) \oplus z \oplus h(y) \rightarrow h(x \oplus y) \oplus z \end{array} \right\}$$

Estes sistemas de reescritas são obtidos por um método de complemento de *Knuth–Bendix* aperfeiçoado sobre as teorias equacionais $ACUN$, $ACUNh$ respectivamente.

Observação 2.1. Denotaremos a relação $\rightarrow_{\mathcal{R}_{\oplus_h}/AC}$ ($\rightarrow_{\mathcal{R}_{\oplus}/AC}$), por simplicidade da notação, por \rightarrow (\rightarrow_{\oplus}).

Teorema 2.1. \mathcal{R}_{\oplus_h} e \mathcal{R}_{\oplus} são convergentes módulo associatividade e comutatividade, isto é, as relações \rightarrow e $\rightarrow_{\mathcal{R}_{\oplus}/AC}$ são convergentes. Em particular, dados dois termos s, t , então

- $s =_{\oplus} t$ se, e somente se, $s \downarrow_{\oplus} =_{AC} t \downarrow_{\oplus}$
- $s =_{\oplus_h} t$ se, e somente se, $s \downarrow =_{AC} t \downarrow$.

Demonstração. Este teorema fornece uma ferramenta de comparação de dois termos olhando para suas formas normais, semelhante ao teorema de Birkhof descrito em Baader [4]. Este resultado foi demonstrado por Bachmair e Dershowitz em [5], e consiste de um método de completamento de sistemas de reescritas módulo uma teoria equacional. \square

Corolário 2.1. $(\Sigma, \mathcal{R}_{\oplus}, AC)$ $(\Sigma, \mathcal{R}_{\oplus_h}, AC)$ são decomposições para as teorias equacional ACUN e ACUNh respectivamente.

Demonstração. Direto dos Teoremas 2.1 e 1.1 \square

2.2 Padronização

Seja $\Gamma = \{t_1 =^? t'_1, \dots, t_n =^? t'_n\}$ um problema de ACUN(h)-unificação. Utilizando a propriedade de nilpotência para converter as equações $t_i =^? t'_i$ para o formato $t_i \oplus t'_i =^? 0$, simplificando a notação, então obtemos um novo problema de ACUN(h)-unificação $\Gamma' := \{t_1 \oplus t'_1 =^? 0, \dots, t_n \oplus t'_n =^? 0\}$, ou ainda, $\Gamma'' = \{s_1 =^? 0, \dots, s_n =^? 0\}$ onde $s'_i = (t_i \oplus t'_i) \downarrow$, está em sua forma normal para cada $i \in \{1, \dots, n\}$ com a propriedade de que Γ, Γ' e Γ'' possuem as mesmas soluções.

Proposição 2.1 (Padronização). *Seja Γ um problema de ACUNh-unificação, então existe um problema de ACUNh-unificação $\Gamma' := \{s'_1 =^? 0, \dots, s'_n =^? 0\}$ tal que para toda substituição σ , temos que σ é ACUNh-unificador de Γ se, e somente se, σ é um ACUNh-unificador de Γ' .*

Demonstração. Sejam Γ um problema de ACUNh-unificação, $\Gamma' := \{s \oplus t =^? 0 \mid s =^? t \in \Gamma\}$ e σ uma substituição.

$$\begin{aligned}
\sigma \text{ é um ACUNh-unificador de } \Gamma &\Leftrightarrow \forall s =^? t \in \Gamma. s\sigma =_{\oplus_h} t\sigma \\
&\Leftrightarrow \forall s =^? t \in \Gamma. s\sigma \oplus t\sigma =_{\oplus_h} t\sigma \oplus t\sigma \\
&\Leftrightarrow \forall s =^? t \in \Gamma. (s \oplus t)\sigma =_{\oplus_h} 0 \\
&\Leftrightarrow \sigma \text{ é um ACUNh-unificador de } \Gamma'
\end{aligned} \tag{2.1}$$

\square

Proposição 2.2 (Normalização). *Sejam Γ um problema de ACUNh-unificação e $\Gamma \downarrow := \{s \downarrow =^? t \downarrow \mid s =^? t \in \Gamma\}$. Então, σ é um ACUNh-unificador de Γ se, e somente se, σ é um ACUNh-unificador de $\Gamma \downarrow$.*

Demonstração. Uma consequência direta do Teorema 2.1 é que $s\sigma \downarrow = (s \downarrow)\sigma \downarrow$, de fato, tome uma substituição σ .

$$\begin{aligned}
\sigma \text{ é um ACUNh-unificador de } \Gamma &\Leftrightarrow \forall s =^? t \in \Gamma. s\sigma =_{\oplus_h} t\sigma \\
&\Leftrightarrow \forall s =^? t \in \Gamma. s\sigma \downarrow =_{AC} t\sigma \downarrow \\
&\Leftrightarrow \forall s =^? t \in \Gamma. (s \downarrow)\sigma \downarrow =_{AC} (t \downarrow)\sigma \downarrow \quad (2.2) \\
&\Leftrightarrow \forall s =^? t \in \Gamma. (s \downarrow)\sigma =_{\oplus_h} (t \downarrow)\sigma \\
&\Leftrightarrow \sigma \text{ é um ACUNh-unificador de } \Gamma \downarrow
\end{aligned}$$

□

Definição 2.1 (Forma padronizada). *Seja Γ um problema de ACUNh-unificação, dizemos que Γ está em sua forma padronizada se, e somente se, para cada equação $s =^? t \in \Gamma$ tem-se que s está em sua forma normal e $t = 0$.*

Observação 2.2. *As Proposições 2.1 e 2.2 demonstradas acima, permitem tratarmos um problema de ACUN(h)-unificação através da sua forma padronizada, transformando um problema de ACUN(h)-unificação em um problema de casamento módulo ACUNh. Portanto dado um problema de ACUN(h)-unificação Γ iremos adotar as transformações nas Proposições 2.1 e 2.2 para obtermos o problema de casamento $\Gamma' := \{S_1, \dots, S_n\}$ tal que um ACUN(h)-unificador Γ é uma substituição que casa cada termo de Γ' com 0 módulo ACUNh.*

Exemplo 2.1. . *Seja Γ um problema de ACUN(h)-unificação, descrito da seguinte forma:*

$$\Gamma := \left\{ \begin{array}{ll} x \oplus h(x) \oplus f(a \oplus x \oplus h(x) \oplus y \oplus w) & =^? f(b \oplus z \oplus h(x)) \\ h(z) \oplus f(x \oplus y) \oplus w & =^? y \oplus b \oplus a \oplus f(x \oplus y \oplus 0) \\ f(x) \oplus g(y) & =^? g(y) \oplus a \oplus a \oplus f(x \oplus 0) \end{array} \right\}$$

Então aplicando a mesma técnica discutida na Proposição 2.1, normalizando e identificando a equação $S =^? 0$ com o termo S , temos:

$$\Gamma'' := \left\{ \begin{array}{c} x \oplus h(x) \oplus f(a \oplus x \oplus h(x) \oplus y \oplus w) \oplus f(b \oplus z \oplus h(x)) \\ h(z) \oplus w \oplus y \oplus b \oplus a \\ 0 \end{array} \right\}$$

$E \Gamma''$ é um problema de ACUNh-unificação que é a forma padronizada de Γ

2.3 ACUN-unificação Elementar com Constantes

Esta seção que é abordada em [11] tem por objetivo mostrar uma classe de problemas ACUN-unificação que são decidíveis em tempo polinomial, a dizer os problemas de ACUN-unificação elementar com constantes. Para isto, vamos considerar a assinatura $\Sigma_{ACUN} = \{0, \oplus\} \cup \Sigma_0$, em que \oplus é um operador binário XOR, 0 a constante nula e Σ_0 consiste apenas de símbolos constantes.

Γ é dito ser um problema de ACUN-unificação elementar com constantes quando para toda equação $s \approx^? t \in \Gamma$, tem-se que $s, t \in T(\Sigma_{ACUN}, \mathcal{V})$, isto é, além de ocorrências dos símbolos $0, \oplus$ os termos podem possuir constantes de Σ_0 ou variáveis. Mostraremos que os ACUN-unificadores de Γ são substituições cujas variáveis do domínio são mapeadas em uma combinação de constantes que ocorrem em Γ . O método proposto em [2] consiste de duas partes:

1. Reordenar os termos das equações em Γ , de forma que as variáveis fiquem do lado esquerdo da equação e as constantes do lado direito.
2. Associar cada constante c ocorrendo em Γ a um sistema de equações lineares S_c com coeficientes em \mathbb{Z}_2

Parte 1: Reordenação de Γ . Para cada $s \approx^? t \in \Gamma$, sejam $x_1, \dots, x_m, x_{m+1}, \dots, x_{m'}$ e $a_1, \dots, a_n, a_{n+1}, \dots, a_{n'}$ as variáveis e constantes ocorrendo na sua estrutura, respectivamente. Digamos,

$$\begin{aligned} t &=_{\oplus} x_1 \oplus \dots \oplus x_m \oplus a_1 \oplus \dots \oplus a_n \\ s &=_{\oplus} x_{m+1} \oplus \dots \oplus x_{m'} \oplus a_{n+1} \oplus \dots \oplus a_{n'} \end{aligned} \tag{2.3}$$

Defina $u := (x_1 \oplus \dots \oplus x_{m'}) \downarrow$ e $k := (a_1 \oplus \dots \oplus a_{n'}) \downarrow$. Observe que u, k não possuem ocorrências de "0", nem termos repetidos. Além disso, $\Sigma(u) = \{\oplus\}$ e $\mathcal{V}ar(k) = \emptyset$.

Lema 2.1. *Sejam Γ um problema de ACUN-unificação elementar com constantes e $s =^? t \in \Gamma$. Existem termos u, k tal que para cada substituição σ tem-se que $s\sigma =_{\oplus} t\sigma$ se, e somente se, $u\sigma =_{\oplus} k$, onde u, k são termos irreduzíveis tais que $\Sigma(u) = \{\oplus\}$ e $\mathcal{V}ar(k) = \emptyset$.*

Demonstração. Seja a equação $s =^? t \in \Gamma$, tome u, k como na equação 2.3.

(\Rightarrow) Suponha σ uma substituição tal que $t\sigma =_{\oplus} s\sigma$, então aplicando as propriedades de ACUN sobre essa equação obtemos as seguintes igualdades:

$$\begin{aligned} \sum_{i=1}^m x_i\sigma \oplus \sum_{i=1}^n a_i\sigma &=_{\oplus} \sum_{i=m+1}^{m'} x_i\sigma \oplus \sum_{i=n+1}^{n'} a_i \\ \sum_{i=1}^m x_i\sigma \oplus \sum_{i=m+1}^{m'} x_i\sigma &=_{\oplus} \sum_{i=1}^n a_i \oplus \sum_{i=n+1}^{n'} a_i \\ \sum_{i=1}^{m'} x_i\sigma &=_{\oplus} \sum_{i=1}^{n'} a_i \end{aligned}$$

Como $(=_{\oplus}) = \leftrightarrow^*$ então obtemos que $u =_{\oplus} \sum_{i=1}^{m'} x_i$ e $k =_{\oplus} \sum_{i=1}^{n'} a_i$ então obtemos:

$$u\sigma =_{\oplus} \sum_{i=1}^{m'} x_i\sigma =_{\oplus} \sum_{i=1}^{n'} a_i\sigma =_{\oplus} k$$

(\Leftarrow) Suponha uma substituição σ tal que $u\sigma =_{\oplus} k$, e por $(=_{\oplus}) = \leftrightarrow^*$, obtemos que

$$\sum_{i=1}^{m'} x_i\sigma =_{\oplus} u\sigma =_{\oplus} k =_{\oplus} \sum_{i=1}^{n'} a_i$$

portanto reordenando como fizemos acima obtemos que $t\sigma =_{\oplus} s\sigma$. □

Observação 2.3. *O Lema 2.1 permite assumir que todos os problemas de ACUN-unificação elementares com constantes são da forma:*

$$\Gamma = \{u_1 =^? k_1, \dots, u_n =^? k_n\}$$

com u_i e k_i obtidas através das equações (2.3), para $i = 1, \dots, n$. Desta forma o problema de ACUN-unificação elementar com constantes se torna um problema de ACUN-casamento.

Observação 2.4. *A menos que seja estabelecido o contrário, no decorrer desta seção, iremos assumir que os ACUN-unificadores de Γ são substituições normalizadas, isto é, para cada $x \in \text{Dom}(\sigma)$ tem-se que $x\sigma$ está em sua forma normal com relação a \mathcal{R}_{\oplus} módulo AC.*

Parte 2: Sistema Linear Seja $\Gamma = \{u_1 =? k_1, \dots, u_n =? k_n\}$ um problema de ACUN-unificação elementar com constantes. Para cada constante c_r que ocorre em Γ vamos criar um sistema linear S_r com coeficientes no corpo $\mathbb{Z}_2 = \{\bar{0}, \bar{1}\}$. Vamos provar que Γ possui um ACUN-unificador se, e somente se, cada sistema linear S_r possui solução. Para isso estabeleceremos as seguintes notações.

1. O conjunto $\mathbb{K}(\Gamma)$ das constantes que ocorrem em Γ é dado por:

$$\mathbb{K}(\Gamma) = \{c \in \Sigma^{(0)} \mid c \text{ é uma constante não nula que ocorre em } \Gamma\}.$$

2. Sejam $\mathcal{Var}(\Gamma) = \{x_1, \dots, x_m\}$ e $c_r \in \mathbb{K} = \{c_1, \dots, c_l\}$. Definiremos, para cada $i \in \{1, \dots, n\}$, $j \in \{1, \dots, m\}$ e $r \in \{1, \dots, l\}$ os seguintes valores:

$$a_{ij} = \begin{cases} \bar{1}, & \text{se } x_j \in \mathcal{Var}(u_i) \\ \bar{0}, & \text{se } x_j \notin \mathcal{Var}(u_i) \end{cases} \quad b_{ir} = \begin{cases} \bar{1}, & \text{se } c_r \in \Sigma(k_i) \\ \bar{0}, & \text{se } c_r \notin \Sigma(k_i) \end{cases} \quad (2.4)$$

Considere, por simplicidade, que $\bar{1}x = x$ e $\bar{0}x = 0$. Então, obtemos as seguintes identidades

$$u_i = \bigoplus_{j=1}^m a_{ij}x_j \quad k_i = \bigoplus_{r=1}^l b_{ir}c_r \quad i = 1, \dots, n$$

Consequentemente, o problema Γ pode ser reescrito da seguinte forma:

$$\Gamma = \begin{cases} u_1 = k_1 \\ u_2 = k_2 \\ \vdots \\ u_n = k_n \end{cases} \implies \begin{cases} a_{11}x_1 \oplus \dots \oplus a_{1m}x_m = b_{11}c_1 \oplus \dots \oplus b_{1l}c_l \\ a_{21}x_1 \oplus \dots \oplus a_{2m}x_m = b_{21}c_1 \oplus \dots \oplus b_{2l}c_l \\ \vdots \\ a_{n1}x_1 \oplus \dots \oplus a_{nm}x_m = b_{n1}c_1 \oplus \dots \oplus b_{nl}c_l \end{cases} \quad (2.5)$$

Para cada $c_r \in \mathbb{K}(\Gamma)$, definiremos o sistema linear S_r sobre \mathbb{Z}_2 da seguinte forma:

$$[S_r] = \left[\begin{array}{cccc|c} a_{11} & a_{12} & \dots & a_{1m} & b_{1r} \\ a_{21} & a_{22} & \dots & a_{2m} & b_{2r} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nm} & b_{nr} \end{array} \right] \quad (2.6)$$

Portanto, dado $\mathbb{K}(\Gamma) = \{c_1, \dots, c_l\}$ como conjunto de constantes que ocorrem em Γ , teremos os sistemas lineares S_1, \dots, S_l associados, respectivamente, às constantes c_1, \dots, c_l . O teorema a seguir

garante que Γ tem solução quando cada sistema linear S_r associado às constantes de Γ tem solução. Para demonstrar tal fato, faremos uso de um coeficiente d_{rj} que determina se a constante c_r ocorre ou não em $x_j\sigma$, uma instância de x_j , por um unificador normalizado σ de Γ . Especificamente, seja σ um *ACUN*-unificador normalizado de Γ (Observação 2.4) e considere a relação \in_{\oplus} dada por:

$$c_r \in_{\oplus} x_j\sigma \Leftrightarrow c_r \in \mathbb{K}(x_j\sigma)$$

Como $x_j\sigma$ está em sua forma normal, c_r ocorre no máximo uma vez em $x_j\sigma$. Desta forma, definiremos d_{rj} , para cada $j = 1, \dots, n$, por:

$$d_{rj} = \begin{cases} \bar{1} & c_r \in_{\oplus} x_j\sigma \\ \bar{0} & c_r \notin_{\oplus} x_j\sigma \end{cases} \quad (2.7)$$

Além disso, dado um unificador normalizado σ de Γ , para cada constante não-nula $c_r \in \mathbb{K}(\Gamma)$ e $i \in \{1, \dots, n\}$, definiremos o conjunto \mathbb{J}_{ir} de índices $j \in \{1, \dots, m\}$ tais que $c_r \in_{\oplus} x_j\sigma$ e $x_j \in_{\oplus} u_i$. Formalmente,

$$\begin{aligned} \mathbb{J}_{ir} &= \{j \in \{1, \dots, m\} \mid c_r \in_{\oplus} x_j\sigma \text{ e } x_j \in_{\oplus} u_i\} \\ &= \{j \in \{1, \dots, m\} \mid a_{ij} = d_{ir} = \bar{1}\} \end{aligned} \quad (2.8)$$

Como $x_j\sigma$ está em sua forma normal, para cada $j \in \mathbb{J}_{ir}$ tem-se que c_r ocorre no máximo uma vez em $x_j\sigma$.

Teorema 2.2 (solubilidade). *Seja Γ um problema de ACUN-unificação elementar com constantes. Γ é ACUN-unificável se, e somente se, para cada $c_r \in \mathbb{K}(\Gamma)$, o sistema linear S_r tem solução em \mathbb{Z}_2 .*

Demonstração. Sejam $\Gamma = \{u_1 =? k_1, \dots, u_n =? k_n\}$, $\text{Var}(\Gamma) = \{x_1, \dots, x_m\}$ e $\mathbb{K}(\Gamma) = \{c_1, \dots, c_l\}$ (\Rightarrow) Suponha que Γ é *ACUN*-unificável e seja σ um unificador normalizado de Γ .

Afirmção: Para cada $r \in \{1, \dots, l\}$ temos que $[d_{r1} \ d_{r2} \ \dots \ d_{rm}]^T$ é uma solução para o sistema linear S_r .

Observe \mathbb{Z}_2 é um corpo, em particular, um domínio de integridade então,

$$a_{ij} \cdot d_{rj} = \bar{1} \text{ se, e somente se, } a_{ij} = d_{rj} = \bar{1}$$

Vamos separar a prova em dois casos possíveis, dependendo do valor de b_{ir} :

- **Caso 1.** Se $b_{ir} = \bar{1}$ então, pela definição de b_{ir} , temos que $c_r \in \Sigma(k_i)$. Por hipótese, σ é um $ACUN$ -unificador de Γ , então $u_i\sigma =_{\oplus} k_i$ e, portanto, $c_r \in_{\oplus} u_i\sigma$.

Como k_i é uma forma normal pela construção dada na Parte 1, não há repetições de constantes. Logo, c_r ocorre uma quantidade ímpar de vezes em $u_i\sigma$; caso contrário, poderíamos usar as propriedades de nilpotência e unidade de $ACUN$ em $u_i\sigma$ obtendo um termo t tal que $c_r \notin \Sigma(t)$ e $u_i\sigma =_{\oplus} t$, o que implicaria em $k_i =_{\oplus} u_i\sigma =_{\oplus} t$. Como k_i é uma forma normal, segue que $t \downarrow_{=AC} k_i$ e teríamos $\Sigma(k_i) \subseteq \Sigma(t)$, o que é uma contradição.

Logo, a quantidade de c_r 's ocorrendo em $u_i\sigma$ é igual a $|\mathbb{J}_{ir}|$ e, portanto $|\mathbb{J}_{ir}| = 2 \cdot k + 1$, para algum inteiro não-negativo k .

- para cada $j \in \mathbb{J}_{ir}$ segue, pelas equações (2.4) e (2.7), que $a_{ij} = d_{rj} = \bar{1}$
- para cada $j \in \mathbb{J}_{ir}^C = \{1, \dots, m\} \setminus \mathbb{J}_{ir}$ temos que $c_r \notin_{\oplus} x_j\sigma$ ou $x_{ij} \notin_{\oplus} u_i$ e, portanto, $a_{ij} = \bar{0}$ ou $d_{rj} = \bar{0}$.

Obtemos as seguintes igualdades em \mathbb{Z}_2 :

$$\begin{aligned} \sum_{j=1}^m a_{ij} \cdot d_{rj} &= \sum_{j \in \mathbb{J}} a_{ij} \cdot d_{rj} + \sum_{j \in \mathbb{J}^C} a_{ij} \cdot d_{rj} \\ &= \sum_{j \in \mathbb{J}} \bar{1} \cdot \bar{1} + \sum_{j \in \mathbb{J}^C} \bar{0} = \sum_{j \in \mathbb{J}} \bar{1} + \bar{0} = |\mathbb{J}| \cdot \bar{1} \end{aligned}$$

Assim, $\sum_{j=1}^m a_{ij} \cdot d_{rj} = |\mathbb{J}_{ir}| \cdot \bar{1}$. Como $|\mathbb{J}_{ir}| = 2k + 1 (\equiv 1 \pmod{2})$, temos que

$$\sum_{j=1}^m a_{ij} \cdot d_{rj} = \bar{1} = b_{ir}$$

- **Caso 2.** Se $b_{ir} = \bar{0}$ então, pela definição de b_{ir} temos que $c_r \notin \Sigma(k_i)$.

Como σ é um $ACUN$ -unificador de Γ , $u_i\sigma =_{\oplus} k_i$ e, portanto c_r ocorre uma quantidade par de vezes em $u_i\sigma$.

- Se $\mathbb{J}_{ir} = \emptyset$ então $a_{ij} = \bar{0}$ ou $d_{rj} = \bar{0}, j = 1, \dots, m$, logo $\sum_{j=1}^m a_{ij} \cdot d_{rj} = \bar{0} = b_{ir}$.
- Se $\mathbb{J}_{ir} \neq \emptyset$ então, para cada $j \in \mathbb{J}_{ir}$, e pelo fato de $x_j\sigma$ ser um elemento irreduzível segue que c_r ocorre exatamente uma vez em $x_j\sigma$. Portanto, o número de ocorrências de c_r em $u_i\sigma$ é $|\mathbb{J}_{ir}|$, donde segue que $|\mathbb{J}_{ir}| = 2k$, para algum inteiro não-negativo k .

Analogamente ao caso anterior, obtemos que $\sum_{j=1}^m a_{ij} \cdot d_{rj} = |\mathbb{J}| \cdot \bar{1}$. Como $|\mathbb{J}| = 2k (\equiv \bar{0} \pmod{2})$ segue que $\sum_{j=1}^m a_{ij} \cdot d_{rj} = \bar{0} = b_{ir}$.

Finalmente, em ambos os casos concluímos que $\sum_{j=1}^m a_{ij} \cdot d_{rj} = b_{ir}$, donde segue que,

$$\begin{bmatrix} a_{11} & a_{12} & \dots & a_{1m} \\ a_{21} & a_{22} & \dots & a_{2m} \\ \vdots & \vdots & \vdots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nm} \end{bmatrix} \cdot \begin{bmatrix} d_{r1} \\ d_{r2} \\ \vdots \\ d_{rm} \end{bmatrix} = \begin{bmatrix} b_{1r} \\ b_{2r} \\ \vdots \\ b_{nr} \end{bmatrix}$$

Portanto, para cada $r \in \{1, \dots, l\}$, tem-se que $[d_{r1}, d_{r2} \dots d_{rm}]^T$ é uma solução para o sistema linear S_r .

(\Leftarrow) Suponha que para cada c_r o sistema linear S_r associado tenha solução.

Seja $[d_{r1} \ d_{r2} \ \dots \ d_{rm}]^T$ tal solução de S_r e defina a seguinte substituição:

$$\sigma := \{x_i \mapsto \sum_{r=1}^l d_{ri} \cdot c_r \mid i \in \{1, \dots, m\}\} \quad (2.9)$$

Afirmção: $c_r \in \Sigma(u_i \sigma \downarrow)$ se, e somente se, $c_r \in \Sigma(k_i)$, $i = 1, \dots, n$ e $r = 1, \dots, l$.

1. Suponha que $c_r \in \Sigma(k_i)$, Pela definição de b_{ir} (Equação (2.4), temos que $b_{ir} = \bar{1}$. Como $[d_{r1}, d_{r2} \dots d_{rm}]^T$ é solução de S_r , temos:

$$b_{ir} = \begin{bmatrix} a_{i1} & a_{i2} & \dots & a_{im} \end{bmatrix} \cdot \begin{bmatrix} d_{r1} \\ d_{r2} \\ \vdots \\ d_{rm} \end{bmatrix}$$

Portanto, $\sum_{j=1}^m a_{ij} \cdot d_{rj} = b_{ir} = \bar{1}$, e isto implica que existe um número ímpar de j 's tal que $a_{ij} \cdot d_{rj} = \bar{1}$, isto é, $|\mathbb{J}_{ir}| = 2k + 1$, para algum inteiro não-negativo k .

Por outro lado, pela definição de a_{ij} e d_{rj} , segue que, para cada $j \in \mathbb{J}_{ir}$ temos que $c_r \in_{\oplus} x_j \sigma$.

Além disso,

$$\sum_{j=1}^m a_{ij} x_j =_{\oplus} \sum_{j \in \mathbb{J}} a_{ij} x_j + \sum_{j \in \mathbb{J}^C} a_{ij} x_j =_{\oplus} \sum_{j \in \mathbb{J}} \bar{1} x_j + \sum_{j \in \mathbb{J}^C} a_{ij} x_j =_{\oplus} \sum_{j \in \mathbb{J}} x_j + \sum_{j \in \mathbb{J}^C} a_{ij} x_j$$

Faça $u'_i = (\sum_{j \in \mathbb{J}^C} a_{ij} x_j) \downarrow$. $c_r \notin_{\oplus} u'_i \sigma$, e então podemos desconsiderar na contagem das ocorrências de c_r em $u_i \sigma$, as variáveis que ocorrem em u'_i . E ao aplicarmos a substituição σ definida na equação (2.9), obtemos: $u_i \sigma =_{AC} \sum_{j \in \mathbb{J}} x_j \sigma + u'_i \sigma$.

Assim, se x_j é uma variável que ocorre em u_i , com $j \in \mathbb{J}_{ir}$, então temos que c_r ocorre em $x_j \sigma$ apenas uma vez.

Por outro lado, para cada ocorrência de c_r em $u_i \sigma$, existe uma variável x_j que ocorre em u_i tal que c_r ocorre em $x_j \sigma$ e portanto $a_{ij} = d_{rj} = \bar{1}$, isto é, $j \in \mathbb{J}_{ir}$. Portanto, o número de ocorrências da constante c_r em $u_i \sigma$ é ímpar, donde segue que c_r ocorre número ímpar de vezes em $u_i \sigma$.

Logo, $c_r \in \Sigma(u_i \sigma \downarrow)$.

2. Se $c_r \notin \Sigma(k_i)$ então $b_{ir} = \bar{0}$, e pelo mesmo argumento utilizado no caso anterior temos que

$$\sum_{j=1}^m a_{ij} \cdot d_{rj} = \bar{0}.$$

Logo existe um número par de j 's tais que $a_{ij} \cdot d_{rj} = \bar{1}$, isto é, $|\mathbb{J}_{ir}| = 2k$, para algum inteiro não-negativo k .

- Se $k = 0$ então $\mathbb{J}_{ir} = \emptyset$ e, portanto $a_{ij} = \bar{0}$ ou $d_{rj} = \bar{0}$, para todo j . Assim, para cada x_j ocorrendo em u_i , temos que $a_{ij} = \bar{1}$ e, portanto $d_{rj} = \bar{0}$.

Logo, $c_r \notin_{\oplus} x_j \sigma$ e então c_r não ocorre em $u_i \sigma$.

- Se $k > 0$ então $\mathbb{J}_{ir} \neq \emptyset$. Para cada $j \in \mathbb{J}_{ir}$, temos que $c_r \in_{\oplus} x_j \sigma$ e $x_j \in_{\oplus} u_i$. Utilizando o raciocínio do caso anterior obtemos: $u_i \sigma =_{AC} \sum_{j \in \mathbb{J}} x_j \sigma + u'_i \sigma$.

Similarmente, o número de ocorrências da constante c_r em $u_i \sigma$ é par, isto é, $|\mathbb{J}_{ir}| = 2k$ e, portanto, c_r ocorre um número par de vezes em $u_i \sigma$. Logo, $c_r \notin_{\oplus} u_i \sigma \downarrow$.

Como $u_i \sigma \downarrow$ e k_i são ambos termos irredutíveis e contém os mesmos símbolos de constantes, e como, além disso, σ é uma substituição básica (Equação 2.9), segue que, $u_i \sigma \downarrow =_{AC} k_i$. Logo, $u_i \sigma =_{\oplus} k_i$, e pelo Lema 2.1, σ é um ACUN-unificador de Γ , para cada $i = 1, \dots, n$.

□

As soluções dos sistemas lineares sobre \mathbb{Z}_2 são obtidos por um algoritmo de complexidade polinomial:

Teorema 2.3 (Complexidade da solubilidade). *O problema de decidir a solubilidade de um problema Γ de ACUN-unificação tem complexidade polinomial.*

Demonstração. A demonstração é consequência direta do Teorema 2.2 e observando que resolver sistemas lineares com coeficientes no corpo \mathbb{Z}_2 tem complexidade polinomial, provado em [14]. \square

Teorema 2.4. *O problema Γ de ACUN-unificação elementar com constantes é unitário, isto é, se Γ é ACUN-unificável então existe um ACUN-unificador mais geral de Γ .*

Demonstração. A demonstração será apresentada na Seção 3.2. \square

2.3.1 ACUNh-unificação Elementar com constantes

Nesta seção consideraremos a assinatura $\Sigma = \{0, \oplus, h\} \cup \Sigma_0$, onde Σ_0 é um conjunto de símbolos constantes e h é um símbolo de função unário que satisfaz a identidade de *homorfismo* com relação ao ACUN operador \oplus .

O objetivo é apresentar a técnica proposta em [11] para o estudo da solubilidade de problemas de ACUNh-unificação elementar com constantes. O método consiste em desenvolver os seguintes pontos:

- Denotar por $G = T(\Sigma \setminus \{h\}, \mathcal{V})$, o modelo que satisfaz as identidades ACUN, como um grupo sobre operador \oplus , isto é, G é um grupo abeliano de expoente 2.
- Utilizar um anel de polinômios $\mathbb{Z}_2[h]$ sobre a incógnita h e com coeficientes no corpo $\mathbb{Z}_2 = \{\bar{0}, \bar{1}\}$. Isto é, se $H \in \mathbb{Z}_2[h]$, então existem coeficientes $a_0, \dots, a_n \in \mathbb{Z}_2$ tais que

$$H = a_0 + a_1h + a_2h^2 + \dots + a_nh^n.$$

Além disso as operações $+$ e multiplicação por escalar “ \cdot ” satisfazem as identidades de corpos.

- Associar a cada termo $t \in T(\Sigma, \mathcal{V})$ a uma combinação linear de $t_1, \dots, t_n \in G$, com coeficientes sendo polinômios de $\mathbb{Z}_2[h]$: para isso provaremos que $T(\Sigma, \mathcal{V}) / \approx_{\oplus_h}$ é um $\mathbb{Z}_2[h]$ -módulo.

Polinômio \times Termo: Seja $H \in \mathbb{Z}_2[h]$, da forma $H = a_0 + a_1h + a_2h^2 + \dots + a_nh^n$ e $t \in T(\Sigma, \mathcal{V})$ um termo, definiremos a operação \cdot da seguinte forma:

$$H \cdot t := a_0 \cdot t \oplus a_1 \cdot h(t) \oplus a_2 \cdot h(h(t)) \oplus \dots \oplus a_n \cdot h(h(\dots h(t)) \dots)) \quad (2.10)$$

Em que os coeficientes a_i agem sobre t segundo a definição:

$$a_i \cdot t := \begin{cases} 0 & ; a_i = \bar{0} \\ t & ; a_i = \bar{1} \end{cases} \quad (2.11)$$

O conjunto V das possíveis combinações lineares sobre G com coeficientes em $\mathbb{Z}_2[h]$ é dado por:

$$V := \left\{ \sum_{i=1}^n H_i \cdot t_i \mid n \in \mathbb{N}, H_i \in \mathbb{Z}_2[h] \text{ e } t_i \in G, i = 1, \dots, n \right\}$$

Isto é, V é um subconjunto de $T(\Sigma, \mathcal{V})$.

V é um $\mathbb{Z}_2[h]$ -módulo, isto é, as operações \cdot e \oplus definidas abaixo, satisfazem as identidades de módulo, com produto escalar \cdot sobre elementos do anel de polinômios $\mathbb{Z}_2[h]$.

1.

$$\begin{aligned} \oplus : V \times V &\longrightarrow V \\ \left(\sum_{i=1}^n H_i \cdot t_i, \sum_{i=1}^n H'_i \cdot t'_i \right) &\mapsto \sum_{i=1}^n H_i \cdot t_i \oplus_h \sum_{i=1}^n H'_i \cdot t'_i \end{aligned}$$

2.

$$\begin{aligned} \cdot : \mathbb{Z}_2[h] \times V &\longrightarrow V \\ \left(H, \sum_{i=1}^n H_i \cdot t_i \right) &\mapsto \sum_{i=1}^n (H \cdot H_i) \cdot t_i \end{aligned}$$

Vamos provar que existe $U \subseteq V$ tal que U é um conjunto completo de representantes para $T(\Sigma, \mathcal{V})$ sobre a relação de equivalência $=_{\oplus_h}$.

Para isto, considere o seguinte conjunto:

$$U := \left\{ \sum_{i=1}^n H_i \cdot t_i \mid n \in \mathbb{N}, t_i \in \mathcal{T}(\Sigma_0, \mathcal{V}) \text{ são distintos e } H_i \in \mathbb{Z}_2[h] \setminus \{\bar{0}\} \right\} \cup \{0\}$$

O seguinte lema garante que cada termo $t \in \mathcal{T}(\Sigma, \mathcal{V})$, pode ser escrito como uma combinação linear de termos $H_i \cdot t_i$. Para isto, a partir da forma normal $t \downarrow$, vamos aplicar uma nova regra de

reescrita $h(x \oplus y) \rightarrow h(x) \oplus h(y)$, que *expande* a forma normal w.r.t. ACUNh. O objetivo desta estratégia é *planificar* o termo t com relação ao operador \oplus , afim de obtê-lo como um termo da forma $t \approx_{\oplus_h} t_1 \oplus t_2 \oplus \dots \oplus t_n$, com t_i 's possivelmente encabeçados por h .

Exemplo 2.2. $t = x \oplus h(h(a \oplus b))$ é uma forma normal com relação \mathcal{R}_{\oplus_h} , aplicando exhaustivamente a regra $r : h(x \oplus y) \rightarrow h(x) \oplus h(y)$, expandimos o termo t da seguinte forma:

$$t \rightarrow_r x \oplus h(h(a) \oplus h(b)) \rightarrow_r x \oplus h(h(a)) \oplus h(h(b)) = t'.$$

É claro que $t \approx_{\oplus_h} t'$. Além disso, não há ocorrências de \oplus abaixo de h 's em t' .

Lema 2.2. Para cada $t \in T(\Sigma, \mathcal{V})$ existe $u \in U$ tal que $t \approx_{\oplus} u$.

Demonstração. Seja $t \neq_{\oplus_h} 0$ um termo e $\mathbb{K}_v(t \downarrow) \neq \emptyset$ o conjunto de símbolos constantes e variáveis que ocorrem em $t \downarrow$. A irreduzibilidade de $t \downarrow$ garante que $0 \notin \mathbb{K}_v(t \downarrow) \neq \emptyset$.

Aplicando a regra $h(x \oplus y) \rightarrow h(x) \oplus h(y)$ exhaustivamente em $t \downarrow$, obtemos um termo t' , tal que $t \downarrow =_{\oplus_h} t'$. Além disso,

- $\mathbb{K}_v(t \downarrow) = \mathbb{K}_v(t')$; e
- não existem ocorrências de \oplus ou 0 abaixo de h em t' .

Para fins de simplicidade denotaremos que $s \in_{\oplus} t$ se, e somente se, s é um argumento de soma de t .

1. Para cada constante $c \in \mathbb{K}_v(t \downarrow)$, considere o seguinte polinômio sobre $\mathbb{Z}_2[h]$.

$$H_c = c_0 + c_1 \cdot h + \dots + c_n \cdot h^n + \dots,$$

os coeficientes c_i são dados por:

$$c_i := \begin{cases} \bar{1}, & h^i(c) \in_{\oplus} t' \\ \bar{0}, & \text{caso contrário.} \end{cases}$$

Simplificando H_c , removendo as ocorrências de $\bar{0}$, obtemos $H_c = h^{i_1} + \dots + h^{i_k}$, onde i_1, \dots, i_k são índices tais que $c_{i_j} \neq \bar{0}$.

Portanto, utilizando a definição da ação de polinômios sobre termos, dada pela equação (2.10), obtemos: $H_c \cdot c = h^{i_1}(c) \oplus \dots \oplus h^{i_k}(c)$.

2. Para cada variável $x \in \mathbb{K}_v(t \downarrow)$ faremos uma construção similar, obtendo primeiramente um polinômio $H_x = g_0 + g_1 \cdot h + \dots + g_u \cdot h^u$, em que os coeficientes g_i são dados por:

$$g_i := \begin{cases} \bar{1}, & h^i(x) \in_{\oplus} t' \\ \bar{0}, & \text{caso contrário.} \end{cases}$$

Removendo ocorrências de 0's e utilizando as identidades da equação (2.10), obtemos: $H_x \cdot x = h^{i_1}(x) \oplus \dots \oplus h^{i_s}(x)$.

Desta forma, enumerando $\mathbb{K}_v(t \downarrow) = \{c_1, \dots, c_n, x_{n+1}, \dots, x_s\}$ temos que, para $t_i \in \mathbb{K}_v(t \downarrow)$:

$$\sum_{i=1}^s H_{t_i} \cdot t_i =_{\oplus_h} t' =_{\oplus_h} t \downarrow =_{\oplus_h} t$$

Pela definição de U , temos que $\sum_{i=1}^s H_{t_i} \cdot t_i \in U$ para cada $t \neq_{\oplus_h} 0$. E caso $t =_{\oplus_h} 0$, basta notar que $0 \in U$.

□

Lema 2.3. Para cada $u, u' \in U$ se $u \neq_{AC} u'$ então $u \neq_{\oplus_h} u'$

Demonstração. Note que $u = \sum_{i=1}^n H_i \cdot t_i$ e $u' = \sum_{i=1}^n H'_i \cdot t'_i$, como $u \neq_{AC} u'$ logo suas formas normais são distintas módulo AC , pois pela própria definição de U , a única regra de reescrita de \mathcal{R}_{\oplus} que pode ser aplicada em u, u' é

$$h(x) \oplus h(y) \rightarrow h(x \oplus y)$$

E portanto obtemos que $u \downarrow \neq_{AC} u' \downarrow$, equivalentemente, $u \neq_{\oplus_h} u'$

□

Teorema 2.5. U é um conjunto completo de representantes de $T(\Sigma, \mathcal{V})$ sobre a relação de equivalência $=_{\oplus_h}$

Demonstração. A prova é consequência direta dos Lemas 2.2 e 2.3.

□

Reordenando Γ . Dado um problema $\Gamma = \{s_1 =? t_1, \dots, s_n =? t_n\}$ de ACUNh-unificação elementar com constantes. Vamos utilizar o lema 2.2 para obtermos um novo problema $\Gamma' = \{u_1 =? k_1, \dots, u_n =? k_n\}$ com as seguintes propriedades, para cada $i = 1, \dots, n$:

1. a cada $s_i =? t_i \in \Gamma$ corresponde $u_i =? k_i$, tal que $u_i, k_i \in U$, u_i contém ocorrências de variáveis, e dos símbolos \oplus e h na sua estrutura, isto é, $\Sigma(u_i) = \{\oplus, h\}$; k_i não possui variáveis, $\mathcal{V}ar(k_i) = \emptyset$.
2. para cada σ : $s_i\sigma =_{\oplus_h} t_i\sigma$ se, e somente se, $u_i\sigma =_{\oplus_h} k_i$

Exemplo 2.3. Considere o problema de ACUNh-unificação elementar com constantes: $\Gamma = \{h(h(x_1) \oplus x_2) \oplus x_3 =? c, h(x \oplus d) =? 0\}$, aplicando exaustivamente a regra $h(x \oplus y) \rightarrow h(x) \oplus h(y)$, como no Lema 2.2, obtemos:

$$\Gamma = \{h(h(x_1)) \oplus h(x_2) \oplus x_3 =? c, h(x) \oplus h(d) =? 0\}$$

Reordenando os termos, para satisfazer as propriedades 1. e 2., obtemos o problema

$$\Gamma' = \{h(h(x_1)) \oplus h(x_2) \oplus x_3 =? c, h(x) =? h(d)\}$$

ACUNh-Unificação com constantes \times Polinômio sobre $\mathbb{Z}_2[h]$: Seja $\Gamma = \{u_1 =? k_1, \dots, u_n =? k_n\}$ um problema de ACUNh-unificação elementar com constantes que satisfaz as propriedades 1. e 2., e tal que o conjunto das suas variáveis é dado por $\mathcal{V}ar(\Gamma) = \{x_1, \dots, x_m\}$ e $\mathbb{K}(\Gamma) = \{c_1, \dots, c_l\}$ denota o conjunto das constantes não-nulas que ocorrem em Γ .

A partir de Γ vamos definir os seguintes polinômios:

$$H_{ij} := \begin{cases} \bar{0} & ; x_j \notin \mathcal{V}ar(u_i) \\ p_j & ; p_j \in \mathbb{Z}_2[h] \setminus \{0\} \text{ e } p_j \cdot x_j \text{ está na combinação linear de } u_i \end{cases} \quad (2.12)$$

$$H'_{ir} := \begin{cases} \bar{0} & ; c_r \notin \mathbb{K}(k_i) \\ p_r & ; p_r \in \mathbb{Z}_2[h] \setminus \{0\} \text{ e } p_r \cdot c_r \text{ está na combinação linear de } k_i \end{cases}$$

com $i = 1, \dots, n$, $j = 1, \dots, m$ e $r = 1, \dots, l$.

E então, obtemos

$$u_i =_{\oplus_h} \sum_{j=1}^m H_{ij} \cdot x_j \text{ e } k_i =_{\oplus_h} \sum_{r=1}^l H'_{ir} \cdot c_r.$$

Para cada $r \in \{1, \dots, l\}$ vamos construir um sistema linear sobre $\mathbb{Z}_2[h]$ nas variáveis $x_1^r, x_2^r, \dots, x_m^r$ da seguinte forma:

$$S_r = \begin{cases} H_{11}x_1^r + H_{12}x_2^r + \dots + H_{1m}x_m^r = H'_{1r} \\ H_{21}x_1^r + H_{22}x_2^r + \dots + H_{2m}x_m^r = H'_{2r} \\ \vdots \\ H_{n1}x_1^r + H_{n2}x_2^r + \dots + H_{nm}x_m^r = H'_{nr} \end{cases} \quad (2.13)$$

Ou ainda na representação matricial $[S_r]$:

$$[S_r] = \left[\begin{array}{cccc|c} H_{11} & H_{12} & \dots & H_{1m} & H'_{1r} \\ H_{21} & H_{22} & \dots & H_{2m} & H'_{2r} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ H_{n1} & H_{n2} & \dots & H_{nm} & H'_{nr} \end{array} \right] \quad (2.14)$$

Exemplo 2.4. Retomando o exemplo 2.3, para $\Gamma = \{h(h(x_1)) \oplus h(x_2) \oplus x_3 =^? c, h(x) =^? h(d)\}$, temos os conjuntos $\mathcal{V}ar(\Gamma) = \{x_1, x_2, x_3\}$ e $\mathbb{K}(\Gamma) = \{c, d\}$. Fazendo $c_1 = c$ e $c_2 = d$, obtemos os seguintes polinômios:

$$\begin{array}{llll} H_{11} = h^2 & H_{21} = h & H'_{11} = \bar{1} & H'_{21} = \bar{0} \\ H_{12} = h & H_{22} = \bar{0} & H'_{12} = \bar{0} & H'_{22} = h \\ H_{13} = 1 & H_{23} = \bar{0} & & \end{array}$$

$$[S_c] = \left[\begin{array}{ccc|c} h^2 & h & \bar{1} & \bar{1} \\ h & \bar{0} & \bar{0} & \bar{0} \end{array} \right] \quad [S_d] = \left[\begin{array}{ccc|c} h^2 & h & \bar{1} & \bar{0} \\ h & \bar{0} & \bar{0} & h \end{array} \right]$$

Teorema 2.6. Γ é unificável se, e somente, se S_r tem solução em $\mathbb{Z}_2[h]$ para cada $r \in \{1, \dots, l\}$

Demonstração. (\Rightarrow) Suponha Γ unificável e seja σ um ACUNh-unificador de Γ . logo $u_i\sigma =_{\oplus_h} k_i$ para cada $i \in \{1, \dots, n\}$, ou ainda,

$$u_i\sigma =_{\oplus_h} \sum_{j=1}^m H_{ij}(x_j\sigma) =_{\oplus_h} k_i =_{\oplus_h} \sum_{r=1}^l H'_{ij}c_{ir} \quad (2.15)$$

Como k_i é um termo básico então podemos supor, sem perda de generalidade, que σ é uma substituição básica e normalizada então $x_j\sigma$ não possui termos repetidos. Desta forma, para cada $j \in \{1, \dots, m\}$,

temos $x_j\sigma =_{\oplus_h} \sum_{r=1}^l x_j^r c_r$ onde $x_j^r \in \mathbb{Z}_2[h]$ para cada $r \in \{1, \dots, l\}$ e pela equação 2.15,

$$\sum_{i=1}^m H_{ij}(x_j\sigma) =_{\oplus_h} \sum_{r=1}^l H'_{ir} c_r$$

Concluindo assim,

$$\sum_{r=1}^l H'_{ir} c_r =_{\oplus_h} \sum_{i=1}^m H_{ij}(x_j\sigma) =_{\oplus_h} \sum_{i=1}^m H_{ij} \sum_{r=1}^l x_j^r c_r =_{\oplus_h} \sum_{r=1}^l \sum_{i=1}^m H_{ij} x_j^r c_r$$

E como não ocorre repetições das constantes c_r em $\sum_{r=1}^l H'_{ir} c_r$ temos que

$$\sum_{j=1}^m H_{ij} x_j^r = H'_{ir}$$

Como tomamos $i \in \{1, \dots, n\}$ de forma arbitrária, temos que a equação logo acima vale para cada i , e portanto:

$$\begin{bmatrix} H_{11} & H_{12} & \dots & H_{1m} \\ H_{21} & H_{22} & \dots & H_{2m} \\ \vdots & \vdots & \vdots & \vdots \\ H_{n1} & H_{n2} & \dots & H_{nm} \end{bmatrix} \cdot \begin{bmatrix} x_1^r \\ x_2^r \\ \vdots \\ x_m^r \end{bmatrix} = \begin{bmatrix} H'_{1r} \\ H'_{2r} \\ \vdots \\ H'_{nr} \end{bmatrix}$$

E portanto para cada $r \in \{1, \dots, l\}$ o sistema S_r tem solução em $\mathbb{Z}_2[h]$.

(\Leftarrow) Suponha cada S_r com solução $[x_1^r, x_2^r, \dots, x_m^r]^T$ em $\mathbb{Z}_2[h]$ para cada $r \in \{1, \dots, l\}$, faça a seguinte substituição: $\sigma := \{x_j \mapsto \sum_{r=1}^l x_j^r \cdot c_r \mid j = 1, \dots, m\}$.

Como $u_i =_{\oplus_h} \sum_{i=1}^m H_{ij} \cdot x_j$ então ao aplica a substituição σ temos:

$$u_i\sigma =_{\oplus_h} \sum_{i=1}^m H_{ij} \cdot (x_j\sigma) =_{\oplus_h} \sum_{i=1}^m H_{ij} \sum_{i=1}^m x_j^r \cdot c_r =_{\oplus_h} \sum_{r=1}^l \left(\sum_{i=1}^m H_{ij} \cdot x_j^r \right) \cdot c_r$$

Mas como $[x_1^r, x_2^r, \dots, x_m^r]^T$ é solução do sistema linear S_r então temos que:

$$H'_{ir} = \begin{bmatrix} H_{i1} & H_{i2} & \dots & H_{im} \end{bmatrix} \cdot \begin{bmatrix} x_1^r \\ x_2^r \\ \vdots \\ x_m^r \end{bmatrix}$$

E portanto: $u_i\sigma =_{\oplus_h} \sum_{r=1}^l H'_{ir} \cdot c_r =_{\oplus_h} k_i$. □

Exemplo 2.5. $\sigma = \{x_1 \mapsto d, x_2 \mapsto 0, x_3 \mapsto h^2(d) \oplus c\}$ é ACUNh-unificador de Γ dado no exemplo 2.4.

A partir de σ , podemos construir soluções para os sistemas representados pelas matrizes $[S_c]$ e $[S_d]$:

$$\begin{array}{l} x_1\sigma = 0 \cdot c + 1 \cdot d \\ x_2\sigma = 0 \cdot c + 0 \cdot d \\ x_3\sigma = 1 \cdot c + h^2 \cdot d \end{array} \quad \begin{bmatrix} x_1^1 \\ x_2^1 \\ x_3^1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \quad \begin{bmatrix} x_1^2 \\ x_2^2 \\ x_3^2 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ h^2 \end{bmatrix}$$

Seguindo a construção dada pelo Teorema 2.6, obtemos que $[0 \ 0 \ 1]^T$ é solução de $[S_c]$ e $[1 \ 0 \ h^2]^T$ é solução de $[S_d]$.

Reciprocamente, podemos obter uma solução de Γ , sempre que os sistemas obtidos para cada constante em Γ , tem solução:

Exemplo 2.6. Voltando ao exemplo 2.4, com $\Gamma = \{h(h(x_1)) \oplus h(x_2) \oplus x_3 =^? c, h(x) =^? h(d)\}$.

Observe que

$$\begin{bmatrix} x_1^1 \\ x_2^1 \\ x_3^1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \quad \begin{bmatrix} x_1^2 \\ x_2^2 \\ x_3^2 \end{bmatrix} = \begin{bmatrix} 1 \\ h \\ 0 \end{bmatrix}$$

são soluções de $[S_c]$ e $[S_d]$, respectivamente. Podemos construir um ACUNh-unificador da seguinte forma:

$$\sigma = \begin{cases} x_1 \mapsto x_1^1 \cdot c \oplus x_1^2 \cdot d = 0 \cdot c \oplus 1 \cdot d \approx_{\oplus_h} d \\ x_2 \mapsto x_2^1 \cdot c \oplus x_2^2 \cdot d = 0 \cdot c \oplus h \cdot d \approx_{\oplus_h} h(d) \\ x_3 \mapsto x_3^1 \cdot c \oplus x_3^2 \cdot d = 1 \cdot c \oplus 0 \cdot d \approx_{\oplus_h} c \end{cases}$$

Isto é, $\sigma = \{x_1 \mapsto d, x_2 \mapsto h(d), x_3 \mapsto c\}$ é solução de Γ .

Teorema 2.7 (Complexidade da solubilidade). *O problema de decidir a solubilidade de um problema Γ de ACUNh-unificação elementar com constantes tem complexidade polinomial.*

Demonstração. A demonstração é consequência direta do Teorema 2.6 e observando que resolver sistemas lineares com coeficientes no domínio principal $\mathbb{Z}_2[h]$ tem complexidade polinomial, provado em [12]. □

Teorema 2.8. *O problema Γ de ACUNh-unificação elementar com constantes é unitário, isto é, se Γ é ACUNh-unificável então existe um ACUNh-unificador mais geral de Γ .*

Demonstração. A demonstração será apresentada na Seção 3.2. □

2.4 Unificação Geral ACUN(h)

Nesta seção consideraremos uma assinatura Σ tal que $\Sigma_{ACUN(h)} \subset \Sigma$ e $\Sigma \setminus \Sigma_{ACUN(h)}$ contém símbolos de função arbitrários. Γ é dito ser um problema de ACUNh-unificação geral, quando para todo $s =^? t \in \Gamma$, tem-se que $s, t \in T(\Sigma, \mathcal{V})$ e os símbolos de função em $\Sigma \setminus \Sigma_{ACUN(h)}$ não serão interpretados.

Em 1997, no artigo [16], Schulz mostra que ao considerarmos símbolos de função diferentes de $\{\oplus, 0\}$, não-interpretados, num problema de ACUNh-unificação, a complexidade da decidibilidade do mesmo torna-se *NP-difícil*. A seguir apresentaremos algumas noções sobre uma teoria equacional E arbitrária, que servirão como ferramentas para uma futura discussão sobre a dificuldade de resolver o problema de ACUNh-unificação geral.

Definição 2.2 (Consistência, Regularidade). *Seja E um conjunto de Σ -identidades sobre o conjunto de termos $T(\Sigma, \mathcal{V})$, dizemos que E é consistente se, e somente se, para cada $x, y \in \mathcal{V}$ tem-se que $x \neq y$ sse $x \neq_E y$. Também definimos que E é regular se para cada $s = t \in E$ tem-se que $\text{Var}(s) = \text{Var}(t)$.*

Observação 2.5. *Se E é regular então para cada par de termos $s, t \in T(\Sigma, \mathcal{V})$, temos que $s =_E t$ implica que $\text{Var}(s) = \text{Var}(t)$.*

Definição 2.3 (E -unificador \vec{x} -atômico). *Sejam Γ um problema de E -unificação sobre a assinatura Σ , $\{x_0, x_1, \dots, x_m\} \subseteq \text{Var}(\Gamma)$ para algum $m \geq 0$. Denote o vetor $\langle x_0, x_1, \dots, x_m \rangle$ por \vec{x} . Então um E -unificador σ é dito \vec{x} -atômico se, e somente se, para cada $i \in \{0, 1, \dots, m\}$ tem-se que $x_i\sigma \in (\Sigma^{(0)} \setminus \Sigma_E) \cup \mathcal{V}$, isto é, para cada $i \in \{0, 1, \dots, m\}$ tem-se que $x_i\sigma$ é uma variável ou $x_i\sigma$ é uma constante que não ocorre em Σ_E .*

A proposição seguir foi proposta e provada em [16], e mostra que a solubilidade de um problema de E -unificação Γ , que contém constantes que não ocorrem na assinatura de uma teoria E , é *NP-difícil*.

Proposição 2.3. [Principal] *Seja E um conjunto de Σ -identidades consistente sobre a assinatura Σ . Suponha que exista um problema de E -unificação elementar com constantes Γ , contendo três constantes distintas a, b e c que não ocorrem em E e variáveis $\{x_0, x_1, \dots, x_m\}$.*

1. Se Γ tem E -unificadores \vec{x} -atômicos σ_a, σ_b e σ_c tais que $x_0\sigma_a = a, x_0\sigma_b = b$ e $x_0\sigma_c = c$, e
2. Para cada E -unificador \vec{x} -atômico σ de Γ tem-se que $x_0\sigma \in \{a, b, c\}$

Então a solubilidade do problema geral de E -unificação é NP-difícil.

Demonstração. A demonstração desta proposição se encontra em [16]. □

Apresentaremos algumas consequências da Proposição 2.3, para teorias equacionais cujas assinaturas possuem símbolos de função associativos (Lema 2.4) ou comutativos (Lema 2.5).

Lema 2.4. *Seja E uma teoria equacional sobre Σ consistente que contém um símbolo de função binário associativo ' \circ '. Se E é regular, então a complexidade de decidir a solubilidade de um problema geral de E -unificação é NP-difícil.*

Demonstração. Considere o problema $\Gamma = \{y \circ x \circ z = a \circ a \circ b \circ c \circ c\}$ de E -unificação elementar com constantes. Seja $\vec{x} = \langle x \rangle$ e por ' \circ ' ser associativa temos que as seguintes substituições são E -unificadores de Γ : $\sigma_a = \{x \mapsto a, y \mapsto a, z \mapsto b \circ c \circ c\}$, $\sigma_b = \{x \mapsto b, y \mapsto a \circ a, z \mapsto c \circ c\}$, e $\sigma_c = \{x \mapsto c, y \mapsto a \circ a \circ b, z \mapsto c\}$.

Pela escolha dos E -unificadores acima temos que são \vec{x} -atômicos, logo Γ possui a propriedade 1 da Proposição 2.3. Tome σ um E -unificador de Γ \vec{x} -atômico qualquer, então temos que $(x \circ y \circ z)\sigma =_E a \circ a \circ b \circ c \circ c$ e, aplicando a substituição para os argumentos do termo $x \circ y \circ c$ com a propriedade associatividade de ' \circ ' obtemos $x\sigma \circ y\sigma \circ z\sigma =_E a \circ a \circ b \circ c \circ c$.

Como, por hipótese, temos que E é regular e com isso pode-se concluir pela Observação 2.5 que $\mathcal{Var}(x\sigma \circ y\sigma \circ z\sigma) = \mathcal{Var}(a \circ a \circ b \circ c \circ c) = \emptyset$.

Portanto $x\sigma$ não pode ser uma variável, logo $x\sigma$ é um subtermo de $a \circ a \circ b \circ c \circ c$ e por hipótese σ é \vec{x} -atômico então $x\sigma \in \{a, b, c\}$. Concluindo assim que Γ possui a propriedade 2. da Proposição 2.3. Então obtemos que um problema geral de E -unificação é NP-difícil. □

Lema 2.5. *Seja E uma teoria equacional sobre Σ consistente que contém um símbolo de função binário comutativo ' \star '. Se E é regular, então a complexidade de decidir a solubilidade de um problema geral de E -unificação é NP-difícil.*

Demonstração. Considere o problema de E -unificação elementar com constantes

$$\Gamma = \{(x \star y) \star (z \star w) = (a \star b) \star (b \star c)\}$$

Seja $\vec{x} = \langle x \rangle$, como ' \star ' é comutativo então obtemos as seguintes identidades:

$$(a \star b) \star (b \star c) =_E (a \star b) \star (b \star c)$$

$$(b \star a) \star (b \star c) =_E (a \star b) \star (b \star c)$$

$$(c \star b) \star (a \star b) =_E (a \star b) \star (b \star c)$$

E portanto as seguintes substituições são E -unificadores de Γ : $\sigma_a = \{x \mapsto a, y \mapsto b, z \mapsto b, w \mapsto c\}$, $\sigma_b = \{x \mapsto b, y \mapsto a, z \mapsto b, w \mapsto c\}$ e $\sigma_c = \{x \mapsto c, y \mapsto b, z \mapsto a, w \mapsto b\}$.

Além disso σ_a, σ_b e σ_c são \vec{x} -atômicos, portanto Γ possui a propriedade 1, da Proposição 2.3.

Seja σ um E -unificador \vec{x} -atômico de Γ qualquer, então temos que por definição de \vec{x} -atômico, $x\sigma \in (\Sigma^{(0)} \setminus \Sigma_E) \dot{\cup} \mathcal{V}$ e $(x\sigma \star y\sigma) \star (z\sigma \star w\sigma) =_E (a \star b) \star (b \star c)$.

Como E é regular segue que $\emptyset = \mathcal{V}ar((a \star b) \star (b \star c)) = \mathcal{V}ar((x\sigma \star y\sigma) \star (z\sigma \star w\sigma))$.

Logo, $x\sigma$ não é uma variável então por σ ser \vec{x} -atômico, implica que, $x\sigma$ é uma constante que não ocorre em Σ_E , portanto $x\sigma \in \{a, b, c\}$, portanto obtemos que Γ possui a propriedade 2. da Proposição 2.3, logo problemas de E -unificação gerais é NP-Difícil. \square

Os lemas 2.4 e 2.5 garantem que a decidibilidade da solubilidade de problemas de E -unificação gerais, quando $E = A, C, AC$ ou ACU , são problemas NP-difíceis, uma vez que as teorias são regulares. Porém, no caso em que $E = ACUN$ ou $ACUNh$, perde-se a regularidade: devido a identidade $x \oplus x = 0$ de *nilpotência*. Nestes casos a Proposição 2.3 não pode ser aplicada, e a análise será discutida abaixo.

Lema 2.6 (Complexidade do Problema Geral de $ACUN, ACUNh$ -unificação). *Solubilidade de problemas gerais de E -unificação são NP-difíceis quando $E = ACUN, ACUNh$.*

Demonstração. Seja o problema de E -unificação $\Gamma = \{x \oplus y \oplus z = a \oplus b \oplus c\}$, por \oplus ser comutativo e associativo então as seguintes substituições são E -unificadores de Γ : $\sigma_a = \{x \mapsto a, y \mapsto b, z \mapsto c\}$, $\sigma_b = \{x \mapsto b, y \mapsto a, z \mapsto c\}$ e $\sigma_c = \{x \mapsto c, y \mapsto a, z \mapsto b\}$.

Tomando $\vec{x} = \langle x, y, z \rangle$ então as substituições acima são \vec{x} -atômicas e em particular $x\sigma_a = a$, $x\sigma_b = b$, $x\sigma_c = c$, portanto Γ possui a propriedade 1. da Proposição 2.3. Seja σ um E -unificador \vec{x} -atômico de Γ então, por definição, $x\sigma, y\sigma, z\sigma \in (\Sigma^{(0)} \setminus \Sigma_E) \dot{\cup} \mathcal{V}$. Por outro lado obtemos $x\sigma \oplus y\sigma \oplus z\sigma =_E a \oplus b \oplus c$.

Suponha, por absurdo, que $x\sigma \notin \{a, b, c\}$. Então, $x\sigma = w$ e w é uma variável ou uma constante que não está em Σ_E e não ocorre no lado direito da equação de Γ . Porém, $w \oplus y\sigma \oplus z\sigma =_E a \oplus b \oplus c$ e então, por w não ocorrer no lado direito temos que utilizar as regras de Nilpotência e Unidade para ignorar w na equação, o que implica que w é subtermo de $y\sigma$ ou subtermo de $z\sigma$. Como σ é \vec{x} -atômico então $y\sigma, z\sigma$ são constantes ou variáveis daí $y\sigma = w$ ou $z\sigma = w$, e portanto, conclui-se que $z\sigma = a \oplus b \oplus c$ ou $y\sigma = a \oplus b \oplus c$ uma contradição, pois σ é \vec{x} -atômico. Assim $x\sigma \in \{a, b, c\}$ e Γ possui a propriedade 2. da Proposição 2.3.

Como $E = ACUN$, $ACUNh$ são consistentes, pela proposição 2.3 o resultado segue.

□

Capítulo 3

Um algoritmo eficiente para ACUNh-unificação

Apresentaremos o algoritmo \mathcal{J}_{XORh} proposto por Liu [18], para resolver problemas de ACUNh-unificação no caso geral. O algoritmo opera em problemas de ACUNh-unificação que estejam em sua forma "purificada", isto é, para cada $S \in \Gamma$ e t um subtermo de S , se $\text{raíz}(t) \neq \oplus, h$ temos que $\oplus, h \notin \Sigma(t)$ e se $t = h(t')$ então $\oplus, h \notin \Sigma(t')$.

Contribuímos com a demonstração que a regra de inferência *purificação* enunciada por Liu [18] é correta e terminante, além disso provamos a existência de uma ACUN(h)-extensão conservativa para cada problema Γ de ACUN(h)-unificação.

3.1 Purificação

Definição 3.1 (Termo puro). *Seja t um termo tal que $\text{raíz}(t) \neq \oplus$. Dizemos que t é um termo puro se, e somente se, para cada $p \in \text{Pos}(t) \setminus \{\varepsilon\}$ tem-se que $\text{raíz}(t|_p) \notin \{\oplus, h\}$. No caso em que $\text{raíz}(t) = h$ diremos que t é um h-termo puro.*

Definição 3.2 (Soma pura). *Seja S um termo, dizemos que S é uma soma pura se, e somente se, existem $n \geq 2$ e t_1, \dots, t_n termos puros tais que $S =_{AC} t_1 \oplus \dots \oplus t_n$ e existe no máximo um $i \in \{1, \dots, n\}$ tal que $\text{raíz}(t_i) = h$. Seja t um termo puro, denotaremos por $t \in_{\oplus} S$ se, e somente se, t é um argumento de*

Então vamos purificar cada equação de Γ , observe que as equações (2) e (3) já estão purificadas, então vamos aplicar a regra de purificação sobre (1):

Observe que os termos $a \oplus h(x) \oplus y$ e $b \oplus z \oplus h(x)$ são somas puras e abaixo de um símbolo de função $f \neq \oplus$ e portanto podemos aplicar a regra sobre esses termos, resultando em:

$$\Gamma' := \left\{ \begin{array}{ll} (1) & x \oplus h(x) \oplus f(v_1) \oplus f(v_2) \quad (4) \quad v_1 \oplus a \oplus x \oplus h(x) \oplus y \oplus w \\ (2) & h(z) \oplus w \oplus y \oplus b \oplus a \quad (5) \quad v_2 \oplus b \oplus z \oplus h(x) \\ (3) & 0 \end{array} \right\}$$

Γ' é irreduzível por [Purif].

Uma vez definida a regra de inferência Purificação, apresentaremos algumas propriedades e definições que serão necessárias para provar que todo problema de ACUNh-unificação Γ pode ser purificado para uma extensão conservativa de Γ .

Lema 3.1. *Sejam $\Gamma = \widehat{\Gamma} \cup \{S\}$, Γ' problemas de ACUNh-unificação tal que cada $T \in \Gamma$ está em sua forma normal módulo AC. Se $\Gamma \Rightarrow_{Purif} \Gamma'$ então Γ' é uma extensão conservativa de Γ tal que $\text{Var}(\Gamma) \subset \text{Var}(\Gamma')$ e para todo $S' \in \Gamma'$ tem-se que S' está em sua forma normal módulo AC.*

Demonstração. Como $\Gamma \Rightarrow_{Purif} \Gamma'$ então pela regra de purificação existem uma variável nova v , $S \in \Gamma$ e $p \in \text{Pos}(S) \setminus \{\varepsilon\}$ tais que $\Gamma = \widehat{\Gamma} \cup \{S\}$, $\Gamma' = \widehat{\Gamma} \cup \{S[v]_p, v \oplus S|_p\}$ satisfazendo as condições exibidas na regra acima.

1. Vamos provar que Γ' é uma extensão conservativa de Γ .

i) Seja σ um ACUNh-unificador de Γ' :

Então para cada $T \in \widehat{\Gamma}$, tem-se que $T\sigma =_{\oplus} 0$, vamos provar que $S\sigma =_{\oplus} 0$.

De fato, $(S[v]_p)\sigma =_{\oplus_h} 0$ e $(v \oplus S|_p)\sigma =_{\oplus_h} 0$ então, $(S\sigma)[v\sigma]_p =_{\oplus_h} 0$ e $v\sigma =_{\oplus_h} (S\sigma)|_p$.

Portanto, $S\sigma =_{\oplus_h} (S\sigma)[(S\sigma)|_p] =_{\oplus_h} (S\sigma)[v\sigma]_p =_{\oplus_h} 0$ e σ é um ACUNh-unificador de Γ .

ii) Seja σ um ACUNh-unificador de Γ , em particular σ é um ACUNh-unificador de $\widehat{\Gamma}$.

Tome $\gamma = \{v \mapsto (S|_p)\sigma\}$, vamos provar que $\sigma\gamma$ é de fato, um ACUNh-unificador de Γ' .

Como σ é um ACUNh-unificador de $\widehat{\Gamma}$, então $\sigma\gamma$ é um ACUNh-unificador de $\widehat{\Gamma}$, então é suficiente provar que $(S[v]_p)\sigma\gamma =_{\oplus_h} 0$ e $(v \oplus S|_p)\sigma\gamma =_{\oplus_h} 0$.

Observe que podemos supor que $v \notin \mathcal{V}ar(\mathcal{I}m(\sigma))$ pois v é uma variável nova, então $S\sigma\gamma = S\sigma$. Portanto temos, $(S[v]_p)\sigma\gamma = (S\sigma\gamma)[v\sigma\gamma]_p = (S\sigma)[v\gamma]_p = (S\sigma)[(S\sigma)|_p]_p = S\sigma$.

Como σ é ACUNh-unificador de Γ , temos que $S\sigma\gamma =_{\oplus_h} 0$, portanto $(S[v]_p)\sigma =_{\oplus_h} 0$, por outro lado temos $(v \oplus S|_p)\sigma\gamma = v\gamma \oplus (S|_p)\sigma = (S|_p)\sigma \oplus (S|_p)\sigma =_{\oplus_h} 0$. Portanto $\sigma\gamma$ é um ACUNh-unificador de Γ' e $\mathcal{D}om(\gamma) = \{v\} \subseteq \mathcal{V}ar(\Gamma') \setminus \mathcal{V}ar(\Gamma)$.

2. $\mathcal{V}ar(\Gamma) \subset \mathcal{V}ar(\Gamma')$.

Dado $x \in \mathcal{V}ar(S)$ existe uma posição $q \in \mathcal{P}os(S)$ tal que $S|_q = x$, então q é uma posição variável, e por $S|_p$ é uma soma pura então $q \not\leq p$ assim temos apenas dois casos, $p \leq q$ ou $p||q$.

i) Se $p \leq q$ então existe um $p' \in \mathcal{P}os(S)$ tal que $q = pp'$, logo $S|_q = S|_{pp'} = (S|_p)|_{p'}$ e portanto $x \in \mathcal{V}ar(S|_p)$ e como $v \oplus S|_p \in \Gamma'$ temos que $x \in \mathcal{V}ar(\Gamma')$.

ii) Se $p||q$ então $(S[v]_p)|_q = S|_q = x$ assim $x \in \mathcal{V}ar(S[v]_p)$ e portanto $x \in \mathcal{V}ar(\Gamma')$.

Assim como em ambos os casos obtemos que $x \in \mathcal{V}ar(\Gamma')$, conclui-se que $\mathcal{V}ar(\Gamma) \subseteq \mathcal{V}ar(\Gamma')$ e como $v \in \mathcal{V}ar(\Gamma')$ e v é uma variável nova temos que $v \notin \mathcal{V}ar(\Gamma)$ e portanto $\mathcal{V}ar(\Gamma) \subset \mathcal{V}ar(\Gamma')$.

3. Para todo $T \in \Gamma'$, T está em sua forma normal com relação a \mathcal{R}_{\oplus_h} módulo AC .

Por hipótese, S é um termo irreduzível com relação a \mathcal{R}_{\oplus_h} . Basta provar que $S[v]_p$ e $v \oplus S|_p$ são irreduzíveis, de fato, por v ser uma variável nova em S então só há uma ocorrência de v em $S[v]_p$, como não foi inserido nenhum termo encabeçado por h , temos que a única forma de $S[v]_p$ ser redutível seria por $v \oplus 0$, isso não ocorre pois caso contrário poderíamos reduzir por $S|_p \oplus 0$, um absurdo pois S está em sua forma normal. Por outro lado, $S|_p$ está em sua forma normal pois S está em sua forma normal e por $v \notin \mathcal{V}ar(S|_p)$ temos que $v \oplus S|_p$ está em sua forma normal.

□

Vamos mostrar que a aplicação exaustiva da regra purificação em um problema Γ em sua forma padronizada de fato nos retorna um problema em sua forma pura, para isso vamos definir alguns conceitos importantes para mostrar que \implies_{Purif} é terminante, correta e confluenta a menos renomeamento das variáveis. A seguir assumiremos que todos os termos estão em suas formas normais a menos que seja mencionado ao contrário.

Seja S um termo, o conjunto de *somas puras internas de S* , denotado por S_{\oplus} , é dado por:

$$S_{\oplus} := \left\{ p \in \mathcal{Pos}(S) \mid \begin{array}{l} S|_p \text{ é uma soma pura e existe } q \in \mathcal{Pos}(S) \\ \text{tal que } p = qi \text{ e } \text{raíz}(S|_q) \neq \oplus, \text{ para } i \in \mathbb{N} \end{array} \right\}$$

Similarmente, o conjunto de *h -subtermos puros internos a S* , denotado por S_h , é dado por:

$$S_h := \left\{ p \in \mathcal{Pos}(S) \mid \begin{array}{l} S|_p \text{ é um } h\text{-termo puro e existe } q \in \mathcal{Pos}(S) \\ \text{tal que } p = qi \text{ e } \text{raíz}(S|_q) \neq \oplus, \text{ para } i \in \mathbb{N} \end{array} \right\}$$

A seguinte proposição consiste de propriedades simples sobre o conjunto de somas puras internas e o conjunto de h -termos puros internos de um termo S . Sendo o diagrama abaixo utilizado para melhor entendimento da demonstração.

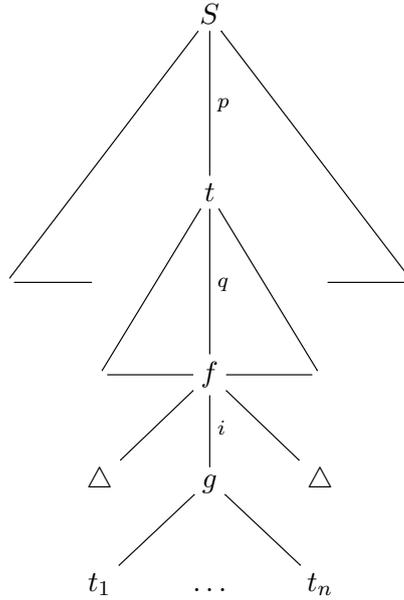


Figura 3.1: caso 3 da Proposição 3.1.

Proposição 3.1. *Seja S um termo em sua forma normal. Então:*

1. $S_{\oplus} \cap S_h = \emptyset$.
2. Se $p, p' \in S_{\oplus} \cup S_h$ e $p \neq p'$, então $p \parallel p'$.
3. Se t é um subtermo de S tal que $S|_p = t$ então para todo $q \in t_{\oplus} \cup t_h$, temos que $pq \in S_{\oplus} \cup S_h$.

Demonstração. Suponha S um termo em sua forma normal e t um subtermo de S tal que $S|_p = t$ onde $p \in \mathcal{Pos}(S)$.

1. Se $S_{\oplus} = \emptyset$ ou $S_h = \emptyset$ então nada a provar, caso contrário, tome $p \in S_{\oplus}$ qualquer, então $raíz(S|_p) = \oplus$, pois $S|_p$ é uma soma pura, e portanto temos $raíz(S|_p) \neq h$, dessa forma $p \notin S_h$, o resultado segue.
2. Sejam $p, p' \in S_{\oplus} \cup S_h$ e $p \neq p'$, então $S|_p$ e $S|_{p'}$ são termos puros encabeçados por h ou somas puras, logo existe $q, q' \in \mathcal{Pos}(S)$ tais que $p = qi$ e $p' = q'j$ tais que $raíz(S|_q) \neq \oplus$ e $raíz(S|_{q'}) \neq \oplus$ portanto supondo por absurdo que $p' \leq p$ então $S|_p$ é um subtermo de $S|_{p'}$ e como $p \neq p'$ então $S|_q$ também é subtermo de $S|_{p'}$, uma contradição pois $S|_{p'}$ é um h -termo ou uma soma pura, de forma totalmente análoga para o outro lado, assim $p \not\leq p'$ e $p' \not\leq p$, equivalentemente $p \parallel p'$.
3. Tome $p' \in t_{\oplus} \cup t_h$, então existe $q \in \mathcal{Pos}(t)$ e $i \in \mathbb{N}$ tal que $p' = qi$ onde $raíz(t|_q) = f \neq \oplus$ e $raíz(q) = g \in \{\oplus, h\}$ (diagrama 3.1). Note que $t = S|_p$ para alguma posição $p \in \mathcal{Pos}(S)$ então $pp' \in \mathcal{Pos}(S)$ e portanto $pp' = pqi$ onde $S|_{pq} = (S|_p)|_q = t|_q$, implicando que $pp' \in S_{\oplus} \cup S_h$.

□

O lema a seguir oferece uma ferramenta para determinarmos quando um termo é uma soma pura ou termo puro e será utilizado para provar que ao aplicar exaustivamente a regra de inferência purificação em Γ , obtemos uma extensão conservativa Γ' de Γ onde cada termo $S' \in \Gamma'$ é tal que $S'_{\oplus} = S'_h = \emptyset$.

Lema 3.2. $S_{\oplus} = S_h = \emptyset$ se, e somente se, S é um termo puro ou soma pura.

Demonstração. (\Rightarrow) Suponha que $S_{\oplus} = S_h = \emptyset$.

1. Suponha, por absurdo, que $raíz(S) \neq \oplus$ e que S não seja um termo puro, então existe um $q' \in \mathcal{Pos}(t) \setminus \{\varepsilon\}$ tal que $raíz(S|_{q'}) \in \{\oplus, h\}$, portanto existem posições $p, q \in \mathcal{Pos}(S)$ tal que $S|_p$ é uma soma pura ou um termo puro encabeçado por h e $p = qi$ tal que $raíz(S|_q) \neq \oplus$, pois $raíz(S) \neq \oplus$, implicando que $p \in S_{\oplus} \cup S_h = \emptyset$, uma contradição. Assim S é um termo puro.
2. Suponha $S = t_1 \oplus \dots \oplus t_n$ para algum $n \in \mathbb{N}$ e para cada $i \in \{1, \dots, n\}$ temos $raíz(t_i) \neq \oplus$. Pelo item 3. do Lema 3.1 temos que para cada $i \in \{1, \dots, n\}$ tem-se que $(t_i)_{\oplus} \cup (t_i)_h = \emptyset$. Então

pelo item anterior, concluímos que para cada $i \in \{1, \dots, n\}$ tem-se que t_i é um termo puro e como $S =_{AC} t_1 \oplus \dots \oplus t_n$ em sua forma normal então S é uma soma pura.

(\Leftarrow) Seja S um termo puro ou soma pura, suponha por absurdo que $S_{\oplus} \cup S_h \neq \emptyset$, assim existe um $p \in S_{\oplus} \cup S_h$.

- Se $p \in S_{\oplus}$ então existem $p, q \in \mathcal{Pos}(S)$ tal que $S|_p$ é uma soma pura, $p = qi$ e $raíz(S|_q) \neq \oplus$, portanto S não é um termo puro, pois \oplus ocorre em S . Logo S é uma soma pura, isto é, $S = t_1 \oplus \dots \oplus t_n$, com t_i é um termo puro para cada $i \in \{1, \dots, n\}$. Como $raíz(S|_q) \neq \oplus$ e $S|_q$ é um subtermo de S , temos que $S|_q$ é subtermo de t_i para algum i , assim $S|_p$ é subtermo de t_i , e portanto \oplus ocorre em t_i , uma contradição pois t_i é um termo puro.
- Se $p \in S_h$ então existem $p, q \in \mathcal{Pos}(S)$ tal que $S|_p$ é um h -termo tal que $p = qi$ e $raíz(S|_q) \neq \oplus$, portanto S não é um termo puro, uma vez que símbolo h ocorre em S numa posição fora da raiz $p \neq \varepsilon$, que é uma contradição. Logo S é uma soma pura e $S = t_1 \oplus \dots \oplus t_n$, com t_i um termo puro para cada $i \in \{1, \dots, n\}$. Como $raíz(S|_q) \neq \oplus$ e $S|_q$ é um subtermo de S , temos que $S|_q$ é subtermo de t_i para algum i , assim $S|_p$ é subtermo de t_i , e portanto h ocorre em t_i que não seja na raiz pois $p \neq \varepsilon$, uma contradição pois t_i é um termo puro.

Como em ambos os casos encontramos uma contradição, obtemos que não existe $p \in S_{\oplus} \cup S_h$, portanto $S_{\oplus} = S_h = \emptyset$.

□

Dado um problema de ACUNh-unificação Γ e $S \in \Gamma$, a *profundidade das somas internas de S* , denotado por $\|S\|_{\oplus}$, é dado por:

$$\|S\|_{\oplus} := \begin{cases} \text{máx}\{\text{len}(p) \mid p \in S_{\oplus}\}, & \text{se } S_{\oplus} \neq \emptyset \\ 0, & \text{caso contrário} \end{cases}$$

Esta noção pode ser estendida para Γ , isto é, a *profundidade das somas internas do problema Γ* é dada por: $\|\Gamma\|_{\oplus} := \{\text{máx}\{\|S\|_{\oplus} \mid S \in S_{\oplus}\}$.

Similarmente, a *profundidade dos h -subtermos internos de S* , denotado por $\|S\|_h$, é dado por:

$$\|S\|_h := \begin{cases} \text{máx}\{\text{len}(p) \mid p \in S_h\}, & \text{if } S_h \neq \emptyset \\ 0, & \text{caso contrário} \end{cases}$$

A profundidade dos h -subtermos internos do problema Γ é dada por: $\|\Gamma\|_h := \{\text{máx}\{\|S\|_h \mid S \in S_h\}\}$.

Provaremos agora uma condição necessária e suficiente para aplicação da regra purificação.

Lema 3.3. *Seja Γ um problema de ACUNh-unificação. $\|\Gamma\|_{\oplus} + \|\Gamma\|_h > 0$ se, e somente se, existe Γ' tal que $\Gamma \implies_{Purif} \Gamma'$*

Demonstração. (\implies) Suponha $\|\Gamma\|_{\oplus} + \|\Gamma\|_h > 0$, então como $\|\Gamma\|_{\oplus} \geq 0$ e $\|\Gamma\|_h \geq 0$, temos que $\|\Gamma\|_{\oplus} > 0$ ou $\|\Gamma\|_h > 0$. A prova se divide em dois casos:

1. $\|\Gamma\|_{\oplus} > 0$: Pela definição de $\|\Gamma\|_{\oplus}$ existe um $S \in \Gamma$ tal que $\|S\|_{\oplus} = \|\Gamma\|_{\oplus} > 0$, portanto existe uma posição $p \in S_{\oplus}$, isto é, $S|_p$ é uma soma pura e existe $q \in \mathcal{Pos}(S)$ com $p = qi$ e $\text{raíz}(S|_q) \neq \oplus$. Como $p \neq \varepsilon$, S cumpre condições da regra de purificação, logo é possível aplicá-la, pois $p \neq \varepsilon$.
2. $\|\Gamma\|_h > 0$: Pela definição de $\|\Gamma\|_h$ existe um $S \in \Gamma$ tal que $\|S\|_h = \|\Gamma\|_h > 0$, portanto existe uma posição $p \in S_h$, isto é, $S|_p$ é um h -termo e existe $q \in \mathcal{Pos}(S)$ tal que $p = qi$ e $\text{raíz}(S|_q) \neq \oplus$, ou seja, S cumpre as condições da regra de purificação.

Como em ambos os casos é possível aplicar a regra de inferência purificação, então concluímos que é suficiente $\|\Gamma\|_{\oplus} + \|\Gamma\|_h > 0$ para aplicar a regra.

(\impliedby) Suponha exista Γ' tal que $\Gamma \implies_{Purif} \Gamma'$. Então existe $S \in \Gamma$ e $p \in \mathcal{Pos}(S) \setminus \{\varepsilon\}$ tais que $S|_p$ é uma soma pura ou um h -termo tal que existe $q \in \mathcal{Pos}(S)$ com $p = qi$ com $i \in \mathbb{N}$ e $\text{raíz}(S|_q) \neq \oplus$. Portanto temos que $p \in S_{\oplus} \cup S_h$, e por conseguinte, $\|S\|_{\oplus} > 0$ ou $\|S\|_h > 0$.

Pela definição de $\|\Gamma\|_h$ e $\|\Gamma\|_{\oplus}$, temos $\|\Gamma\|_{\oplus} \geq \|T\|_{\oplus}$ e $\|\Gamma\|_h \geq \|T\|_h$ para cada $T \in \Gamma$ em particular para S , logo $\|\Gamma\|_{\oplus} + \|\Gamma\|_h \geq \|S\|_{\oplus} + \|S\|_h > 0$. \square

Nos resultados a seguir vamos assumir que $\Gamma = \widehat{\Gamma} \cup \{S\}$ e $\Gamma' = \widehat{\Gamma} \cup \{S[v]_p, v \oplus S|_p\}$, problemas de ACUNh-unificação.

Lema 3.4. *Se $\Gamma \implies_{Purif} \Gamma'$ então, as seguintes propriedades são válidas.*

- i) $\|v \oplus S|_p\|_{\oplus} = \|v \oplus S|_p\|_h = 0$
- ii) $\|\Gamma'\|_{\oplus} = \text{máx}\{\|\widehat{\Gamma}\|_{\oplus}, \|S[v]_p\|_{\oplus}\}$
- iii) $\|\Gamma'\|_h = \text{máx}\{\|\widehat{\Gamma}\|_h, \|S[v]_p\|_h\}$

Demonstração. Sejam Γ, Γ' como na hipótese. Como $S|_p$ é uma soma pura ou um h -termo, pelo Lema 3.2 temos que $\|S|_p\|_{\oplus} = \|S|_p\|_h = 0$ e como v é uma variável nova, segue que $v \oplus S|_p$ é uma soma pura irredutível, então novamente pelo Lema 3.2, temos $\|v \oplus S|_p\|_{\oplus} = \|v \oplus S|_p\|_h = 0$, assim provamos o resultado (i), os dois outros itens são consequências diretas do item(i). \square

Proposição 3.2. *Suponha que $\Gamma \implies_{\text{purif}} \Gamma'$. Então,*

1. *Se $p \in S_{\oplus}$ então $(S[v]_p)_h \cap S_h = S_h$ e $(S[v]_p)_{\oplus} \cap S_{\oplus} = S_{\oplus} \setminus \{p\}$.*
2. *Se $p \in S_h$ então $(S[v]_p)_{\oplus} \cap S_{\oplus} = S_{\oplus}$ e $(S[v]_p)_h \cap S_h = S_h \setminus \{p\}$.*

Demonstração. Sejam Γ e Γ' como na hipótese.

1. Suponha $p \in S_{\oplus}$.

(a) $(S[v]_p)_h \cap S_h = S_h$.

No caso em que $(S[v]_p)_h \cap S_h \subseteq S_h$, a prova é trivial.

Vamos mostrar que $S_h \subseteq (S[v]_p)_h \cap S_h$:

Seja $q \in S_h$, então $S|_q$ é um h -termo puro tal que existe $q' \in \mathcal{P}os(S)$, com $q = q'j$ e $raíz(S|_{q'}) \neq \oplus$. Pela Proposição 3.1 segue que $q||p$ e, portanto $(S[v]_p)|_q = S|_q$. Logo, $(S[v]_p)|_q$ é um h -termo puro.

Como $S|_p$ é uma soma pura, segue que $p \not\leq q'$. Vamos analisar os seguintes casos:

- Se $q' \leq p$ então $p = q'l$ e portanto $(S[v]_p)|_{q'} = (S[v]_{q'l})_{q'} = (S|_{q'})[v]_p$ pela Proposição 1.1. Assim, $\oplus \neq raíz(S|_{q'}) = raíz((S|_{q'})[v]_p) = raíz((S[v]_p)|_{q'})$.
- Se $q' || p$ então $(S[v]_p)|_{q'} = raíz(S|_{q'})$. Assim, $raíz((S[v]_p)|_{q'}) \neq \oplus$.

Logo, $raíz((S[v]_p)|_{q'}) \neq \oplus$ e, portanto $q \in (S[v]_p)_h \cap S_h$

(b) $(S[v]_p)_{\oplus} \cap S_{\oplus} = S_{\oplus} \setminus \{p\}$.

- $(S[v]_p)_{\oplus} \cap S_{\oplus} \subseteq S_{\oplus} \setminus \{p\}$:

Tome $q \in (S[v]_p)_{\oplus} \cap S_{\oplus}$, então $q \in (S[v]_p)_{\oplus}$ e, portanto $(S[v]_p)|_q$ é uma soma pura.

Como $(S[v]_p)|_p = v$ é uma variável, segue que $q \neq p$. Portanto $q \in S_{\oplus} \setminus \{p\}$.

- $S_{\oplus} \setminus \{p\} \subseteq (S[v]_p)_{\oplus} \cap S_{\oplus}$:

Suponha $q \in S_{\oplus} \setminus \{p\}$, então $S|_q$ é uma soma pura tal que existe $q' \in \mathcal{P}os(S)$ com $q = q'j$ e $raíz(S|_{q'}) \neq \oplus$. Pela Proposição 3.1 segue que $q||p$. Assim $(S[v]_p)|_q = S|_q$ e, portanto $(S[v]_p)|_q$ é uma soma pura.

Como $S|_q$ é uma soma pura segue que $p \not\leq q'$. Temos que analisar os dois seguintes casos

- $q' \leq p$: neste caso, $p = q'l$, para algum l . Pela Proposição 1.1 segue que $(S[v]_p)|_{q'} = (S[v]_{q'l})|_{q'} = (S|_{q'})[v]_l$ e, portanto $raíz((S[v]_p)|_{q'}) = raíz(S|_{q'}) \neq \oplus$.
- $q' || p$: neste caso $(S[v]_p)|_{q'} = S|_{q'}$ o que implica em $raíz((S[v]_p)|_{q'}) \neq \oplus$.

Portanto $raíz((S[v]_p)|_{q'}) \neq \oplus$ e $q \in (S[v]_p)_{\oplus} \cap S_{\oplus}$.

2. Suponha $p \in S_h$.

A prova de que $(S[v]_p)_{\oplus} \cap S_{\oplus} = S_{\oplus}$ é idêntica ao caso acima, basta trocar \oplus por h .

□

Proposição 3.3. *Suponha que $\Gamma \implies_{Purif} \Gamma'$. Então,*

1. Para cada $q \in (S[v]_p)_{\oplus} \setminus S_{\oplus}$, $len(q) < len(p)$.
2. Para cada $q \in (S[v]_p)_h \setminus S_h$, $len(q) < len(p)$.

Demonstração. 1. Para cada $q \in (S[v]_p)_{\oplus} \setminus S_{\oplus}$, $len(q) < len(p)$:

Suponha $q \in (S[v]_p)_{\oplus} \setminus S_{\oplus}$. Então $(S[v]_p)|_q$ é uma soma pura então $q \neq p$ pois $(S[v]_p)|_p = v$, uma variável.

Por outro lado por $q \in (S[v]_p)_{\oplus}$, então existe $q' \in \mathcal{P}os(S[v]_p)$ tal que $q = q'j$ com $j \in \mathbb{N}$ e $raíz((S[v]_p)|_{q'}) \neq \oplus$, logo $p \not\leq q$ e $p \not\leq q'$ pois $(S[v]_p)|_p = v$ uma variável, então $q \leq p$ ou $q||p$.

Suponha por absurdo que $q||p$, pela Proposição 1.1 temos que $\mathcal{P}os(S[v]_p) \subseteq \mathcal{P}os(S)$ logo $q, q' \in \mathcal{P}os(S)$ e $(S[v]_p)|_q = S|_q$ implicando que $S|_q$ é uma soma pura, daí existem dois casos a serem estudados, $q' \leq p$ ou $q' || p$:

- Se $q' || p$ então $(S[v]_p)|_q = S|_q$ e $(S[v]_p)|_{q'} = S|_{q'}$, portanto $S|_q$ é uma soma pura e $raíz(S|_{q'}) \neq \oplus$, assim $q \in S_{\oplus}$ uma contradição.

- Se $q' \leq p$ então $p = q'r$ e por $q' \in \mathcal{Pos}(S)$ temos que $(S[v]_p)|_{q'} = (S|_{q'})[v]_r$ implicando que $\text{raíz}(S|_{q'}) \neq \oplus$, portanto $q \in S_{\oplus}$ uma contradição.

E assim segue que $p \neq q$ e portanto $\text{len}(q) < \text{len}(p)$.

2. Para cada $q \in (S[v]_p)_{\oplus} \setminus S_{\oplus}$, $\text{len}(q) < \text{len}(p)$:

Este casos é análogo ao anterior.

□

3.1.1 Terminação e correção de [Purif]

Definição 3.5 (Medida μ). *Seja Γ um problema de ACUNh-unificação e $S \in \Gamma$, então definimos a seguinte medida μ para terminação.*

- $\mu(S) := \text{máx}\{\|S\|_{\oplus}, \|S\|_h\}$
- $\mu(\Gamma) := \text{máx}\{\mu(S) \mid S \in \Gamma\}$

Lema 3.5. *Seja Γ um problema de ACUNh-unificação. $\mu(\Gamma) > 0$ se, e somente se, é possível aplicar a regra [Purif] em Γ .*

Demonstração. Seja Γ um problema de ACUNh-unificação temos que por definição $\|\Gamma\|_{\oplus} \geq 0$ e $\|\Gamma\|_h \geq 0$, então $\|\Gamma\|_{\oplus} + \|\Gamma\|_h > 0$ se, e somente se, $\|\Gamma\|_{\oplus} > 0$ ou $\|\Gamma\|_h > 0$ se, e somente se, $\mu(\Gamma) > 0$ e o resultado segue. □

Corolário 3.1. *Seja Γ um problema de ACUNh-unificação. Γ está em sua forma normal com relação a \implies_{Purif} se, e somente se, $\mu(\Gamma) = 0$.*

Demonstração. Pelo Lema 3.5 obtemos que $\mu(\Gamma) = 0$ se, e somente se, não for possível aplicar a regra [Purif] em Γ , equivalentemente, não existe um Γ' tal que $\Gamma \implies_{\text{Purif}} \Gamma'$, assim o resultado segue. □

Lema 3.6. *Sejam Γ, Γ' tais que, $\Gamma = \widehat{\Gamma} \cup \{S\} \implies_{\text{Purif}} \Gamma' = \widehat{\Gamma} \cup \{S[v]_p, v \oplus S|_p\}$ então $\mu(\Gamma') = \text{máx}\{\mu(\widehat{\Gamma}), \mu(S[v]_p)\}$.*

Demonstração. Como $\Gamma \implies_{\text{Purif}} \Gamma'$, segue que, pelo Lema 3.4 obtemos que

$$\|\Gamma'\|_{\oplus} = \text{máx}\{\|\widehat{\Gamma}\|_{\oplus}, \|S[v]_p\|_{\oplus}\} \text{ e } \|\Gamma'\|_h = \text{máx}\{\|\widehat{\Gamma}\|_h, \|S[v]_p\|_h\}$$

E portanto pela definição de μ concluimos que

$$\begin{aligned}\mu(\Gamma') &= \text{máx}\{\|\Gamma'\|_{\oplus}, \|\Gamma'\|_h\} \\ &= \text{máx}\{\text{máx}\{\|\widehat{\Gamma}\|_{\oplus}, \|S[v]_p\|_{\oplus}\}, \text{máx}\{\|\widehat{\Gamma}\|_h, \|S[v]_p\|_h\}\} \\ &= \text{máx}\{\mu(\widehat{\Gamma}), \mu(S[v]_p)\}\end{aligned}$$

□

Lema 3.7. *Seja Γ um problema de ACUNh-unificação. Γ está em sua forma pura se, e somente se, $\mu(\Gamma) = 0$.*

Demonstração. Seja Γ um problema de ACUNh-unificação padronizado, então cada elemento de Γ está em sua forma normal.

(\Rightarrow) Suponha Γ em sua forma pura, então para cada $S \in \Gamma$ temos que S é uma soma pura ou um termo puro, e pelo Lema 3.2, $S_{\oplus} = S_h = \emptyset$. Portanto para cada $S \in \Gamma$, $\mu(S) = 0$, implicando que $\mu(\Gamma) = 0$

(\Leftarrow) Suponha que $\mu(\Gamma) = 0$, então para cada $S \in \Gamma$ temos que $\mu(S) = 0$ e portanto pela definição de μ temos que $0 \leq \|S\|_{\oplus}, \|S\|_h \leq 0$, isto é, $S_{\oplus} = S_h = \emptyset$ e portanto S é um termo puro ou soma pura pelo Lema 3.2, implicando que Γ está em sua forma pura. □

Pelo Lema 3.1.1 e o corolário do Lema 3.5, torna-se evidente que dado Γ um problema de ACUNh-unificação, para encontrarmos Γ' um problema de ACUNh-unificação em sua forma pura que é uma extensão conservativa de Γ devemos olhar as formas normais de Γ com relação a \Longrightarrow_{Purif} , então precisamos garantir existência de uma forma normal com relação a \Longrightarrow_{Purif} , além disso, para computarmos uma forma pura precisaremos garantir que a regra de inferência purificação termina.

O próximo lema, diz que ao aplicarmos a regra [Purif] exhaustivamente, independentemente da escolha das variáveis em cada passo, temos que a medida μ eventualmente será reduzida, implicando que para cada Γ existe um ramo de aplicações de regras purificação onde μ é reduzida, porém isso não é suficiente para a demonstração da terminação, pois garante apenas a existência de uma forma normal com relação a relação \Longrightarrow_{Purif} para cada problema Γ de ACUNh-unificação. Então será necessário mostrar que a menos de escolhas de variáveis novas, a regra \Longrightarrow_{Purif} é confluenta.

Lema 3.8. *Seja Γ um problema de ACUNh-unificação. Se $\mu(\Gamma) > 0$ então, existem $n \geq 1$ e um problema Γ' de ACUNh-unificação tais que $\Gamma \Longrightarrow_{Purif}^n \Gamma'$ e $\mu(\Gamma') < \mu(\Gamma)$.*

Demonstração. Suponha $\mu(\Gamma) > 0$. Vamos definir os seguintes conjuntos auxiliares para a demonstração.

- $T_\Gamma := \{S \in \Gamma \mid \mu(S) = \mu(\Gamma)\}$
- Para cada $S \in T_\Gamma$, definimos $P_{S,\Gamma} := \{p \in S_\oplus \cup S_h \mid \text{len}(p) = \mu(S)\}$

Como $\mu(\Gamma) > 0$ então existe um $S \in \Gamma$ tal que $\mu(S) = \mu(\Gamma)$, assim $T_\Gamma \neq \emptyset$ e para cada $S \in T_\Gamma$ tem-se que $P_{S,\Gamma} \neq \emptyset$, vamos fixar um $S \in T_\Gamma$ qualquer. Como $P_{S,\Gamma} \neq \emptyset$ então existe um $p \in P_{S,\Gamma}$.

Denotaremos $\Gamma', \widehat{\Gamma}$ e $\overline{\Gamma}$ problemas de ACUNh-unificação.

Hipótese de indução 1: Suponha por indução sobre $|P_{S,\Gamma}| = n \geq 1$ e seja um problema $\overline{\Gamma}$ de ACUNh-unificação tal que $\mu(\overline{\Gamma}) > 0$, se $|T_{\overline{\Gamma}}| = |T_\Gamma|$ e existe $\overline{S} \in T_{\overline{\Gamma}}$ tal que $|P_{\overline{S},\overline{\Gamma}}| < |P_{S,\Gamma}|$ então existem $m \geq 1$, um problema $\widehat{\Gamma}$ tais que $\overline{\Gamma} \xrightarrow{m}_{Purif} \widehat{\Gamma}$ com $T_{\widehat{\Gamma}} = T_{\overline{\Gamma}} \setminus \{\overline{S}\}$ ou $\mu(\widehat{\Gamma}) < \mu(\overline{\Gamma})$.

Hipótese de indução 2: Suponha por indução sobre $|T_\Gamma| = n \geq 1$ que se Γ' é um problema com $\mu(\Gamma') > 0$ e $|T_{\Gamma'}| < |T_\Gamma|$ então existem $\overline{\Gamma}$ e $m' \geq 1$ tais que $\Gamma' \xrightarrow{m'}_{Purif} \overline{\Gamma}$ e $\mu(\overline{\Gamma}) < \mu(\Gamma')$.

Caso base da indução 1: Suponha $|P_{S,\Gamma}| = 1$, então $P_{S,\Gamma} = \{p\} \subseteq S_\oplus \cup S_h$, assim vamos aplicar a regra [Purif] em S sobre p obtendo:

$$\frac{\Gamma = \widehat{\Gamma} \cup \{S\}}{\Gamma' = \widehat{\Gamma} \cup \{S[v]_p, v \oplus S|_p\}} \text{ Purif}$$

E pelo Lema 3.6 temos que $\mu(\Gamma') = \max\{\mu(\widehat{\Gamma}), \mu(S[v]_p)\}$

Como temos não existem posições $q \in S_\oplus$, tai que $q||p$, uma vez que essa seria uma posição em $P_{S,\Gamma}$, diferente de p . E como,

$$\|S[v]_p\|_\oplus = \max\{\text{len}(q) \mid q \in (S[v]_p)_\oplus \cup \{\varepsilon\}\} \text{ e } \|S[v]_p\|_h = \max\{\text{len}(q) \mid q \in (S[v]_p)_h \cup \{\varepsilon\}\}$$

obtemos $\|S[v]_p\|_\oplus < \text{len}(p)$ e $\|S[v]_p\|_h < \text{len}(p)$ e portanto obtemos

$$\mu(S[v]_p) < \text{len}(p) = \mu(S) = \mu(\Gamma) \quad (3.1)$$

Para provarmos o caso base temos que verificar dois novos possíveis casos.

- $|T_\Gamma| = 1$:

Então $T_\Gamma = \{S\}$ e como para todo $\widehat{S} \in \widehat{\Gamma}$ temos que $S \neq \widehat{S}$, implica que $\widehat{S} \notin T_\Gamma$, equivalentemente, $\mu(\widehat{S}) < \mu(\Gamma)$, implicando que $\mu(\widehat{\Gamma}) < \mu(\Gamma)$.

- $|T_\Gamma| > 1$:

Então existe $\widehat{S} \in T_\Gamma \setminus \{S\}$ logo $\mu(\widehat{S}) = \mu(S)$ e $\widehat{S} \in \widehat{\Gamma} \subseteq \Gamma'$ portanto $\mu(\Gamma') \geq \mu(\Gamma)$. Por outro lado, como $\Gamma' = \widehat{\Gamma} \cup \{S[v]_p, v \oplus S|_p\}$:

1. Pelo Lema 3.4 temos que $\mu(v \oplus S|_p) = 0 < \mu(\Gamma)$.
2. Pela equação 3.1 temos $\mu(S[v]_p) < \mu(\Gamma)$, logo $S[v]_p, v \oplus S|_p \notin T_{\Gamma'}$, implicando que se $S' \in T_{\Gamma'}$ então $S' \in \widehat{\Gamma}$, logo $\mu(\Gamma') = \mu(S') \leq \mu(\Gamma)$, concluímos que $\mu(\Gamma) = \mu(\Gamma')$, e então $T_{\Gamma'} = T_\Gamma \setminus \{S\}$.

Assim concluímos o caso base da indução 1, vamos provar agora o caso base da indução 2 supondo que vale a hipótese de indução (1).

Passo indutivo da indução (1): Suponha $|P_{S,\Gamma}| = n > 1$, então existem $p, p' \in P_S \subseteq S_\oplus \cup S_h$ posições distintas. Vamos aplicar a regra de inferência purificação em S na posição p , obtendo:

$$\frac{\Gamma = \widehat{\Gamma} \cup \{S\}}{\Gamma' = \widehat{\Gamma} \cup \{S[v]_p, v \oplus S|_p\}} \text{ Purif}$$

e portanto $\mu(\Gamma') = \max\{\mu(\widehat{\Gamma}), \mu(S[v]_p)\}$ Como $p \in S_\oplus \cup S_h$ então pela Proposição 3.2 temos que vale um dos seguintes resultados:

- $(S[v]_p)_\oplus \cap S_\oplus = S_\oplus \setminus \{p\}$ e $(S[v]_p)_h \cap S_h = S_h$ ou,
- $(S[v]_p)_\oplus \cap S_\oplus = S_\oplus$ e $(S[v]_p)_h \cap S_h = S_h \setminus \{p\}$

Observe que $(S_\oplus \cup S_h) \setminus \{p\} = (S_\oplus \setminus \{p\}) \cup (S_h \setminus \{p\})$ e portanto para cada $p' \in P_{S,\Gamma} \setminus \{p\} \subseteq (S_\oplus \cup S_h) \setminus \{p\}$ temos que $p' \in (S_\oplus \setminus \{p\}) \cup (S_h \setminus \{p\})$, isto é,

$$p' \in [(S[v]_p)_\oplus \cap S_\oplus] \cup [(S[v]_p)_h \cap S_h] \subseteq (S[v]_p)_\oplus \cup (S[v]_p)_h \quad (3.2)$$

A partir da equação acima obtemos os seguintes resultados:

1. $\mu(\Gamma') = \mu(\Gamma)$.

Para cada $q \in (S[v]_p)_\oplus \cup (S[v]_p)_h$, tem-se que $\mu(\Gamma') \geq \text{len}(q)$ em particular $\mu(\Gamma') \geq \text{len}(p') = \mu(\Gamma)$. Por outro lado, se $q \in (S[v]_p)_\oplus \cup (S[v]_p)_h \setminus (S_\oplus \cup S_h) = [(S[v]_p)_\oplus \setminus S_\oplus] \cup [(S[v]_p)_h \setminus S_h]$ então pelo Proposição 3.3 temos que $\text{len}(q) < \text{len}(p) = \text{len}(p')$, e como para cada $q \in S_\oplus \cup S_h$ temos que $\text{len}(q) \leq \text{len}(p) = \mu(\Gamma)$, assim $\mu(\Gamma') \leq \mu(\Gamma)$. Portanto, $\mu(\Gamma') = \mu(\Gamma) > 0$.

2. $S[v]_p \in T_{\Gamma'}$.

Note que $\mu(v \oplus S|_p) = 0 < \mu(\Gamma')$ então $v \oplus S|_p \notin T_{\Gamma'}$. Por outro lado $p' \in (S[v]_p)_\oplus \cup (S[v]_p)_h$ então $\mu(\Gamma') = \text{len}(p') \leq \mu(S[v]_p) \leq \mu(\Gamma')$, equivalentemente,

$$\mu(\Gamma') = \text{len}(p') = \mu(S[v]_p) \Rightarrow S[v]_p \in T_{\Gamma'}$$

3. $T_{\Gamma'} = (T_\Gamma \setminus \{S\}) \cup \{S[v]_p\}$.

Como $\widehat{\Gamma} \subseteq \Gamma'$, temos que $(T_\Gamma \setminus \{S\}) \cup \{S[v]_p\} \subseteq T_{\Gamma'}$. Para todo $S' \in \Gamma'$, temos que $S' \in \widehat{\Gamma}$ ou $S' \in \{S[v]_p, v \oplus S|_p\}$, então $T_{\Gamma'} \subseteq (T_\Gamma \setminus \{S\}) \cup \{S[v]_p\}$. Daí, $T_{\Gamma'} = (T_\Gamma \setminus \{S\}) \cup \{S[v]_p\}$.

4. $|P_{S[v]_p, \Gamma'}| < |P_{S, \Gamma}|$. Basta provar que $P_{S[v]_p, \Gamma'} \subseteq P_{S, \Gamma}$, pois temos que $(S[v]_p)|_p = v$ implicando que $p \notin P_{S[v]_p, \Gamma'}$.

Tome $q \in P_{S[v]_p, \Gamma'} \subseteq (S[v]_p)_\oplus \cup (S[v]_p)_h$ então $\text{len}(q) = \mu(S[v]_p) = \mu(S) = \text{len}(p)$. Suponha por absurdo que $q \notin S_\oplus \cup S_h$ então obtemos que $q \in [(S[v]_p)_\oplus \setminus S_\oplus] \cup [(S[v]_p)_h \setminus S_h]$ e pela Proposição 3.3 temos $\text{len}(q) < \text{len}(p)$ uma contradição e portanto $q \in S_\oplus \cup S_h$, e como $\text{len}(q) = \text{len}(p) = \mu(\Gamma)$ temos que $q \in P_{S, \Gamma}$.

Assim podemos aplicar a hipótese de indução (1) em Γ' , e então existem um $m \geq 1$ e $\overline{\Gamma}$ tais que $\Gamma' \xRightarrow{m}_{Purif} \overline{\Gamma}$ onde ocorre

$$\mu(\overline{\Gamma}) < \mu(\Gamma') \text{ ou } T_{\overline{\Gamma}} = T_{\Gamma'} \setminus \{S[v]_p\}$$

Portanto temos $\Gamma \xRightarrow{m}_{Purif} \Gamma' \xRightarrow{m}_{Purif} \overline{\Gamma}$ com as seguintes propriedades,

- $\mu(\overline{\Gamma}) < \mu(\Gamma') = \mu(\Gamma)$ ou,
- $T_{\overline{\Gamma}} = T_{\Gamma'} \setminus \{S[v]_p\} = [(T_\Gamma \setminus \{S\}) \cup \{S[v]_p\}] \setminus \{S[v]_p\} = T_\Gamma \setminus \{S\}$

Assim vamos considerar dois casos $|T_\Gamma| = 1$, provando o caso base da indução (2) e $|T_\Gamma| > 1$, provando o caso geral supondo o passo indutivo (2).

Base da indução 2: $|T_\Gamma| = 1$:

Portanto $T_\Gamma \setminus \{S\} = \emptyset$, e como $T_{\overline{\Gamma}} \neq \emptyset$ pois $\overline{\Gamma}$ contém pelo menos um termo então $\mu(\overline{\Gamma}) < \mu(\Gamma)$.

Assim fica provado o caso base da indução (2).

Passo indutivo (2): $|T_\Gamma| > 1$:

Como obtemos pela aplicação da indução (1) que $T_{\overline{\Gamma}} = T_\Gamma \setminus \{S\}$ ou $\mu(\overline{\Gamma}) < \mu(\Gamma)$ então se $\mu(\overline{\Gamma}) < \mu(\Gamma)$ nada a provar. Suponha que $T_{\overline{\Gamma}} = T_\Gamma \setminus \{S\}$.

Observe que $\mu(\bar{\Gamma}) > 0$, pois $|T_\Gamma| > 1$ então existe um $\bar{S} \in T_\Gamma \setminus \{S\} = T_{\bar{\Gamma}}$, assim $\mu(\bar{\Gamma}) = \mu(\bar{S}) = \mu(\Gamma) > 0$. Então pela HI (2), temos que existem $\bar{\Gamma}'$ e $m' \geq 1$ tais que $\bar{\Gamma} \xRightarrow{m'}_{Purif} \bar{\Gamma}'$ e $\mu(\bar{\Gamma}') < \mu(\bar{\Gamma})$.

Portanto $\Gamma \xRightarrow{Purif} \Gamma' \xRightarrow{m}_{Purif} \bar{\Gamma} \xRightarrow{m'}_{Purif} \bar{\Gamma}'$ com $\mu(\bar{\Gamma}') < \mu(\bar{\Gamma}) = \mu(\Gamma)$. \square

Lema 3.9. *Seja Γ um problema de ACUNh-unificação então, existem Γ' um problema de ACUNh-unificação e $n \in \mathbb{N}$ tais que $\Gamma \xRightarrow{n}_{Purif} \Gamma'$ e $\mu(\Gamma') = 0$.*

Demonstração. Seja Γ um problema de ACUNh-unificação, se $\mu(\Gamma) = 0$ então defina $\Gamma' := \Gamma$ e $n = 0$, assim obtemos $\Gamma \xRightarrow{n}_{Purif} \Gamma'$ onde $\mu(\Gamma') = 0$.

Suponha que $\mu(\Gamma) > 0$ então vamos provar por indução sobre $\mu(\Gamma) = m$.

Hipótese de indução: Seja $\hat{\Gamma}$ um problema de ACUNh-unificação tal que

$\mu(\hat{\Gamma}) < \mu(\Gamma)$, então existem $\tilde{\Gamma}$ um problema de ACUNh-unificação e $n \in \mathbb{N}$ tais que $\hat{\Gamma} \xRightarrow{n}_{Purif} \tilde{\Gamma}$ e $\mu(\tilde{\Gamma}) = 0$

Base da Indução: Suponha $\mu(\Gamma) = 1$, então pelo Lema 3.8 existe $n \in \mathbb{N}$ e Γ' um problema de ACUNh-unificação tais que $\Gamma \xRightarrow{n}_{Purif} \Gamma'$ e $0 \leq \mu(\Gamma') < \mu(\Gamma) = 1$ e portanto $\mu(\Gamma') = 0$.

Passo indutivo: Agora suponha $\mu(\Gamma) = m > 0$ então pelo Lema 3.8 obtemos que existe Γ' e $k \in \mathbb{N}$ tais que $\Gamma \xRightarrow{k}_{Purif} \Gamma'$ e $\mu(\Gamma') < \mu(\Gamma)$ portanto pela hipótese de indução temos que existe $\tilde{\Gamma}$ e $n \in \mathbb{N}$ tais que $\Gamma' \xRightarrow{n}_{Purif} \tilde{\Gamma}$ onde $\mu(\tilde{\Gamma}) = 0$. E assim obtemos: $\Gamma \xRightarrow{k}_{Purif} \Gamma' \xRightarrow{n}_{Purif} \tilde{\Gamma}$ e $\mu(\tilde{\Gamma}) = 0$. \square

3.1.2 Confluência da purificação

Agora precisamos provar que, a menos de escolhas de variáveis novas na regra [Purif], temos que \xRightarrow{Purif} é confluente.

Seja um conjunto infinito enumerável de variáveis \mathcal{V} que é disjunta da assinatura Σ , por \mathcal{V} ser infinito enumerável então existe uma família $\{\mathcal{V}_i\}_{i \in \mathbb{N}}$ de subconjuntos de \mathcal{V} disjuntos dois a dois e infinitos tais que $\mathcal{V} = \dot{\bigcup}_{i \in \mathbb{N}} \mathcal{V}_i$.

Sem perda de generalidade podemos supor que para os problemas Γ de ACUNh-unificação que mencionamos nesta seção, tem-se que para cada $S \in \Gamma$, $S \in T(\Sigma, \mathcal{V}_0)$

Definição 3.6 (\mathcal{V}_i - problema de ACUNh-unificação). *Seja Γ um problema de ACUNh-unificação tal que para cada $S \in \Gamma$ tem-se que $S \in T(\Sigma, \mathcal{V})$. Defina que Γ é um \mathcal{V}_i -problema de ACUNh-unificação se, e somente se, existe um $i \in \mathbb{N}$ tal que $\text{Var}(\Gamma) \cap \mathcal{V}_i \neq \emptyset$ e para cada $j > i$ temos que $\text{Var}(\Gamma) \cap \mathcal{V}_j = \emptyset$.*

Definição 3.7 (Variável nova). *Seja Γ um \mathcal{V}_i -problema de ACUNh-unificação. Dizemos que $v \in \mathcal{V}$ é uma variável nova em Γ se, e somente se, $v \in \mathcal{V}_{i+i}$*

Vamos criar uma relação de equivalência $\approx_{\mathcal{V}}$ sobre o conjunto \mathcal{P} definido abaixo:

$$\mathcal{P} := \{\Gamma \mid \Gamma \text{ é um problema de ACUNh-unificação sobre } T(\Sigma, \mathcal{V})\}$$

Definição 3.8. *Seja $\approx_{\mathcal{V}}$ uma relação sobre \mathcal{P} definido da seguinte forma. Para cada $\Gamma, \Gamma' \in \mathcal{P}$ dizemos que $\Gamma \approx_{\mathcal{V}} \Gamma'$ se, e somente se, possui as propriedades abaixo:*

1. Γ, Γ' são \mathcal{V}_i -problemas de ACUNh-unificação para algum $i \in \mathbb{N}$.
2. Existe uma substituição $\alpha : \mathcal{V} \rightarrow \mathcal{V}$ tal que α é um renomeamento variáveis de S para cada $S \in \Gamma$, $\Gamma' = \Gamma\alpha$ e $\text{Dom}(\alpha) \cap \mathcal{V}_0 = \emptyset = \text{Im}(\alpha) \cap \mathcal{V}_0$.

Observação 3.2. *Quando quisermos explicitar o renomeamento α denotaremos por $\Gamma \approx_{\mathcal{V}, \alpha} \Gamma'$.*

Lema 3.10. *A relação $\approx_{\mathcal{V}}$ é uma relação de equivalência.*

Demonstração. Sejam Γ, Γ' e $\Gamma'' \in \mathcal{P}$.

(i) $\approx_{\mathcal{V}}$ é reflexiva:

Seja a substituição $id : \mathcal{V} \rightarrow \mathcal{V}$, a substituição identidade. Então $\text{Dom}(id) = \emptyset = \text{Im}(id)$. Observe que Γ é um \mathcal{V}_i -problema de ACUNh-unificação para algum $i \in \mathbb{N}$, $\Gamma = (\Gamma)id$ e $\text{Dom}(id) \cap \mathcal{V}_i = \emptyset$ e portanto obtemos $\Gamma \approx_{\mathcal{V}} \Gamma$

(ii) $\approx_{\mathcal{V}}$ é simétrica:

Suponha $\Gamma \approx_{\mathcal{V}} \Gamma'$, então existe um renomeamento α tal que $\Gamma' = \Gamma\alpha$ com $\text{Dom}(\alpha) \cap \mathcal{V}_0 = \text{Im}(\alpha) \cap \mathcal{V}_0 = \emptyset$. Seja α^{-1} o renomeamento inverso de α . Então $\text{Im}(\alpha^{-1}) = \text{Dom}(\alpha)$ e $\text{Dom}(\alpha^{-1}) = \text{Im}(\alpha)$, implicando que:

$$\text{Dom}(\alpha^{-1}) \cap \mathcal{V}_0 = \text{Im}(\alpha) \cap \mathcal{V}_0 = \emptyset \text{ e } \text{Im}(\alpha^{-1}) \cap \mathcal{V}_0 = \text{Dom}(\alpha) \cap \mathcal{V}_0 = \emptyset$$

e $\Gamma'\alpha^{-1} = \Gamma\alpha\alpha^{-1} = \{S\alpha\alpha^{-1} \mid S \in \Gamma\}$, como α é um renomeamento de variáveis de S para cada $S \in \Gamma$ temos que α^{-1} é um renomeamento de variáveis de $S\alpha$ e $S\alpha\alpha^{-1} = S$ para cada $S \in \Gamma$ e portanto $\Gamma'\alpha^{-1} = \Gamma$. Portanto $\Gamma' \approx_{\mathcal{V}} \Gamma$.

(iii) $\approx_{\mathcal{V}}$ é transitiva:

Suponha $\Gamma \approx_{\mathcal{V}} \Gamma'$ e $\Gamma' \approx_{\mathcal{V}} \Gamma''$, logo existem $i, j \in \mathbb{N}$ tais que Γ, Γ' são \mathcal{V}_i -problemas de ACUNh-unificação e Γ', Γ'' são \mathcal{V}_j -problemas de ACUNh-unificação portanto $i = j$ implicando que Γ, Γ'' são \mathcal{V}_i -problemas de ACUNh-unificação.

Desta forma existem $\alpha, \beta : \mathcal{V} \rightarrow \mathcal{V}$ tais que α é um renomeamento de variáveis de S para cada $S \in \Gamma$, β é um renomeamento de variáveis de S' para cada $S' \in \Gamma'$ com:

$$\Gamma' = \Gamma\alpha, \Gamma'' = \Gamma'\beta, \text{Dom}(\alpha) \cap \mathcal{V}_0 = \text{Im}(\alpha) \cap \mathcal{V}_0 = \emptyset \text{ e } \text{Dom}(\beta) \cap \mathcal{V}_0 = \text{Im}(\beta) \cap \mathcal{V}_0 = \emptyset$$

Portanto $\Gamma'' = \Gamma(\alpha\beta)$, basta provar que $\text{Dom}(\alpha\beta) \cap \mathcal{V}_0 = \text{Im}(\alpha\beta) \cap \mathcal{V}_0 = \emptyset$.

Note que $\text{Dom}(\alpha\beta) \subseteq \text{Dom}(\alpha) \cup \text{Dom}(\beta)$ e $\text{Im}(\alpha\beta) \subseteq \text{Im}(\alpha) \cup \text{Im}(\beta)$ então obtemos que

$$\text{Dom}(\alpha\beta) \cap \mathcal{V}_0 \subseteq \text{Dom}(\alpha) \cap \mathcal{V}_0 \cup \text{Dom}(\beta) \cap \mathcal{V}_0 = \emptyset \quad \text{Im}(\alpha\beta) \cap \mathcal{V}_0 \subseteq \text{Im}(\alpha) \cap \mathcal{V}_0 \cup \text{Im}(\beta) \cap \mathcal{V}_0 = \emptyset$$

Assim concluímos que $\Gamma \approx_{\mathcal{V}} \Gamma''$.

□

Vamos provar agora que para Γ, Γ' problemas de ACUNh-unificação tais que $\Gamma \Longrightarrow_{\text{Purif}} \Gamma'$ temos que $\Gamma \not\approx_{\mathcal{V}} \Gamma'$, considerando a definição de variável nova que fizemos. Isso será utilizado para provar que não é possível existir uma família $\{\Gamma_n\}_{n \in \mathbb{N}} \subseteq \mathcal{P}$ tal que $\Gamma_0 \Longrightarrow_{\text{Purif}} \Gamma_1 \Longrightarrow_{\text{Purif}} \dots \Longrightarrow_{\text{Purif}} \Gamma_n \Longrightarrow_{\text{Purif}} \dots$

Lema 3.11. *Seja Γ um \mathcal{V}_i -problema de ACUNh-unificação. Se $\Gamma \Longrightarrow_{\text{Purif}} \Gamma'$ então Γ' é um \mathcal{V}_{i+1} -problema de ACUNh-unificação, em particular, $\Gamma \not\approx_{\mathcal{V}} \Gamma'$*

Demonstração. Suponha $\Gamma = \bar{\Gamma} \dot{\cup} \{S\}$ onde é possível aplicar uma regra de purificação sobre S na posição $p \in \text{Pos}(S)$. Então temos v uma variável nova em Γ e

$$\frac{\bar{\Gamma} \cup \{S\}}{\bar{\Gamma} \cup \{S[v]_p, v \oplus S|_p\}} \text{Purif}$$

Faça $\Gamma' := \bar{\Gamma} \cup \{S[v]_p, v \oplus S|_p\}$ e então $\text{Var}(\Gamma') = \text{Var}(\Gamma) \dot{\cup} \{v\}$ e pela nossa definição de variável nova, temos que $v \in \mathcal{V}_{i+1}$. Por Γ ser um \mathcal{V}_i -problema de ACUNh-unificação, então para cada $j > i$ tem-se que $\text{Var}(\Gamma) \cap \mathcal{V}_j = \emptyset$. Então obtemos:

$$\text{Var}(\Gamma') \cap \mathcal{V}_{i+1} = (\text{Var}(\Gamma) \cap \mathcal{V}_{i+1}) \cup (\{v\} \cap \mathcal{V}_{i+1}) = \emptyset \cup \{v\} = \{v\} \neq \emptyset$$

e para cada $j > i + 1 > i$ temos: $(\mathcal{V}ar(\Gamma) \cap \mathcal{V}_j) \cup (\{v\} \cap \mathcal{V}_j) = \emptyset \cup \emptyset = \emptyset$.

E portanto Γ' é um \mathcal{V}_{i+1} - problema de ACUNh-unificação, logo pela definição da relação de equivalência $\approx_{\mathcal{V}}$ temos $\Gamma \not\approx_{\mathcal{V}} \Gamma'$. \square

Vamos agora definir uma relação $\Longrightarrow_{\mathcal{V}}$ sobre $\mathcal{P}/\approx_{\mathcal{V}}$ tal que sua terminação implica na terminação de \Longrightarrow_{Purif} .

Definição 3.9. Seja $\Gamma \in \mathcal{P}$ e defina o conjunto $[\Gamma]_{\approx_{\mathcal{V}}} := \{\Gamma' \in \mathcal{P} \mid \Gamma \approx_{\mathcal{V}} \Gamma'\}$, a classe de equivalência de Γ na relação $\approx_{\mathcal{V}}$ e defina o conjunto $\mathcal{P}/\approx_{\mathcal{V}} := \{[\Gamma]_{\approx_{\mathcal{V}}} \mid \Gamma \in \mathcal{P}\}$ o quociente de \mathcal{P} pela relação $\approx_{\mathcal{V}}$.

Definimos a relação $\Longrightarrow_{\mathcal{V}}$ sobre $\mathcal{P}/\approx_{\mathcal{V}}$ da seguinte forma, $[\Gamma]_{\approx_{\mathcal{V}}} \Longrightarrow_{\mathcal{V}} [\Gamma']_{\approx_{\mathcal{V}}}$ se, e somente se, existem $\bar{\Gamma} \in [\Gamma]_{\approx_{\mathcal{V}}}$ e $\hat{\Gamma} \in [\Gamma']_{\approx_{\mathcal{V}}}$ tais que $\bar{\Gamma} \Longrightarrow_{Purif} \hat{\Gamma}$.

Observação 3.3. A partir de agora faremos um abuso de notação sobre a relação \Longrightarrow_{Purif} , denotaremos apenas por \Longrightarrow .

Lema 3.12. Sejam $\Gamma_1, \Gamma_2 \in \mathcal{P}$ tais que $\Gamma_1 \approx_{\mathcal{V}, \alpha} \Gamma_2$. Se $\Gamma_1 \Longrightarrow_{Purif} \Gamma'$ então $\Gamma_2 \Longrightarrow_{Purif} \Gamma'\alpha$, em particular $\Gamma' \approx_{\mathcal{V}} \Gamma'\alpha$.

Demonstração. Como por hipótese temos $\Gamma_1 \approx_{\mathcal{V}} \Gamma_2$ com o renomeamento de variáveis α , então Γ_1, Γ_2 são \mathcal{V}_i - problemas de ACUNh-unificação tais que $\Gamma_2 = \Gamma_1\alpha$ cumprindo com as propriedades mencionadas na Definição 3.8. Podemos supor sem perda de generalidade que $Dom(\alpha) \cap \mathcal{V}_{i+1} = \emptyset$.

Suponha que seja possível aplicar a regra [Purif] em Γ_1 sobre S na posição $p \in \mathcal{P}os(S)$, isto é, $\Gamma_1 = \bar{\Gamma} \cup \{S\}$ e então:

$$\frac{\bar{\Gamma} \cup \{S\}}{\bar{\Gamma} \cup \{S[v]_p, v \oplus S|_p\}} \text{Purif}$$

Com $v \in \mathcal{V}_{i+1}$ e $p \in S_{\oplus} \cup S_h$, isto é, $p = qk$ onde $q \in \mathcal{P}os(S)$ e $k \in \mathbb{N}$ e $S|_p$ é uma soma pura ou um h -termo puro com $raíz(S|_q) \neq \oplus$.

Faça $\Gamma' := \bar{\Gamma} \cup \{S[v]_p, v \oplus S|_p\}$, portanto $\Gamma'\alpha = \bar{\Gamma}\alpha \cup \{(S[v]_p)\alpha, (v \oplus S|_p)\alpha\}$, e como $(S[v]_p)\alpha = (S\alpha)[v\alpha]_p = (S\alpha)[v]_p$ e $(S|_p)\alpha = (S\alpha)|_p$ obtemos que: $\Gamma'\alpha = \bar{\Gamma}\alpha \cup \{(S\alpha)[v]_p, v \oplus (S\alpha)|_p\}$.

Observe que se $S|_p$ é um h -termo puro ou soma pura então $(S|_p)\alpha$ é um h -termo puro ou soma pura pois α é um renomeamento de variáveis e portanto não altera os símbolos de função de um termo, e portanto $(S\alpha)|_p$ é um h -termo puro ou soma pura.

Por outro lado $raíz((S\alpha)|_q) = raíz(S|_q) \neq \oplus$ e portanto temos que $p \in (S\alpha)_{\oplus} \cup (S\alpha)_h$, podendo assim aplicar a regra de inferência purificação em $\Gamma_2 = \Gamma_1\alpha = \bar{\Gamma}\alpha \cup \{S\alpha\}$ sobre $S\alpha$ na posição $p \in Pos(S\alpha)$. Como Γ_2 é um \mathcal{V}_i -problema de ACUNh-unificação, podemos escolher qualquer variável nova em Γ_2 para aplicar a regra, em particular, vamos tomar o mesmo v utilizado em Γ_1 . Logo,

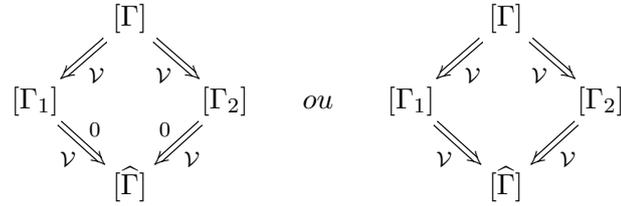
$$\frac{\bar{\Gamma}\alpha \cup \{S\alpha\}}{\bar{\Gamma}\alpha \cup \{(S\alpha)[v]_p, v \oplus (S\alpha)|_p\}} \text{ Purif}$$

E portanto concluímos que $\Gamma_2 \implies_{Purif} \Gamma'\alpha$ se $\Gamma \implies_{Purif} \Gamma'$.

Como $v \notin Dom(\alpha)$ e α é um renomeamento de variáveis de Γ_1 então para cada $T \in \Gamma_1$ temos que α é um renomeamento de variáveis de T , em particular α também é um renomeamento de variáveis para $S[v]_p$ e $v \oplus S|_p$ e portanto α é um renomeamento de variáveis para Γ' . Assim por α cumprir as hipóteses da Definição 3.8, $\Gamma', \Gamma'\alpha$ serem \mathcal{V}_{i+1} -problemas de ACUNh-unificação e $\Gamma'\alpha = (\Gamma')\alpha$ temos que $\Gamma' \approx_{\mathcal{V}} \Gamma'\alpha$. \square

Observação 3.4. Iremos omitir na representação da classe $[\Gamma]_{\approx_{\mathcal{V}}}$, a referência da relação $\approx_{\mathcal{V}}$, pois estaremos sempre no contexto das classes de equivalência de $\mathcal{P}/\approx_{\mathcal{V}}$

Lema 3.13. $\implies_{\mathcal{V}}$ sobre $\mathcal{P}/\approx_{\mathcal{V}}$ possui a propriedade diamante, isto é, para $[\Gamma], [\Gamma_1]$ e $[\Gamma_2] \in \mathcal{P}/\approx_{\mathcal{V}}$, se $[\Gamma_1] \longleftarrow [\Gamma] \implies [\Gamma_2]$ então existe $[\hat{\Gamma}] \in \mathcal{P}/\approx_{\mathcal{V}}$ tal que:



Consequentemente, $\implies_{\mathcal{V}}$ sobre $\mathcal{P}/\approx_{\mathcal{V}}$ é confluenta.

Demonstração. Sejam as classes $[\Gamma_1], [\Gamma]$ e $[\Gamma_2] \in \mathcal{P}/\approx_{\mathcal{V}}$ tais que

$$[\Gamma_1] \xleftarrow{\mathcal{V}} [\Gamma] \xrightarrow{\mathcal{V}} [\Gamma_2] \quad (3.3)$$

Portanto pela definição de \implies sobre $\mathcal{P}/\approx_{\mathcal{V}}$, existem $\Gamma', \Gamma'' \in [\Gamma]$, $\Gamma'_1 \in [\Gamma_1]$ e $\Gamma'_2 \in [\Gamma_2]$ tais que $\Gamma'_1 \xleftarrow{\mathcal{V}} \Gamma' \approx_{\mathcal{V}} \Gamma'' \xrightarrow{\mathcal{V}} \Gamma'_2$.

Como $\Gamma' \approx_{\mathcal{V}, \alpha} \Gamma''$ temos pelo Lema 3.12 que $\Gamma'_2 \alpha \approx_{\mathcal{V}} \Gamma'_2$ e $\Gamma' \implies \Gamma'_2 \alpha$, e portanto existem $\Gamma'_1 \in [\Gamma_1], \Gamma''_2 \in [\Gamma_2]$ e $\Gamma' \in [\Gamma]$ tais que $\Gamma'_1 \longleftarrow \Gamma' \Longrightarrow \Gamma''_2$.

Suponha que Γ' seja um \mathcal{V}_i - problema de ACUNh-unificação então Γ'_1, Γ''_2 são \mathcal{V}_{i+1} -problemas de ACUNh-unificação. Por outro lado existem $S_1, S_2 \in \Gamma'$ e $p \in \mathcal{P}os(S_1), q \in \mathcal{P}os(S_2)$ onde é possível aplicar a regra de purificação sobre S_1, S_2 nas posições p, q , onde $v, w \in \mathcal{V}_{i+1}$, isto é, variáveis novas em Γ' , então obtemos:

$$[i] \frac{\Gamma' = \bar{\Gamma}_1 \cup \{S_1\}}{\Gamma'_1 = \bar{\Gamma}_1 \cup \{S_1[v]_p, v \oplus S_1|_p\}} \text{ [Purif]} \quad [ii] \frac{\Gamma' = \bar{\Gamma}_2 \cup \{S_2\}}{\Gamma''_2 = \bar{\Gamma}_2 \cup \{S_2[w]_q, w \oplus S_2|_q\}} \text{ [Purif]}$$

Existem três possíveis casos:

1. $S_1 = S_2$ e $p = q$:

Então $\bar{\Gamma}_1 = \bar{\Gamma}_2$, tome o renomeamento de variáveis $\alpha = \{v \mapsto w\}$, aplicando sobre Γ'_1 obtemos:

$$\begin{aligned} \Gamma'_1 \alpha &= \bar{\Gamma}_1 \alpha \cup \{(S_1[v]_{p_1})\alpha, (v \oplus S_1|_{p_1})\alpha\} = \bar{\Gamma}_1 \alpha \cup \{(S_1 \alpha)[v\alpha]_p, v\alpha \oplus (S_1|_p)\alpha\} \\ &= \bar{\Gamma}_1 \cup \{S_1[w]_p, w \oplus S_1|_p\} = \bar{\Gamma}_2 \cup \{S_2[w]_q, w \oplus S_2|_q\} = \Gamma''_2 \end{aligned}$$

Logo $\Gamma''_2 = \Gamma'_1 \alpha$, onde $\mathcal{D}om(\alpha) \cap \mathcal{V}_0 = \mathcal{I}m(\alpha) \cap \mathcal{V}_0 = \emptyset$, α é um renomeamento de variáveis de cada $S' \in \Gamma'_1$ e Γ''_2, Γ'_1 são \mathcal{V}_{i+1} -problemas de ACUNh-unificação. Pela Definição 3.8 obtemos $\Gamma''_2 \approx_{\mathcal{V}} \Gamma'_1$, e então $[\hat{\Gamma}] = [\hat{\Gamma}_1] = [\hat{\Gamma}_2]$. Portanto, obtemos:

$$\begin{array}{ccc} [\Gamma_1] & & [\Gamma_2] \\ & \searrow^0 & \swarrow^0 \\ & \nu & \nu \\ & & [\hat{\Gamma}] \end{array}$$

2. $S := S_1 = S_2$ e $p \neq q$:

Então $\bar{\Gamma} := \bar{\Gamma}_1 = \bar{\Gamma}_2$ e por ser possível aplicar a purificação em S nas posições p, q temos que $p, q \in S_{\oplus} \dot{\cup} S_h$, porém por hipótese, $p \neq q$ e pela Proposição 3.1 item 2. obtemos que $p \parallel q$ implicando que $p \in \mathcal{P}os(S[w]_q), q \in \mathcal{P}os(S[v]_p)$ onde $(S[w]_q)|_p = S|_p, (S[v]_p)|_q = S|_q$.

Porém p, q são posições tais que $S|_p, S|_q$ são somas puras ou h -termos puros para os quais existem $p', q' \in \mathcal{P}os(S)$ e $i, j \in \mathbb{N}$ tais que $p = p'i, q = q'j$ e $raíz(S|_{q'}) \neq \oplus, raíz(S|_{p'}) \neq \oplus$, portanto obtemos:

$$p \in (S[w]_q)_{\oplus} \dot{\cup} (S[w]_q)_h \text{ e } q \in (S[v]_p)_{\oplus} \dot{\cup} (S[v]_p)_h$$

Assim de acordo com a inferência [i], podemos aplicar a regra purificação em Γ'_1 sobre $S_1[v]_p = S[v]_p$ na posição q , onde $v' \in \mathcal{V}_{i+2}$ obtendo:

$$[\text{iii}] \frac{\Gamma'_1 = \bar{\Gamma} \cup \{S[v]_p, v \oplus S|_p\}}{\hat{\Gamma}_1 = \bar{\Gamma} \cup \{(S[v]_p)[v']_q, v' \oplus (S[v]_p)|_q, v \oplus S|_p\}} \text{ Purif}$$

Isto é, $\Gamma'_1 \implies \hat{\Gamma}_1$. Logo pela Definição 3.9 obtemos que na relação no conjunto das classes de equivalência $\mathcal{P}_{\approx_{\mathcal{V}}}$ temos $[\Gamma_1] \implies [\hat{\Gamma}_1]$.

E da mesma forma observando a inferência [ii], podemos aplicar a regra de purificação em Γ''_2 sobre $S_2[w]_q = S[w]_q$ na posição p , onde $w' \in \mathcal{V}_{i+2}$ obtendo:

$$[\text{iv}] \frac{\Gamma''_2 = \bar{\Gamma} \cup \{S[w]_q, v \oplus S|_q\}}{\hat{\Gamma}_2 = \bar{\Gamma} \cup \{(S[w]_q)[w']_p, w' \oplus (S[w]_q)|_p, w \oplus S|_q\}} \text{ Purif}$$

Equivalentemente $\Gamma''_2 \implies \hat{\Gamma}_2$ logo pela Definição 3.9 obtemos que na relação no conjunto das classes de equivalência $\mathcal{P}_{\approx_{\mathcal{V}}}$ temos $[\Gamma_2] \implies [\hat{\Gamma}_2]$.

Como $p||q$, $(S[v]_p)[v']_q = (S[v']_q)[v]_p$, $(S[v]_p)|_q = S|_q$ e $(S[w]_q)|_p = S|_p$. Portanto, obtemos os seguintes conjuntos:

$$\hat{\Gamma}_1 = \bar{\Gamma} \cup \{(S[v']_q)[v]_p, v' \oplus S|_q, v \oplus S|_p\} \quad \hat{\Gamma}_2 = \bar{\Gamma} \cup \{(S[w]_q)[w']_p, w' \oplus S|_q, w' \oplus S|_p\} \quad (3.4)$$

Tome o renomeamento de variáveis $\gamma = \{v' \mapsto w, v \mapsto w'\}$, note que γ é um renomeamento do termo $(S[v']_q)[v]_p$ pois $v' \neq v$ e $w' \neq w$. Então γ é um renomeamento de variáveis de $\hat{\Gamma}_1$, e diretamente da Eq. 3.4 temos a seguinte igualdade $\hat{\Gamma}_2 = \hat{\Gamma}_1\gamma$.

Como $\hat{\Gamma}_1, \hat{\Gamma}_2$ são \mathcal{V}_{i+2} -problemas de ACUNh-unificação, segue pela Definição 3.8 que $\hat{\Gamma}_1 \approx_{\mathcal{V}} \hat{\Gamma}_2$, isto é, $[\hat{\Gamma}] := [\hat{\Gamma}_1] = [\hat{\Gamma}_2]$ e, $[\Gamma_1] \xrightarrow{\mathcal{V}} [\hat{\Gamma}] \xleftarrow{\mathcal{V}} [\Gamma_2]$.

3. $S_1 \neq S_2$:

Então temos que $\Gamma' = \tilde{\Gamma} \cup \{S_1, S_2\}$ e portanto para $v, w \in \mathcal{V}_{i+1}$, variáveis novas em Γ' , obtemos das inferências [i] e [ii]:

$$\Gamma'_1 = \tilde{\Gamma} \cup \{S_1[v]_p, v \oplus S_1|_p, S_2\} \quad \Gamma''_2 = \tilde{\Gamma} \cup \{S_1, S_2[w]_q, v \oplus S_2|_q\}$$

Portanto podemos aplicar a regra de inferência purificação em Γ'_1 sobre S_2 na posição q , onde $v' \in \mathcal{V}_{i+2}$ obtendo:

$$[\text{v}] \frac{\Gamma'_1 = \tilde{\Gamma} \cup \{S_1[v]_p, v \oplus S_1|_p, S_2\}}{\hat{\Gamma}_1 = \tilde{\Gamma} \cup \{S_1[v]_p, v \oplus S_1|_p, S_2[v']_q, v' \oplus S_2|_q\}}$$

Isto é, $\Gamma'_1 \implies \hat{\Gamma}_1$ e então $[\Gamma_1] \implies [\hat{\Gamma}_1]$.

E da mesma forma, podemos aplicar a regra de purificação em Γ''_2 sobre S_1 na posição p , onde $w' \in \mathcal{V}_{i+2}$ obtendo:

$$[\text{vi}] \frac{\Gamma''_2 = \tilde{\Gamma} \cup \{S_1, S_2[w]_q, v \oplus S_2|_q\}}{\hat{\Gamma}_2 = \tilde{\Gamma} \cup \{S_1[w']_p, w' \oplus S_1|_p, S_2[w]_q, w \oplus S_2|_q\}}$$

Tomando $\gamma = \{v \mapsto w', v' \mapsto w\}$ obtemos pelas inferências de [v] e [vi] que $\hat{\Gamma}_2 = \hat{\Gamma}_1\gamma$, e por γ ser um renomeamento de variáveis de $\hat{\Gamma}_1$ então obtemos que $\hat{\Gamma}_1 \approx_{\mathcal{V}} \hat{\Gamma}_2$ pois $\hat{\Gamma}_1, \hat{\Gamma}_2$ são \mathcal{V}_{i+2} -problemas de ACUNh-unificação. Concluindo então que $[\hat{\Gamma}] := [\hat{\Gamma}_1] = [\hat{\Gamma}_2]$ e portanto: $[\Gamma_1] \xrightarrow{\mathcal{V}} [\hat{\Gamma}] \xleftarrow{\mathcal{V}} [\Gamma_2]$.

Logo, em todos os casos, segue o resultado. \square

Vamos provar agora que para cada classe de equivalência $[\Gamma] \in \mathcal{P}/\approx_{\mathcal{V}}$, $[\Gamma]$ possui uma forma normal com relação a $\implies_{\mathcal{V}}$, concluindo que $\implies_{\mathcal{V}}$ sobre $\mathcal{P}/\approx_{\mathcal{V}}$ é uma relação terminante, pois é confluyente.

Lema 3.14. *Para cada $[\Gamma] \in \mathcal{P}/\approx_{\mathcal{V}}$, $[\Gamma]$ possui uma forma normal com relação a \implies sobre $\mathcal{P}/\approx_{\mathcal{V}}$.*

Demonstração. Tome $[\Gamma] \in \mathcal{P}/\approx_{\mathcal{V}}$, e seja Γ_0 um representante para a classe $[\Gamma]$. Então Γ_0 é um problema de ACUNh-unificação, e pelo Lema 3.9, existem $n \in \mathbb{N}$ e Γ_n um problema de ACUNh-unificação tais que $\Gamma_0 \implies_{Purif}^n \Gamma_n$ e $\mu(\Gamma_n) = 0$.

- $n = 0$:

Então Γ_0 está em sua forma normal pois $\mu(\Gamma_0) = 0$, suponha por absurdo que exista $[\Gamma'] \in \mathcal{P}/\approx_{\mathcal{V}}$ tal que $[\Gamma] \implies_{\mathcal{V}} [\Gamma']$. Então existem $\Gamma_1 \in [\Gamma], \Gamma'_1 \in [\Gamma']$ tais que $\Gamma_1 \implies_{Purif} \Gamma'_1$, como $\Gamma_0, \Gamma_1 \in [\Gamma]$ então $\Gamma_0 \approx_{\mathcal{V}} \Gamma_1$ por um renomeamento α , logo pelo Lema 3.12 temos que $\Gamma_0 \implies \Gamma'_1\alpha$, que é uma contradição, pois Γ_0 está em sua forma normal. Portanto $[\Gamma]$ está em sua forma normal com relação a $\implies_{\mathcal{V}}$ sobre $\mathcal{P}/\approx_{\mathcal{V}}$

- $n > 0$:

Logo existem $\Gamma_1, \Gamma_2, \dots, \Gamma_{n-1} \in \mathcal{P}$ tais que $\Gamma_0 \implies \Gamma_1 \implies \Gamma_2 \implies \dots \implies \Gamma_{n-1} \implies \Gamma_n$. e portanto obtemos a sequência $[\Gamma] \implies_{\mathcal{V}} [\Gamma_1] \implies_{\mathcal{V}} [\Gamma_2] \implies_{\mathcal{V}} \dots \implies_{\mathcal{V}} [\Gamma_{n-1}] \implies_{\mathcal{V}} [\Gamma_n]$.

Com $\mu(\Gamma_n) = 0$, recaindo no caso anterior e portanto $[\Gamma_n]$ está em sua forma normal com relação a $\Longrightarrow_{\mathcal{V}}$ sobre $\mathcal{P}/\approx_{\mathcal{V}}$.

Dessa forma concluímos que $[\Gamma]$ possui um forma normal com relação a \Longrightarrow sobre $\mathcal{P}/\approx_{\mathcal{V}}$. \square

Lema 3.15. *A relação $\Longrightarrow_{\mathcal{V}}$ sobre $\mathcal{P}/\approx_{\mathcal{V}}$ é terminante.*

Demonstração. Pelos Lema 3.13 3.14 a relação \Longrightarrow sobre $\mathcal{P}/\approx_{\mathcal{V}}$ é confluyente e toda classe de equivalência $[\Gamma] \in \mathcal{P}/\approx_{\mathcal{V}}$ possui uma forma normal. Portanto cada classe de equivalência $[\Gamma] \in \mathcal{P}/\approx_{\mathcal{V}}$ possui uma única forma normal e $\Longrightarrow_{\mathcal{V}}$ tem a propriedade diamante, equivalentemente, $\Longrightarrow_{\mathcal{V}}$ sobre $\mathcal{P}/\approx_{\mathcal{V}}$ é terminante. \square

3.1.3 Algoritmo Purif

$$Purif(\Gamma) := \begin{cases} \Gamma & \text{se } \mu(\Gamma) = 0 \\ Purif(\Gamma') & \text{se } \mu(\Gamma) > 0 \text{ e } \Gamma \Longrightarrow_{Purif} \Gamma' \end{cases} \quad (3.5)$$

Teorema 3.1. *Purif é terminante, isto é, Purif é um algoritmo.*

Demonstração. Suponha por absurdo que exista Γ_0 um problema de ACUNh-unificação tal que $Purif(\Gamma_0)$ não termina, isto é, existe uma sequência infinita $\{\Gamma_i\}_{i \in \mathbb{N}}$ de problemas de ACUNh-unificação tais que $\Gamma_i \Longrightarrow_{Purif} \Gamma_{i+1}$ para cada $i \in \mathbb{N}$. Pelo Lema 3.11 e pela definição de $\Longrightarrow_{\mathcal{V}}$ temos que $[\Gamma_i]_{\approx_{\mathcal{V}}} \Longrightarrow_{\mathcal{V}} [\Gamma_{i+1}]_{\approx_{\mathcal{V}}}$ para cada $i \in \mathbb{N}$, que é uma contradição, pois $\Longrightarrow_{\mathcal{V}}$ é terminante. Portanto $Purif(\Gamma)$ termina para qualquer Γ problema de ACUNh-unificação. \square

Teorema 3.2. *O algoritmo Purif é correto, isto é, se $\tilde{\Gamma} = Purif(\Gamma)$ então $\tilde{\Gamma}$ está em sua forma pura e $\tilde{\Gamma}$ é uma extensão conservativa de Γ .*

Demonstração. Seja $\tilde{\Gamma} = Purif(\Gamma)$, e portanto pela definição de $Purif$, temos que $\mu(\tilde{\Gamma}) = 0$ e pelo Lema 3.7, $\tilde{\Gamma}$ está em sua forma pura. Por outro lado, temos que existem $n \in \mathbb{N}$ e $\Gamma_1, \dots, \Gamma_{n-1}$ problemas de ACUNh-unificação tais que $\Gamma = \Gamma_0 \Longrightarrow_{Purif} \Gamma_1 \Longrightarrow_{Purif} \dots \Longrightarrow_{Purif} \Gamma_{n-1} \Longrightarrow_{Purif} \Gamma_n = \tilde{\Gamma}$. E pelo Lema 3.1 temos que Γ_i é uma extensão conservativa de Γ_{i-1} tal que $\mathcal{Var}(\Gamma_{i-1}) \subset \mathcal{Var}(\Gamma_i)$ para cada $i \in \{1, \dots, n\}$ e portanto pela Proposição 1.5 da transitividade de extensões conservativas, temos que Γ_n é uma extensão conservativa de Γ_0 , isto é, $\tilde{\Gamma}$ é uma extensão conservativa de Γ . \square

Exemplo 3.2. Seja Γ o problema de ACUNh-unificação, descrito no Exemplo 2.1 na página 36, após padroniza-lo e purificá-lo no Exemplo 3.1, obtemos:

$$\Gamma_0 := \left\{ \begin{array}{ll} (1) & x \oplus h(x) \oplus f(v_1) \oplus f(v_2) \\ (2) & h(z) \oplus w \oplus y \oplus b \oplus a \\ (3) & 0 \end{array} \quad \begin{array}{l} (4) \quad v_1 \oplus a \oplus x \oplus h(x) \oplus y \oplus w \\ (5) \quad v_2 \oplus b \oplus z \oplus h(x) \end{array} \right\}$$

Pelo Teorema 3.2, Γ_0 está em sua forma pura e é uma extensão conservativa de Γ .

3.2 \mathcal{J}_{XORh} : um algoritmo para ACUNh-unificação

Nesta seção apresentaremos o algoritmo \mathcal{J}_{XORh} para solubilidade para problemas de ACUNh-unificação, que foi proposto por Liu em [18]. Este algoritmo age em triplas da forma $\Gamma \parallel \Delta \parallel \Lambda$, que chamaremos por estados, obtidos a partir de do problema de ACUNh-unificação (em sua forma pura) que queremos resolver. Δ consiste de um conjunto de inequação da forma $s \neq t$, com $s, t \in T(\Sigma, \mathcal{V})$ e Λ consiste de um conjunto de equações da forma $x = S$, onde S é um termo e x uma variável *solta* de Γ , descrita na Definição 3.4.

Dado um problema Γ de ACUNh-unificação em sua forma pura, dizemos que um estado de \mathcal{J}_{XORh} é *inicial*, desde que, tem a forma $\Gamma \parallel \emptyset \parallel \emptyset$. Um estado $\Gamma' \parallel \Delta' \parallel \Lambda'$ é dito um estado *válido* de \mathcal{J}_{XORh} se, e somente se, é um estado inicial de \mathcal{J}_{XORh} ou é obtido de um estado inicial de \mathcal{J}_{XORh} por uma aplicação finita e sucessiva de suas regras de inferência.

Definição 3.10 (Estado final). *Seja um estado $\Gamma \parallel \Delta \parallel \Lambda$ um estado de \mathcal{J}_{XORh} , dizemos que é um estado final se não for possível aplicar mais nenhuma de suas regras de inferência. Se $\Gamma \parallel \Delta \parallel \Lambda$ é um estado final e $\Gamma \neq \emptyset$ dizemos que o $\Gamma \parallel \Delta \parallel \Lambda$ é um estado de falha e quando $\Gamma = \emptyset$ dizemos que $\Gamma \parallel \Delta \parallel \Lambda$ é um estado de solução.*

Regras de inferência de \mathcal{J}_{XORh}

As regras descritas aqui são executadas com a prioridade que são listadas abaixo, assim Trivial tem a maior prioridade e nulificação a menor prioridade. Vamos descrever as regras abaixo como regras de inferência, explicitando as condições necessárias sobre o estado $\Gamma \parallel \Delta \parallel \Lambda$ para poderem ser aplicadas, assim como o novo estado obtido.

Trivial: Esta regra de inferência tem como objetivo eliminar equações trivias de Γ , isto é, remover os '0' que se encontram em Γ .

Trivial

$$\frac{\widehat{\Gamma} \cup \{0\} \parallel \Delta \parallel \Lambda}{\widehat{\Gamma} \parallel \Delta \parallel \Lambda} \text{Triv}$$

Exemplo 3.3. Seja Γ_0 obtido no Exemplo 3.2, isto é:

$$\Gamma_0 := \left\{ \begin{array}{ll} (1) & x \oplus h(x) \oplus f(v_1) \oplus f(v_2) \\ (2) & h(z) \oplus w \oplus y \oplus b \oplus a \\ (3) & 0 \end{array} \quad \begin{array}{l} (4) & v_1 \oplus a \oplus x \oplus h(x) \oplus y \oplus w \\ (5) & v_2 \oplus b \oplus z \oplus h(x) \end{array} \right\}$$

Então Γ_0 está em sua forma pura, portanto $\Gamma_0 \parallel \emptyset \parallel \emptyset$ é um estado válido de \mathcal{J}_{XORh} e portanto podemos aplicar as regras de \mathcal{J}_{XORh} .

Observe que pela prioridade das regras, devemos verificar se é possível aplicar a regra trivial, note que o termo (3) em Γ_0 é o termo nulo, então ao aplicarmos a regra trivial em $\Gamma_0 \parallel \emptyset \parallel \emptyset$ obtemos o estado $\Gamma_1 \parallel \emptyset \parallel \emptyset$ onde Γ_1 é dado por:

$$\Gamma_1 := \left\{ \begin{array}{ll} (1) & x \oplus h(x) \oplus f(v_1) \oplus f(v_2) \\ (2) & h(z) \oplus w \oplus y \oplus b \oplus a \end{array} \quad \begin{array}{l} (4) & v_1 \oplus a \oplus x \oplus h(x) \oplus y \oplus w \\ (5) & v_2 \oplus b \oplus z \oplus h(x) \end{array} \right\}$$

E $\Gamma_1 \parallel \emptyset \parallel \emptyset$ é um estado válido de \mathcal{J}_{XORh} .

Simplificação: Quando temos um termo $x \oplus S \in \Gamma$, e x é uma variável solta de Γ , isto é, ela não ocorre sob nenhum subtermo t de Γ onde $raiz(t) \neq \oplus$ então iremos remover o termo $x \oplus S$ de Γ e inserir $x = S$ no conjunto Λ após substituir cada ocorrência de x em Λ por S .

Simplificação

$$\frac{\widehat{\Gamma} \cup \{x \oplus S\} \parallel \Delta \parallel \Lambda}{Purif(\widehat{\Gamma} \downarrow) \parallel \Delta \downarrow \parallel \Lambda \downarrow \cup \{x = S\}} \text{Simp}$$

Condições:

- x é uma variável solta de $\Gamma = \widehat{\Gamma} \cup \{x \oplus S\}$ e temos que ocorre apenas uma das seguintes opções.
 - O símbolo de função h não ocorre em S ou
 - Para todo $x \oplus T \in \Gamma$, o símbolo de função h ocorre em T .
- $\gamma = \{x \mapsto S\}$.
- Se S é um termo vazio, então vamos considerar S como 0.

Exemplo 3.4. Continuando o Exemplo 3.3 por não ser mais possível aplicar a regra [Triv] então pela prioridade que definimos, devemos verificar se é possível aplicar a regra [Simp]. Note que no termo (2), $h(z) \oplus w \oplus y \oplus b \oplus a$.

A variável y é uma variável solta de Γ_1 , qualquer outra equação da forma $y \oplus T \in \Gamma_1$, T tem uma ocorrência de h , então podemos aplicar a regra [Simp]. Seja $\gamma = \{y \mapsto h(z) \oplus w \oplus b \oplus a\}$, removendo a equação (2) de Γ_1 , aplicando a substituição γ e normalizando obtemos

$$\Gamma_2 := \left\{ \begin{array}{ll} (1) & x \oplus h(x) \oplus f(v_1) \oplus f(v_2) & (5) & v_2 \oplus b \oplus z \oplus h(x) \\ (4) & v_1 \oplus b \oplus x \oplus h(v_3) & (7) & v_3 \oplus x \oplus z \end{array} \right\}$$

Note que podemos aplicar novamente a regra simplificação no estado $\Gamma_2 \parallel \emptyset \parallel \Lambda_2$ pois z na equação (7) é uma variável solta em Γ_2 , assim obtemos o estado $\Gamma_3 \parallel \emptyset \parallel \Lambda_3$, onde: $\gamma' = \{z \mapsto x \oplus v_3\}$

$$\Lambda_3 = \Lambda_2 \gamma' \cup \{z = x \oplus v_3\} = \{y = h(x \oplus v_3) \oplus w \oplus b \oplus a, z = x \oplus v_3\}$$

$$\Gamma_3 := \text{Purif}(\widehat{\Gamma}_2 \downarrow) = \left\{ \begin{array}{l} (1) \quad x \oplus h(x) \oplus f(v_1) \oplus f(v_2) \\ (4) \quad v_1 \oplus b \oplus x \oplus h(v_3) \\ (5) \quad v_2 \oplus b \oplus x \oplus v_3 \oplus h(x) \end{array} \right\}$$

Note que as variáveis que ocorrem em Γ_3 estão todas presas e portanto não é mais possível aplicar a regra simplificação.

N-decomposição: Quando temos $f \in \Sigma^n$ um símbolo de função não interpretado com $n \geq 1$ e o termo $f(t_1, \dots, t_n) \oplus f(s_1, \dots, s_n) \oplus S \in \Gamma$, podemos aplicar a regra *N-decomposição* gerando dois ramos, o primeiro caso os termos acima são unificáveis sintaticamente, mas pode ser que resulte em falha, então a regra N-decomposição gera outro ramo onde $f(t_1, \dots, t_n) \neq f(s_1, \dots, s_n)$ é adicionado no conjunto Δ impedindo que refaça essa escolha de unificação.

N-decomposição

$$\frac{\widehat{\Gamma} \cup \{s \oplus t \oplus T\} \parallel \Delta \parallel \Lambda}{\widehat{\Gamma} \downarrow \cup \{T\gamma \downarrow\} \parallel \Delta \gamma \downarrow \parallel \Lambda \gamma \downarrow \cup [\gamma] \vee \Gamma \parallel \Delta \cup \{s \neq t\} \parallel \Lambda} \text{ [N-dec]}$$

Condições:

- Os termos s, t são termos puros e não variáveis tais que $\text{raíz}(s) = \text{raíz}(t) \neq h$.
- $s \neq t \notin \Delta$
- γ é um mgu de s, t , via unificação sintática, onde γ é idempotente, $\text{Dom}(\gamma) \subseteq \text{Var}(s) \cup \text{Var}(t)$ e $\text{Var}(\text{Im}(\gamma)) \subseteq \text{Var}(\Gamma)$.
- $[\gamma] := \{x = S \mid x \mapsto S \in \gamma\}$

Exemplo 3.5. Continuando o Exemplo 3.4, note que a próxima regra imposta pela prioridade é a regra [N-dec]. Observe que na equação (1) de Γ_3 temos a soma $f(v_1) \oplus f(v_2)$ então podemos aplicar a regra N-decomposição, onde $\gamma = \{v_1 \mapsto v_2\}$ é um unificador sintático como na regra [N-dec]. Obtendo assim dois novos estados, $\Gamma_4 \parallel \emptyset \parallel \Lambda_4$ e $\Gamma'_4 \parallel \Delta'_4 \parallel \Lambda'_4$.

- $\Gamma_4 \parallel \emptyset \parallel \Lambda_4$: $\Lambda_4 = \Lambda_3 \gamma \cup [\gamma] = \{y = h(x \oplus v_3) \oplus w \oplus b \oplus a, z = x \oplus v_3, v_1 = v_2\}$ e

$$\Gamma_4 = \left\{ \begin{array}{ll} (1) & x \oplus h(x) \\ (4) & v_2 \oplus b \oplus x \oplus h(v_3) \end{array} \quad (5) \quad v_2 \oplus b \oplus x \oplus v_3 \oplus h(x) \right\}$$

Note que agora podemos aplicar a regra de simplificação na equação (4) pois quando unificamos $f(v_1) =^? f(v_2)$ tornamos v_2 uma variável solta. então ao aplicarmos de forma semelhante ao

Exemplo 3.4 temos o estado $\Gamma_5 \parallel \emptyset \parallel \Lambda_5$, onde:

$$\Gamma_5 = \left\{ \begin{array}{l} (1) \quad x \oplus h(x) \\ (4) \quad v_3 \oplus h(v_4) \\ (8) \quad v_4 \oplus x \oplus v_3 \end{array} \right\} \quad \Lambda_5 = \left\{ \begin{array}{l} y = h(x \oplus v_3) \oplus w \oplus b \oplus a \\ z = x \oplus v_3 \\ v_1 = b \oplus x \oplus v_3 \oplus h(x) \end{array} \right\}$$

E aplicando novamente a regra simplificação agora na equação (8) na variável solta v_3 temos o estado $\Gamma_6 \parallel \emptyset \parallel \Lambda_6$, onde:

$$\Gamma_6 = \left\{ \begin{array}{l} (1) \quad x \oplus h(x) \\ (4) \quad x \oplus v_4 \oplus h(v_4) \end{array} \right\} \quad \Lambda_6 = \left\{ \begin{array}{l} y = h(v_4) \oplus w \oplus b \oplus a \\ z = v_4 \\ v_1 = b \oplus v_4 \oplus h(x) \\ v_2 = b \oplus v_4 \oplus h(x) \\ v_3 = x \oplus v_4 \end{array} \right\}$$

Não sendo mais possível aplicar as regras trivial, simplificação e N-decomposição

- $\Gamma'_4 \parallel \Delta'_4 \parallel \Lambda'_4$: $\Lambda'_4 = \Lambda_3$ $\Gamma'_4 = \Gamma_3$ $\Delta'_4 = \{f(v_1) \neq f(v_2)\}$ Note que todas as variáveis deste estado estão presas e não é possível aplicar N-decomposição.

Nulificação: Uma regra simples para resolver o problema específico $x \oplus h(x) =^? 0$, a única solução é fazendo $x = 0$.

Nulificação

$$\frac{\widehat{\Gamma} \cup \{S \oplus h(t)\} \parallel \Delta \parallel \Lambda}{\widehat{\Gamma} \cup \{S, t\} \parallel \Delta \parallel \Lambda} \text{Null}$$

Condições:

- Para cada $S_i \in \Gamma = \widehat{\Gamma} \cup \{S \oplus h(t)\}$, temos que $S_i = x_{i1} \oplus \dots \oplus x_{ik_i} \oplus h(s_i)$, tais que x_{ij} são variáveis presas de Γ e $k_i \in \mathbb{N}$

Exemplo 3.6. Continuando o Exemplo 3.5. Observe que temos dois estados em execução de forma paralela, $\Gamma_6 \parallel \emptyset \parallel \Lambda_6$ e $\Gamma_3 \parallel \Delta'_4 \parallel \Lambda_3$:

- $\Gamma_3 \parallel \Delta'_4 \parallel \Lambda_3$:

Observe que em Γ_3 existe uma equação contendo $f(v_1)$ uma não variável e $f \neq h$ e portanto não é possível aplicar a regra nulificação, logo é um estado de falha pois $\Gamma_3 \neq \emptyset$.

- $\Gamma_6 \parallel \emptyset \parallel \Lambda_6$: podemos aplicar a regra [Simp] sobre a equação (1) pois contém o símbolo h , todas as variáveis de Γ_6 são presas e toda equação não tem nenhum símbolo de função não interpretado. Obtendo o estado $\Gamma_7 \parallel \emptyset \parallel \Lambda_7$, onde:

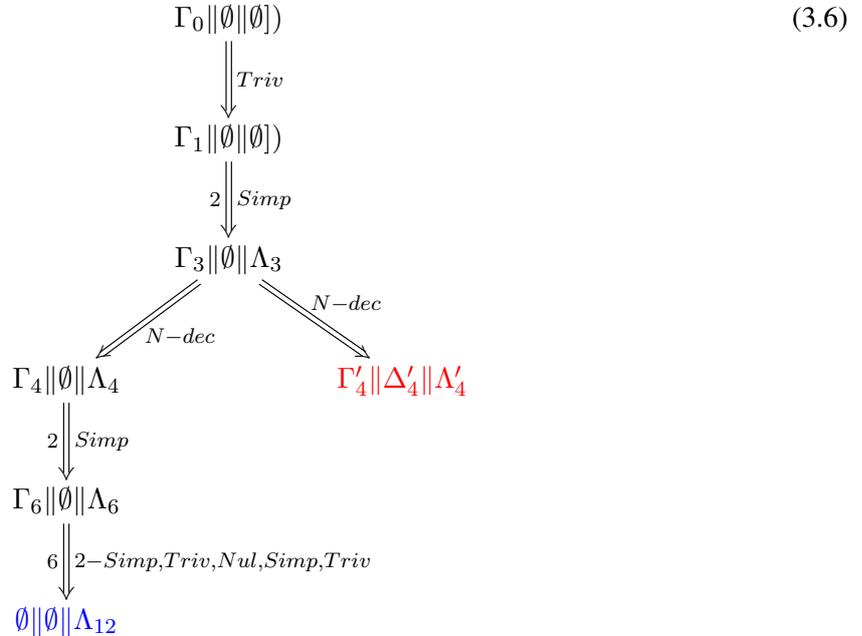
$$\Gamma_7 = \left\{ \begin{array}{ll} (1) & x \\ (4) & x \oplus v_4 \oplus h(v_4) \end{array} \right. \quad (9) \quad x \quad \left. \right\} \quad \Lambda_7 = \Lambda_6$$

Aplicando agora a regra simplificação na equação (9), seja $\gamma = \{x \mapsto 0\}$ então obtemos o estado $\Gamma_8 \parallel \emptyset \parallel \Lambda_8$, onde:

$$\Gamma_8 = \left\{ \begin{array}{ll} (1) & 0 \\ (4) & v_4 \oplus h(v_4) \end{array} \right\} \quad \Lambda_8 = \left\{ \begin{array}{ll} y = h(v_4) \oplus w \oplus b \oplus a & v_2 = b \oplus v_4 \\ z = v_4 & v_3 = v_4 \\ v_1 = b \oplus v_4 & x = 0 \end{array} \right\}$$

Aplicando agora as regras nessa sequência trivial, nulificação, simplificação e trivial obtemos o estado $\emptyset \parallel \emptyset \parallel \Lambda_{12}$, tal que: $\Lambda_{12} = \{y = w \oplus b \oplus a, z = 0, v_1 = b, v_2 = b, v_3 = 0, x = 0, v_4 = 0\}$.

Podemos representar a execução do algoritmo \mathcal{J}_{XORh} como um árvore de estados. Para esses exemplos acima, vamos exibir sua representação em árvore:



Vamos provar que se $\emptyset \parallel \Delta \parallel \Lambda$ é um estado válido de \mathcal{J}_{XORh} obtido do estado inicial $\Gamma \parallel \emptyset \parallel \emptyset$ então a substituição $\sigma_\Lambda := \{x \mapsto S \mid x = S \in \Lambda\}$ é um ACUNh-unificador de Γ . Se $\tilde{\Gamma} \parallel \tilde{\Delta} \parallel \tilde{\Lambda}$ for um estado de falha obtido do estado inicial $\Gamma \parallel \emptyset \parallel \emptyset$ então $\sigma_{\tilde{\Lambda}}$ não é um ACUNh-unificador de Γ , chamaremos isso por *corretude* de \mathcal{J}_{XORh} . Também provaremos que se σ é um ACUNh-unificador de Γ , então existe algum estado de solução $\emptyset \parallel \Delta \parallel \Lambda$ obtido do estado inicial $\Gamma \parallel \emptyset \parallel \emptyset$ tal que $\sigma|_{\mathcal{V}ar(\Gamma)}$ é uma instância de σ_Λ , isto é, σ_Λ é um ACUNh-unificador de Γ mais geral que σ sobre $\mathcal{V}ar(\Gamma)$, chamaremos isso por completude de \mathcal{J}_{XORh} .

Definição 3.11. *Sejam $\Gamma \parallel \Delta \parallel \Lambda$ e $\Gamma' \parallel \Delta' \parallel \Lambda'$ dois estados válidos de \mathcal{J}_{XORh} . definimos a relação $\Longrightarrow_{\mathcal{J}_{XORh}}$ sobre o conjunto de todos os estados válidos de \mathcal{J}_{XORh} , como: $\Gamma \parallel \Delta \parallel \Lambda \Longrightarrow_{\mathcal{J}_{XORh}} \Gamma' \parallel \Delta' \parallel \Lambda'$ se, e somente se, $\Gamma' \parallel \Delta' \parallel \Lambda'$ é obtido de $\Gamma \parallel \Delta \parallel \Lambda$ por alguma regra de inferência de \mathcal{J}_{XORh} . Quando quisermos explicitar a regra de inferência utilizada, substituiremos \mathcal{J}_{XORh} por *Triv*, *Simp*, *N-dec* e *Nul*.*

Definição 3.12 (Solução de $\Gamma \parallel \Delta \parallel \Lambda$). *Seja $\Gamma \parallel \Delta \parallel \Lambda$ um estado de \mathcal{J}_{XORh} , e σ uma substituição. Dizemos que σ é uma solução de $\Gamma \parallel \Delta \parallel \Lambda$, e denotaremos por $\sigma \models \Gamma \parallel \Delta \parallel \Lambda$ se, e somente se, para cada termo $T \in \Gamma$, inequação $s \neq t \in \Delta$ e variável resolvida $x = S \in \Lambda$ tem-se que, $T\sigma =_{\oplus_h} 0$, $s\sigma \neq_{\oplus_h} t\sigma$ e $x\sigma =_{\oplus_h} S\sigma$. Quando quisermos ignorar o conjunto Δ diremos que σ é uma solução de $\Gamma \parallel \Lambda$ se, e somente se, $\sigma \models \Gamma \parallel \emptyset \parallel \Lambda$, denotando por $\sigma \models \Gamma \parallel \Lambda$.*

Definição 3.13 (Extensão dirigida). *Sejam os estados $\Gamma \parallel \Delta \parallel \Lambda$, $\Gamma' \parallel \Delta' \parallel \Lambda'$ de \mathcal{J}_{XORh} , dizemos que $\Gamma' \parallel \Delta' \parallel \Lambda'$ é uma extensão dirigida de $\Gamma \parallel \Delta \parallel \Lambda$ se, e somente se, para toda substituição σ tal que $\sigma \models \Gamma \parallel \Delta \parallel \Lambda$ existe uma substituição γ tal que $\text{Dom}(\gamma) \subseteq \mathcal{V}ar(\Gamma', \Lambda') \setminus \mathcal{V}ar(\Gamma, \Lambda)$ e $\sigma\gamma \models \Gamma' \parallel \Delta' \parallel \Lambda'$.*

Vamos apresentar um esquema do algoritmo de ACUNh-unificação \mathcal{J}_{XORh} , onde o símbolo de função binária **concat**, é interpretado como concatenação de listas, assim sendo, o resultado é uma lista de substituições. Esquema em código de programação:

Algoritmo 1: Algoritmo de ACUNh-unificação \mathcal{J}_{XORh}

```

1  $\mathcal{J}_{XORh}(\Gamma\|\Delta\|\Lambda)$  /* Algoritmo de ACUNh-unificação */
   |
   | Data: um estado válido  $\Gamma\|\Delta\|\Lambda$  de  $\mathcal{J}_{XORh}$ 
   | Result: Lista  $L$  de ACUNh-unificadores  $\Gamma$ 
2 if  $\Gamma\|\Delta\|\Lambda \Rightarrow_{Triv} \Gamma'\|\Delta'\|\Lambda'$  then
3   | return  $\text{concat}(\emptyset, \mathcal{J}_{XORh}(\Gamma'\|\Delta'\|\Lambda'))$ 
4 else
5   | if  $\Gamma\|\Delta\|\Lambda \Rightarrow_{Simp} \Gamma'\|\Delta'\|\Lambda'$  then
6     | return  $\text{concat}(\emptyset, \mathcal{J}_{XORh}(\Gamma'\|\Delta'\|\Lambda'))$ 
7   else
8     | if  $\Gamma\|\Delta\|\Lambda \Rightarrow_{N-Dec} \Gamma'\|\Delta'\|\Lambda' \vee \Gamma''\|\Delta''\|\Lambda''$  then
9       | return  $\text{concat}(\mathcal{J}_{XORh}(\Gamma'\|\Delta'\|\Lambda'), \mathcal{J}_{XORh}(\Gamma''\|\Delta''\|\Lambda''))$ 
10    else
11      | if  $\Gamma\|\Delta\|\Lambda \Rightarrow_{Nul} \Gamma'\|\Delta'\|\Lambda'$  then
12        | return  $\text{concat}(\emptyset, \mathcal{J}_{XORh}(\Gamma'\|\Delta'\|\Lambda'))$ 
13      end
14    end
15  end
16 end
17 if  $\Gamma = \emptyset$  then
18   | return  $\{\sigma_\Lambda\}$ 
19 else
20   | return  $\emptyset$ 
21 end

```

O algoritmo \mathcal{J}_{XORh} só é possível ser aplicado em estados $\Gamma\|\Delta\|\Lambda$ tal que Γ está em sua forma pura, e portanto vamos provar que dado um estado inicial $\tilde{\Gamma}\|\emptyset\|\emptyset$ onde $\tilde{\Gamma}$ está em sua forma pura e se $\Gamma\|\Delta\|\Lambda$

é obtido de $\tilde{\Gamma} \parallel \emptyset \parallel \emptyset$ por regras de inferência de \mathcal{J}_{XORh} então temos que Γ está em sua forma pura.

Proposição 3.4. *Seja $\Gamma \parallel \Delta \parallel \Lambda$ um estado válido de \mathcal{J}_{XORh} tal que Γ está em sua forma pura. Se $\Gamma \parallel \Delta \parallel \Lambda \Longrightarrow_{\mathcal{J}_{XORh}} \Gamma' \parallel \Delta' \parallel \Lambda'$ então $\Gamma' \parallel \Delta' \parallel \Lambda'$ é um estado válido e Γ' está em sua forma pura.*

Demonstração. Sejam $\Gamma \parallel \Delta \parallel \Lambda$ e $\Gamma' \parallel \Delta' \parallel \Lambda'$ como na hipótese, portanto existe um estado inicial $\hat{\Gamma} \parallel \emptyset \parallel \emptyset$ tal que $\hat{\Gamma} \parallel \emptyset \parallel \emptyset \Longrightarrow_{\mathcal{J}_{XORh}}^* \Gamma \parallel \Delta \parallel \Lambda$, e como $\Gamma \parallel \Delta \parallel \Lambda \Longrightarrow_{\mathcal{J}_{XORh}} \Gamma' \parallel \Delta' \parallel \Lambda'$ por hipótese, obtemos

$$\hat{\Gamma} \parallel \emptyset \parallel \emptyset \Longrightarrow_{\mathcal{J}_{XORh}}^* \Gamma \parallel \Delta \parallel \Lambda \Longrightarrow_{\mathcal{J}_{XORh}} \Gamma' \parallel \Delta' \parallel \Lambda'$$

e portanto $\Gamma' \parallel \Delta' \parallel \Lambda'$ é um estado válido.

Para provar que Γ' está em sua forma pura, vamos avaliar cada regra de inferência de \mathcal{J}_{XORh} .

- (a) *Trivial:* Então $\Gamma = \tilde{\Gamma} \cup \{0\}$ e $\Gamma' = \tilde{\Gamma}$. Logo por Γ estar em sua forma pura então $\tilde{\Gamma}$ está em sua forma pura.
- (b) *Simplificação:* Então $\Gamma = \tilde{\Gamma} \cup \{x \oplus S\}$, $\Gamma' = Purif(\tilde{\Gamma}\gamma \downarrow)$ onde $\gamma := \{x \mapsto S\}$ e portanto por definição da regra *simplificação* temos que Γ' está em sua forma pura.
- (c) *N-decomposição:* Então $\Gamma = \tilde{\Gamma} \cup \{s \oplus t \oplus T\}$, onde s, t são termos puros tais que $raíz(s) = raíz(t) \neq h$. Neste caso obtemos uma bifurcação e portanto existem dois casos:
 - i) $\Gamma' = \tilde{\Gamma}\gamma \downarrow \cup \{T\gamma \downarrow\}$, onde γ é um mgu sintático da equação $s =^? t$ e por s, t serem termos puros que não contém os símbolos de função \oplus, h então os símbolos de função \oplus, h não ocorrem em $Im(\gamma)$, portanto se S é uma soma pura ou termo puro em sua forma normal então $S\gamma \downarrow$ também é e portanto Γ' está em sua forma pura.
 - ii) $\Gamma' = \Gamma$, neste ramo é trivialmente verdadeiro, pois Γ já se encontra em sua forma pura.
- (d) *Nulificação:* $\Gamma = \tilde{\Gamma} \cup \{S \oplus h(t)\}$ e $\Gamma' = \tilde{\Gamma} \cup \{S, t\}$, logo Γ está em sua forma pura pois $\tilde{\Gamma}$ está em sua forma pura, S é soma pura ou termo puro e t é um termo puro.

□

Corolário 3.2. *Seja $\Gamma \parallel \Delta \parallel \Lambda$ é um estado válido de \mathcal{J}_{XORh} tal que Γ está em sua forma pura. Se $\Gamma \parallel \Delta \parallel \Lambda \Longrightarrow_{\mathcal{J}_{XORh}}^* \Gamma' \parallel \Delta' \parallel \Lambda'$ então $\Gamma' \parallel \Delta' \parallel \Lambda'$ é um estado válido e Γ' está em sua forma pura.*

Demonstração. Por uma indução simples sobre a quantidade de regras foram aplicadas, usando a Proposição 3.4 demonstrado acima como passo da indução. □

3.2.1 Terminação de \mathcal{J}_{XORh}

Nesta seção vamos provar que \mathcal{J}_{XORh} é terminante, isto é, não existe uma sequência infinita de estados válidos $\{\Gamma_i \parallel \Delta_i \parallel \Lambda_i\}_{i \in \mathbb{N}}$ tal que

$$\Gamma_i \parallel \Delta_i \parallel \Lambda_i \Longrightarrow_{\mathcal{J}_{XORh}} \Gamma_{i+1} \parallel \Delta_{i+1} \parallel \Lambda_{i+1}. \forall i \in \mathbb{N}$$

Para isso criaremos uma medida μ do conjunto dos estados válidos de \mathcal{J}_{XORh} em \mathbb{N}^4 , que decresce a cada passo de \mathcal{J}_{XORh} na relação *noetheriana* $>_{lex}$, isto é a relação lexicográfica sobre $>$.

Definição 3.14. *Uma relação $>$ é dita noetheriana em M se, e somente se, não existe uma sequência infinita $\{a_i\}_{i \in \mathbb{N}} \subseteq M$ tal que $a_i > a_{i+1}$ para cada $i \in \mathbb{N}$.*

Definição 3.15 (Relação lexicográfica). *Seja a relação $>$ noetheriana em \mathbb{N}^n usual. Definimos a relação $>_{lex}$ sobre a relação $>$, isto é a relação lexicográfica em \mathbb{N}^n por:*

$$(a_1, \dots, a_n) >_{lex} (b_1, \dots, b_n) \Leftrightarrow \exists i \in \{1, \dots, n\}. \forall j < i, a_j = b_j \text{ e } a_i > b_i$$

Observação 3.5. *A relação lexicográfica $>_{lex}$ sobre a relação noetheriana $>$ usual de \mathbb{N} é também noetheriana.*

Os seguintes conceitos serão necessários para a construção de μ .

Definição 3.16. 1. $P := \{\text{Purif}(\Gamma \downarrow) \mid \Gamma \text{ é um problema de XORh-unificação padronizado}\}$, podemos identificar P com o conjunto de todos os subconjuntos finitos de termos puros ou somas puras em sua forma normal.

2. Definimos $E_v := \{\Gamma' \parallel \Delta' \parallel \Lambda' \mid \exists \Gamma \in P. \Gamma \parallel \emptyset \parallel \emptyset \Longrightarrow_{\mathcal{J}_{XORh}}^* \Gamma' \parallel \Delta' \parallel \Lambda'\}$, o conjunto de todos os estados válidos de \mathcal{J}_{XORh} .

3. $\text{Par}(\Delta) := \{(s, t) \mid s \neq t \in \Delta\}$

4. $\text{Par}(\Gamma) := \{(s, t) \mid s, t \text{ são subtermos em } \Gamma \text{ e } \text{ratz}(s) = \text{ratz}(t) \notin \{\oplus, h\}\}$

5. $\text{Par}(\Gamma \setminus \Delta) =: \text{Par}(\Gamma) \setminus \text{Par}(\Delta)$

6. $\#_h(\Gamma) :=$ o número de ocorrências do símbolo de função h em Γ .

Então com os conjuntos acima definiremos funções de $E_v \longrightarrow \mathbb{N}$ da seguinte forma:

$$i) \mu_1(\Gamma \parallel \Delta \parallel \Lambda) := \#_h(\Gamma)$$

$$ii) \mu_2(\Gamma \parallel \Delta \parallel \Lambda) := |\mathcal{V}ar(\Gamma)|$$

$$iii) \mu_3(\Gamma \parallel \Delta \parallel \Lambda) := |\Sigma(\Gamma)|$$

$$iv) \mu_4(\Gamma \parallel \Delta \parallel \Lambda) := |\mathit{Par}(\Gamma \setminus \Delta)|$$

Portanto definimos medida $\mu : E_v \longrightarrow \mathbb{N}^4$ onde: $\mu = (\mu_1, \mu_2, \mu_3, \mu_4)$.

Lema 3.16. *Sejam $\Gamma \parallel \Delta \parallel \Lambda$ e $\Gamma' \parallel \Delta' \parallel \Lambda'$ estados válidos de \mathcal{J}_{XORh} . Se $\Gamma \parallel \Delta \parallel \Lambda \Longrightarrow_{\mathcal{J}_{XORh}} \Gamma' \parallel \Delta' \parallel \Lambda'$ então $\mu(\Gamma \parallel \Delta \parallel \Lambda) >_{lex} \mu(\Gamma' \parallel \Delta' \parallel \Lambda')$.*

Demonstração. Vamos provar que para cada regra de inferência de \mathcal{J}_{XORh} a medida μ decresce.

$$a) \Gamma \parallel \Delta \parallel \Lambda \Longrightarrow_{\mathit{Triv}} \Gamma' \parallel \Delta' \parallel \Lambda':$$

Então $\Gamma = \tilde{\Gamma} \cup \{0\}$ e $\Gamma' = \tilde{\Gamma}$. Se $S \in \Gamma$ é um termo que contém o símbolo de função h então $S \in \tilde{\Gamma}$ e portanto $\#_h(\Gamma) = \#_h(\tilde{\Gamma})$, equivalentemente: $\mu_1(\Gamma \parallel \Delta \parallel \Lambda) = \mu_1(\Gamma' \parallel \Delta' \parallel \Lambda')$.

Como $\mathcal{V}ar(\Gamma) = \mathcal{V}ar(\tilde{\Gamma})$, então $|\mathcal{V}ar(\Gamma)| = |\mathcal{V}ar(\tilde{\Gamma})|$. Logo, $\mu_2(\Gamma \parallel \Delta \parallel \Lambda) = \mu_2(\Gamma' \parallel \Delta' \parallel \Lambda')$.

Por outro lado, um símbolo 0 foi removido, e então a quantidade de símbolos de função 0 ocorrendo em $\tilde{\Gamma}$ é menor que em Γ , portanto $|\Sigma(\tilde{\Gamma})| < |\Sigma(\Gamma)|$, isto é, $\mu_3(\Gamma' \parallel \Delta' \parallel \Lambda') < \mu_3(\Gamma \parallel \Delta \parallel \Lambda)$.

E então pela definição da relação $>_{lex}$ temos que, $\mu(\Gamma \parallel \Delta \parallel \Lambda) >_{lex} \mu(\Gamma' \parallel \Delta' \parallel \Lambda')$.

$$b) \Gamma \parallel \Delta \parallel \Lambda \Longrightarrow_{\mathit{Simp}} \Gamma' \parallel \Delta' \parallel \Lambda':$$

Então $\Gamma = \tilde{\Gamma} \cup \{x \oplus S\}$ e $\Gamma' = \mathit{Purif}(\tilde{\Gamma} \downarrow \gamma)$ onde $\gamma := \{x \mapsto S\}$. Podem ocorrer dois casos:

1. S não possui ocorrências do símbolo de função h . Como cada ocorrência de x em Γ é substituída por S , a quantidade de símbolos de função h não se altera, então temos $\#_h(\Gamma) = \#_h(\Gamma')$, logo:

$$\mu_1(\Gamma \parallel \Delta \parallel \Lambda) = \mu_1(\Gamma' \parallel \Delta' \parallel \Lambda')$$

Por outro lado, $\mathit{Im}(\gamma) = \{S\}$, isto é, γ não introduz novas variáveis, e remove todas as ocorrências da variável x em Γ , implicando que $\mathcal{V}ar(\Gamma') \subseteq \mathcal{V}ar(\Gamma) \setminus \{x\}$ então $|\Gamma| > |\Gamma'|$, equivalentemente:

$$\mu_2(\Gamma \parallel \Delta \parallel \Lambda) > \mu_2(\Gamma' \parallel \Delta' \parallel \Lambda')$$

2. S possui uma ocorrência do símbolo h . Para cada $x \oplus T \in \tilde{\Gamma}$, tem-se que T possui um ocorrência do símbolo de função h . Após aplicar γ em $\tilde{\Gamma}$, normalizar e purificar obtemos Γ' tal que não são inseridos novos símbolos h em Γ' pois por x ser uma variável solta, então x ocorre apenas da forma $x \oplus T \in \tilde{\Gamma}$ e ao normalizar os símbolos h se unem, da forma $(h(s) \oplus h(t)) \downarrow = h(s \oplus t) \downarrow$. Então $\#_h(\Gamma') \leq \#_h(\tilde{\Gamma}) < \#_h(\Gamma)$ pois S possui um símbolo de função h , e portanto: $\mu_1(\Gamma \parallel \Delta \parallel \Lambda) > \mu_1(\Gamma' \parallel \Delta' \parallel \Lambda')$,

Então em ambos os casos obtemos $\mu(\Gamma \parallel \Delta \parallel \Lambda) >_{lex} \mu(\Gamma' \parallel \Delta' \parallel \Lambda')$.

c) $\Gamma \parallel \Delta \parallel \Lambda \implies_{N-dec} \Gamma' \parallel \Delta' \parallel \Lambda'$:

Então $\Gamma = \tilde{\Gamma} \cup \{s \oplus t \oplus T\}$, onde s, t são termos puros tais que $raiz(s) = raiz(t) \neq h$, e sem perda de generalidade são, s, t são unificáveis sintaticamente com $s \neq t \notin \Delta$, caso não sejam sintaticamente unificáveis, então apenas o segundo ramo é criado. Assim temos dois casos para analisar:

- Se $\Gamma' = \tilde{\Gamma}\gamma \downarrow \cup \{T\gamma \downarrow\}$, $\Delta' = \Delta\gamma \downarrow$ e $\Lambda' = \Lambda\gamma \downarrow \cup [\gamma]$ onde γ é um mgu sintático de $s =? t$ com $Dom(\gamma) \subseteq Var(s) \cup Var(t)$, $Var(Im(\gamma)) \subseteq Var(\Gamma)$ e γ idempotente. Como s, t são termos puros então \oplus, h não ocorre em $Im(\gamma)$ e novos símbolos de função h não são inseridos em Γ' . Logo $\#_h(\Gamma) \geq \#_h(\Gamma')$ e portanto obtemos: $\mu_1(\Gamma \parallel \Delta \parallel \Lambda) \geq \mu_1(\Gamma' \parallel \Delta' \parallel \Lambda')$.

Como Γ esta em sua forma pura então cada termo em Γ está em sua forma normal, em particular $s \oplus t \oplus T$ está em sua forma normal, assim temos $s \neq_{\oplus_h} t$ e então $s \neq t$. Porém s, t são unificáveis por γ e portanto $\emptyset \neq Dom(\gamma) \subseteq Var(s) \cup Var(t)$, pois caso contrário $s\gamma = s$ e $t\gamma = t$ e portanto $s\gamma = s \neq t = t\gamma$ que é uma contradição. Como γ não insere novas variáveis e é idempotente temos que $Var(\Gamma') \subseteq Var(\Gamma) \setminus Dom(\gamma)$, implicando que $|Var(\Gamma')| = |Var(\Gamma) \setminus Dom(\gamma)| < |Var(\Gamma)|$. Equivalentemente, $\mu_2(\Gamma \parallel \Delta \parallel \Lambda) > \mu_2(\Gamma' \parallel \Delta' \parallel \Lambda')$.

- Se $\Gamma' = \Gamma$, $\Delta' = \Delta \dot{\cup} \{s \neq t\}$ e $\Lambda' = \Lambda$, então $Var(\Gamma') = Var(\Gamma)$ e $\Sigma(\Gamma) = \Sigma(\Gamma')$, então valem as seguintes igualdades $\#_h(\Gamma) = \#_h(\Gamma')$, $|Var(\Gamma')| = |Var(\Gamma)|$ e $|\Sigma(\Gamma')| = |\Sigma(\Gamma)|$. Assim, $\mu_1(\Gamma \parallel \Delta \parallel \Lambda) = \mu_1(\Gamma' \parallel \Delta' \parallel \Lambda')$, $\mu_2(\Gamma \parallel \Delta \parallel \Lambda) = \mu_2(\Gamma' \parallel \Delta' \parallel \Lambda')$ e $\mu_3(\Gamma \parallel \Delta \parallel \Lambda) = \mu_3(\Gamma' \parallel \Delta' \parallel \Lambda')$. Como, $Par(\Gamma) = Par(\Gamma')$ e $Par(\Delta') = Par(\Delta) \dot{\cup} \{(s, t)\}$ temos

$$\begin{aligned} Par(\Gamma' \setminus \Delta') &= Par(\Gamma') \setminus Par(\Delta') = Par(\Gamma) \setminus (Par(\Delta) \cup \{(s, t)\}) \\ &= (Par(\Gamma) \setminus Par(\Delta)) \setminus \{(s, t)\} = Par(\Gamma \setminus \Delta) \setminus \{(s, t)\} \end{aligned}$$

Observe que $(s, t) \in \text{Par}(\Gamma) \setminus \text{Par}(\Delta)$, então $(s, t) \in \text{Par}(\Gamma \setminus \Delta)$ e portanto, $|\text{Par}(\Gamma \setminus \Delta)| > |\text{Par}(\Gamma \setminus \Delta) \setminus \{(s, t)\}| = |\text{Par}(\Gamma \setminus \Delta)|$, equivalentemente: $\mu_4(\Gamma \parallel \Delta \parallel \Lambda) > \mu_4(\Gamma' \parallel \Delta' \parallel \Lambda')$.

Assim, $\mu(\Gamma \parallel \Delta \parallel \Lambda) >_{lex} \mu(\Gamma' \parallel \Delta' \parallel \Lambda')$

d) $\Gamma \parallel \Delta \parallel \Lambda \implies_{Nul} \Gamma' \parallel \Delta' \parallel \Lambda'$:

Então $\Gamma = \tilde{\Gamma} \cup \{S \oplus h(t)\}$ e $\Gamma' = \tilde{\Gamma} \cup \{S, t\}$ e como $h(t)$ é um termo puro t é um termo puro com $\text{raíz}(t) \neq h$. Assim $\#_h(\Gamma') = \#_h(\tilde{\Gamma})$, pois $S \oplus h(t)$ é uma soma pura então há ocorrências do símbolo de função h em S , isto é, $\#_h(\Gamma) > \#_h(\tilde{\Gamma}) = \#_h(\Gamma')$, e portanto: $\mu_1(\Gamma \parallel \Delta \parallel \Lambda) > \mu_1(\Gamma' \parallel \Delta' \parallel \Lambda')$. E portanto, obtemos: $\mu(\Gamma \parallel \Delta \parallel \Lambda) >_{lex} \mu(\Gamma' \parallel \Delta' \parallel \Lambda')$.

□

Teorema 3.3 (Terminação de \mathcal{J}_{XORh}). \mathcal{J}_{XORh} é terminante.

Demonstração. Sejam Γ um problema de ACUNh-unificação em sua forma padronizada e $\tilde{\Gamma} := \text{Purif}(\Gamma \downarrow)$. Vamos mostrar que não existe uma sequência infinita de aplicações das regras de \mathcal{J}_{XORh} sobre o estado inicial $\tilde{\Gamma} \parallel \emptyset \parallel \emptyset$. Suponha por absurdo que existe uma sequência infinita $\{E_i\}_{i \in \mathbb{N}}$ de estados válidos de \mathcal{J}_{XORh} onde $E_0 = \tilde{\Gamma} \parallel \emptyset \parallel \emptyset$ e para cada $i \in \mathbb{N}$ tem-se que $E_i \implies_{\mathcal{J}_{XORh}} E_{i+1}$.

Então defina a sequência $n_i := \mu(E_i) \in \mathbb{N}^4$, $i \in \mathbb{N}$, e pelo Lema 3.16 temos que $\mu(E_i) >_{lex} \mu(E_{i+1})$ e portanto $n_i >_{lex} n_{i+1}$ para cada $i \in \mathbb{N}$, isto é, $\{n_i\}_{i \in \mathbb{N}} \subseteq \mathbb{N}^4$ é uma sequência infinita tal que $n_i >_{lex} n_{i+1}$ para cada $i \in \mathbb{N}$, porém $(\mathbb{N}^4, \geq_{lex})$ é um poset e \geq_{lex} é uma relação de ordem parcial noetheriana e portanto $>_{lex}$ não admite tal sequência, logo uma contradição. □

3.2.2 Correção de \mathcal{J}_{XORh}

Nesta seção provaremos a correção de \mathcal{J}_{XORh} , isto é, para cada substituição $\sigma \in S$ tem-se que σ é um ACUNh-unificador idempotente de Γ . No Lema a seguir usaremos a noção de solução de um estado $\Gamma \parallel \Delta \parallel \Lambda$ dada na Definição 3.2

Lema 3.17. *Sejam $\Gamma \parallel \Delta \parallel \Lambda$, $\Gamma' \parallel \Delta' \parallel \Lambda'$ estados válidos de \mathcal{J}_{XORh} tais que $\Gamma \parallel \Delta \parallel \Lambda \implies_{\mathcal{J}_{XORh}} \Gamma' \parallel \Delta' \parallel \Lambda'$. Se $\phi \models \Gamma' \parallel \Delta' \parallel \Lambda'$ então $\phi \models \Gamma \parallel \Delta \parallel \Lambda$.*

Demonstração. Sejam $\Gamma \parallel \Delta \parallel \Lambda$, $\Gamma' \parallel \Delta' \parallel \Lambda'$ e ϕ como na hipótese, vamos provar que o resultado vale para cada regra de inferência \mathcal{J}_{XORh} .

a) $\Gamma \parallel \Delta \parallel \Lambda \implies_{Triv} \Gamma' \parallel \Delta' \parallel \Lambda'$:

Então temos $\Lambda' = \Lambda$ e $\Gamma = \Gamma' \cup \{0\}$, pela hipótese, $\phi \models \Gamma' \parallel \Lambda'$ então para cada $T \in \Gamma'$ e para cada $x = S \in \Lambda'$ temos que $x\phi =_{\oplus_h} S\phi$ e $T\phi =_{\oplus_h} 0$.

Note que $0\phi =_{\oplus_h} 0$ então para cada $x = S \in \Lambda$ e cada $T \in \Gamma$ temos $x\phi =_{\oplus_h} S\phi$ e $T\phi =_{\oplus_h} 0$, equivalentemente, $\phi \models \Gamma \parallel \Lambda$.

b) $\Gamma \parallel \Delta \parallel \Lambda \implies_{Simp} \Gamma' \parallel \Delta' \parallel \Lambda'$:

Então temos $\Gamma = \tilde{\Gamma} \cup \{x \oplus S\}$, onde x é uma variável solta, e $\Gamma' = Purif(\tilde{\Gamma}\gamma \downarrow)$, $\Delta' = \Delta\gamma \downarrow$ e $\Lambda' = \Lambda\gamma \downarrow \cup \{x = S\}$ onde $\gamma = \{x \mapsto S\}$. Como x é uma variável solta de Γ e $x \oplus S$ está em sua forma normal então $x \notin \mathcal{V}ar(S)$ e portanto γ é idempotente.

Vamos provar que $\phi \models \Gamma \parallel \Lambda$

1. Para cada $T \in \Gamma$ tem-se que $T\phi =_{\oplus_h} 0$:

Tome $T \in \Gamma$ qualquer.

• $x \in \mathcal{V}ar(T)$:

Caso $T = x \oplus S$ então obtemos $T\gamma = x\gamma \oplus S = S \oplus S =_{\oplus_h} 0$; caso contrário, $T =_{AC} x \oplus T'$ pois x é uma variável solta de Γ . Logo $x \notin \mathcal{V}ar(T')$ pois $x \oplus T'$ está em sua forma normal. Seja o conjunto $P := Purif(\{(x \oplus T')\gamma \downarrow\})$ então P é uma extensão conservativa de $\{(x \oplus T')\gamma \downarrow\}$. Note que $P \subseteq \Gamma'$. Como por hipótese $\phi \models \Gamma' \parallel \Lambda'$, temos que ϕ é um ACUNh-unificador para P , então por P ser uma extensão conservativa de $\{(x \oplus T')\gamma \downarrow\}$, ϕ é um ACUNh-unificador de $((S \oplus T') \downarrow)\phi \downarrow =_{\oplus_h} 0$, equivalentemente, $(S \oplus T')\phi \downarrow =_{\oplus_h} 0$ e pelo Teorema 2.1 podemos concluir que $(S \oplus T')\phi =_{\oplus_h} 0$.

Note que $x = S \in \Lambda'$ e portanto $x\phi =_{\oplus_h} S\phi$, então temos as seguintes igualdades:

$$T\phi = (x \oplus T')\phi = x\phi \oplus T'\phi =_{\oplus_h} S\phi \oplus T'\phi = (S \oplus T')\phi =_{\oplus_h} 0$$

• $x \notin \mathcal{V}ar(T)$: Neste caso $T\gamma \downarrow = T \downarrow$. Como por hipótese Γ está em sua forma pura temos que $Purif(T \downarrow) = T \downarrow$ e então $T \downarrow \in \Gamma'$. Como $\phi \models \Gamma' \parallel \Lambda'$ temos que $T \downarrow \phi =_{\oplus_h} 0$, e portanto, $T \downarrow \phi \downarrow =_{\oplus_h} 0$, isto é, $T\phi \downarrow =_{\oplus_h} 0$ e pelo Teorema 2.1 obtemos $T\phi =_{\oplus_h} 0$.

2. Para cada $y = T \in \Lambda$ tem-se que $y\phi =_{\oplus_h} T\phi$:

Tome uma equação resolvida $y = T \in \Lambda$ qualquer, então $y = T\gamma \downarrow \in \Lambda'$.

- $x \in \mathcal{V}ar(T)$:

Defina o conjunto $X := \{p \in \mathcal{P}os(T) \mid T|_p = x\}$, em outros termos, o conjunto das posições de ocorrência da variável x em T .

Observe que para cada $p, q \in X$, $p \neq q$ então $p \parallel q$, pois são posições variáveis. Então enumerando o conjunto X obtemos $X = \{p_1, \dots, p_n\}$, e considere o seguinte contexto:

$$T[S]_X := T[S]_{p_1}[S]_{p_2} \cdots [S]_{p_n}$$

P definição de substituição, temos que $T[S]_{p_1}[S]_{p_2} \cdots [S]_{p_n} = T\gamma$, como $y = T\gamma \downarrow \in \Lambda'$, temos que $y\phi =_{\oplus_h} (T\gamma \downarrow)\phi$, e portanto,

$$y\phi =_{\oplus_h} y\phi \downarrow =_{AC} (T\gamma \downarrow)\phi \downarrow = T\gamma\phi \downarrow =_{\oplus_h} T\gamma\phi$$

Porém $T\gamma\phi = (T[S]_{p_1}[S]_{p_2} \cdots [S]_{p_n})\phi = (T[S]_X)\phi = (T\phi)[S\phi]_X$. Como $x = S \in \Lambda'$ temos que $x\phi =_{\oplus_h} S\phi$, portanto $T\gamma\phi = (T\phi)[S\phi]_X =_{\oplus_h} (T\phi)[S\phi]_X$.

Note que $T[x]_p = T$ para cada $p \in X$, pela definição do conjunto X e portanto:

$$(T\phi)[x\phi]_X = (T[x]_X)\phi = (T[x]_{p_1}[x]_{p_2} \cdots [x]_{p_n})\phi = T\phi$$

Assim concluindo que $y\phi =_{\oplus_h} T\gamma\phi =_{\oplus_h} (T\phi)[x\phi]_X = T\phi$.

- $x \notin \mathcal{V}ar(T)$:

Então $T\gamma \downarrow = T \downarrow$ logo $y = T \downarrow \in \Lambda'$, e pela hipótese de $\phi \models \Gamma' \parallel \Lambda'$, temos que $y\phi =_{\oplus_h} (T \downarrow)\phi$. Portanto obtemos: $y\phi =_{\oplus_h} y\phi \downarrow =_{AC} (T \downarrow)\phi \downarrow = T\phi \downarrow =_{\oplus_h} T\phi$.

Logo por (1) e (2) segue que $\phi \models \Gamma \parallel \Lambda$

c) $\Gamma \parallel \Delta \parallel \Lambda \implies_{N-dec} \Gamma' \parallel \Delta' \parallel \Lambda'$:

Temos $\Gamma = \tilde{\Gamma} \cup \{s \oplus t \oplus S\}$ e γ um mgu sintático de $s =^? t$.

Como N -decomposição bifurca para dois ramos então existem dois possíveis casos para o estado $\Gamma' \parallel \Delta' \parallel \Lambda'$.

- $\Gamma' = \Gamma$, $\Delta' = \Delta \cup \{s \neq t\}$ e $\Lambda' = \Lambda$: Esse caso é trivial pois $\Gamma' = \Gamma$ e $\Lambda' = \Lambda$ e portanto, $\phi \models \Gamma' \parallel \Lambda'$ implica que $\phi \models \Gamma \parallel \Lambda$.

- $\Gamma' = \tilde{\Gamma}\gamma \downarrow \cup \{S\gamma \downarrow\}$, $\Delta' = \Delta\gamma$ e $\Lambda' = \Lambda\gamma \cup [\gamma]$: Como $\phi \models \Gamma' \parallel \Lambda'$ e para cada $x \in \text{Dom}(\gamma)$, tem-se que $x = x\gamma \in \Lambda'$ segue que $x\phi =_{\oplus} x\gamma\phi$. Tomando $y \in \mathcal{V} \setminus \text{Dom}(\gamma)$ temos $y\gamma = y$ então $y\gamma\phi = y\phi =_{\oplus_h} y\phi$, donde concluímos que $\gamma\phi =_{\oplus_h} \phi$.

Vamos provar que $\phi \models \Gamma \parallel \Lambda$.

1. Tome $T \in \Gamma$ qualquer.

– $T \in \tilde{\Gamma}$:

Observe que $T\gamma \downarrow \in \Gamma'$, e por hipótese temos $\phi \models \Gamma' \parallel \Lambda'$, então $(T\gamma \downarrow)\phi =_{\oplus_h} 0$ e pelo Teorema 2.1 obtemos $(T\gamma \downarrow)\phi \downarrow =_{AC} 0$. Como $(T\gamma \downarrow)\phi \downarrow = T\gamma\phi \downarrow$ e $\gamma\phi =_{\oplus_h} \phi$ obtemos as seguintes igualdades:

$$0 =_{AC} (T\gamma \downarrow)\phi \downarrow = T\gamma\phi \downarrow =_{\oplus_h} T\gamma\phi =_{\oplus_h} T\phi.$$

– $T = s \oplus t \oplus S \in \Gamma$:

Como γ é um mgu de $s = ? t$ temos que $u = s\gamma = t\gamma$. Como $\gamma\phi =_{\oplus_h} \phi$ temos que $s\phi \oplus t\phi \oplus S\phi =_{\oplus_h} s\gamma\phi \oplus t\gamma\phi \oplus S\gamma\phi = u\phi \oplus u\phi \oplus S\gamma\phi =_{\oplus_h} S\gamma\phi$.

Por outro lado, $S\gamma\phi =_{\oplus_h} S\gamma\phi \downarrow = (S\gamma \downarrow)\phi \downarrow =_{\oplus_h} (S\gamma \downarrow)\phi$. Como por hipótese, $\phi \models \Gamma' \parallel \Lambda'$ e $S\gamma \downarrow \in \Gamma'$ temos que $(S\gamma \downarrow) =_{\oplus_h} 0$. Logo, para cada $T \in \Gamma$, $T\phi =_{\oplus_h} 0$.

2. Tome $y = T \in \Lambda$ qualquer então $y = T\gamma \downarrow \in \Lambda'$ e então, $y\phi =_{\oplus_h} (T\gamma \downarrow)\phi$.

Como $\gamma\phi =_{\oplus_h} \phi$ e $(T\gamma \downarrow)\phi \downarrow = T\gamma\phi \downarrow$ temos igualdades, $(T\gamma \downarrow)\phi =_{\oplus_h} (T\gamma \downarrow)\phi \downarrow = T\gamma\phi \downarrow =_{\oplus_h} T\gamma\phi =_{\oplus_h} T\phi$, concluindo que $y\phi =_{\oplus_h} T\phi$.

d) $\Gamma \parallel \Delta \parallel \Lambda \implies_{Nul} \Gamma' \parallel \Delta' \parallel \Lambda'$:

Pela definição da regra de inferência *nulificação* temos que $\Gamma = \tilde{\Gamma} \cup \{S \oplus h(t)\}$, $\Gamma' = \tilde{\Gamma} \cup \{S, t\}$, $\Delta' = \Delta$ e $\Lambda' = \Lambda$.

Por hipótese temos que $\phi \models \Gamma' \parallel \Lambda'$ e portanto para cada $T \in \Gamma'$ e para cada $x = T' \in \Lambda'$ tem-se que $T\phi =_{\oplus_h} 0$ e $x\phi =_{\oplus_h} T'\phi$. Falta provar apenas que $(S \oplus h(t))\phi =_{\oplus_h} 0$.

Note que $t \in \Gamma'$, logo $t\phi =_{\oplus_h} 0$, e lembrando que $h(0) =_{\oplus_h} 0$ é uma regra de *XORh* portanto obtemos: $(S \oplus h(t))\phi = S\phi \oplus h(t\phi) =_{\oplus_h} 0 \oplus h(0) =_{\oplus_h} 0$, e portanto $\phi \models \Gamma \parallel \Lambda$.

□

Lema 3.18. *Sejam $\Gamma \parallel \Delta \parallel \Lambda$, $\Gamma' \parallel \Delta' \parallel \Lambda'$ estados válidos de \mathcal{J}_{XORh} tais que $\Gamma \parallel \Delta \parallel \Lambda \implies^*_{\mathcal{J}_{XORh}} \Gamma' \parallel \Delta' \parallel \Lambda'$. Se $\phi \models \Gamma \parallel \Lambda'$ então $\phi \models \Gamma \parallel \Lambda$.*

Demonstração. Sejam $\Gamma \parallel \Delta \parallel \Lambda$, $\Gamma' \parallel \Delta' \parallel \Lambda'$ e ϕ como na hipótese. Então existe um $n \in \mathbb{N}$ tal que $\Gamma \parallel \Delta \parallel \Lambda \implies^n_{\mathcal{J}_{XORh}} \Gamma' \parallel \Delta' \parallel \Lambda'$, vamos provar por indução sobre n .

Hipótese de indução: Sejam $E_1 := \Gamma_1 \parallel \Delta_1 \parallel \Lambda_1$, $E_2 := \Gamma_2 \parallel \Delta_2 \parallel \Lambda_2$ estados válidos de \mathcal{J}_{XORh} tais que $E_1 \implies^m_{\mathcal{J}_{XORh}} E_2$ e $m < n$. Se $\varphi \models \Gamma_2 \parallel \Lambda_2$ então $\varphi \models \Gamma_1 \parallel \Lambda_1$.

Base da indução: Suponha $n = 0$ e portanto $\Gamma \parallel \Delta \parallel \Lambda \implies^0_{\mathcal{J}_{XORh}} \Gamma' \parallel \Delta' \parallel \Lambda'$ implicando que $\Gamma \parallel \Delta \parallel \Lambda = \Gamma' \parallel \Delta' \parallel \Lambda'$ e portanto $\Gamma' = \Gamma, \Delta' = \Delta$ e $\Lambda' = \Lambda$ e como por hipótese $\phi \models \Gamma' \parallel \Lambda'$ assim temos que $\phi \models \Gamma \parallel \Lambda$.

Suponha $n > 1$ então existe $\Gamma'' \parallel \Delta'' \parallel \Lambda''$ um estado válido de \mathcal{J}_{XORh} tal que:

$$\Gamma \parallel \Delta \parallel \Lambda \implies^{n-1}_{\mathcal{J}_{XORh}} \Gamma'' \parallel \Delta'' \parallel \Lambda'' \implies_{\mathcal{J}_{XORh}} \Gamma' \parallel \Delta' \parallel \Lambda'$$

Como $\phi \models \Gamma' \parallel \Lambda'$ temos que pelo Lema 3.17, $\phi \models \Gamma'' \parallel \Lambda''$ e como $n - 1 < n$ e $\Gamma \parallel \Delta \parallel \Lambda \implies^{n-1}_{\mathcal{J}_{XORh}} \Gamma'' \parallel \Delta'' \parallel \Lambda''$ temos pela hipótese de indução que $\phi \models \Gamma \parallel \Lambda$, como queríamos demonstrar.

Assim provamos que para todo $n \in \mathbb{N}$, se $\Gamma \parallel \Delta \parallel \Lambda \implies^n_{\mathcal{J}_{XORh}} \Gamma' \parallel \Delta' \parallel \Lambda'$ e $\phi \models \Gamma' \parallel \Lambda'$ então $\phi \models \Gamma \parallel \Lambda$. □

Iremos agora enunciar o *Teorema da Correção de \mathcal{J}_{XORh}* e demonstra-lo utilizando principalmente o Lema 3.18 e o fato de que cada solução gerada pelo algoritmo é uma substituição idempotente.

Lema 3.19. *Sejam $\Gamma \parallel \Delta \parallel \Lambda$, $\Gamma' \parallel \Delta' \parallel \Lambda'$ estados válidos de \mathcal{J}_{XORh} e substituições $\sigma_\Lambda := \{x \mapsto S \mid x = S \in \Lambda\}$, $\sigma_{\Lambda'} := \{x \mapsto S \mid x = S \in \Lambda'\}$ tais que $\Gamma \parallel \Delta \parallel \Lambda \implies^*_{\mathcal{J}_{XORh}} \Gamma' \parallel \Delta' \parallel \Lambda'$. Se σ_Λ é idempotente, então $\sigma_{\Lambda'}$ é idempotente.*

Demonstração. Sejam $\Gamma \parallel \Delta \parallel \Lambda$, $\Gamma' \parallel \Delta' \parallel \Lambda'$, σ_Λ e $\sigma_{\Lambda'}$ como na hipótese. Vamos provar para cada regra de inferência de \mathcal{J}_{XORh} .

a) $\Gamma \parallel \Delta \parallel \Lambda \implies_{Triv} \Gamma' \parallel \Delta' \parallel \Lambda'$:

Temos que $\Lambda' = \Lambda$ e portanto $\sigma_{\Lambda'} = \sigma_\Lambda$, e o resultado segue.

b) $\Gamma \parallel \Delta \parallel \Lambda \implies_{Simp} \Gamma' \parallel \Delta' \parallel \Lambda'$:

Temos que $\Gamma = \tilde{\Gamma} \cup \{x \oplus S\}$, $\Gamma' = Purif(\tilde{\Gamma} \gamma \downarrow)$, $\Delta' = \Delta \gamma \downarrow$ e $\Lambda' = \Lambda \gamma \downarrow \cup \{x = S\}$ onde $\gamma = \{x \mapsto S\}$ e x uma variável solta.

Afirmação: Para cada $y = T \in \Lambda$, $y \notin \mathcal{V}ar(S)$:

Observe que por $\Gamma \parallel \Delta \parallel \Lambda$ ser um estado válido de \mathcal{J}_{XORh} , então existe um estado inicial $\bar{\Gamma} \parallel \emptyset \parallel \emptyset$ tal que $\bar{\Gamma} \parallel \emptyset \parallel \emptyset \Longrightarrow_{\mathcal{J}_{XORh}}^* \Gamma \parallel \Delta \parallel \Lambda$ e portanto, para cada $y = T \in \Lambda$, existem $\Gamma_y \parallel \Delta_y \parallel \Lambda_y$, $\Gamma'_y \parallel \Delta'_y \parallel \Lambda'_y$ estados válidos de \mathcal{J}_{XORh} tais que $\Gamma_y = \tilde{\Gamma}_y \cup \{y \oplus T'\}$ onde y é uma variável solta de Γ_y , $\Gamma'_y = Purif((\tilde{\Gamma}_y)\gamma' \downarrow)$, $\Delta'_y = \Delta_y \gamma' \downarrow$, $\Lambda'_y = \Lambda_y \gamma' \downarrow \cup \{y = T'\}$ e

$$\bar{\Gamma} \parallel \emptyset \parallel \emptyset \Longrightarrow_{\mathcal{J}_{XORh}}^* \Gamma_y \parallel \Delta_y \parallel \Lambda_y \Longrightarrow_{Simp} \Gamma'_y \parallel \Delta'_y \parallel \Lambda'_y \Longrightarrow_{\mathcal{J}_{XORh}}^* \Gamma \parallel \Delta \parallel \Lambda$$

E portanto a variável $y \notin \mathcal{V}ar(\Gamma'_y)$ e como as regras de inferência só inserem variáveis novas, então $y \notin \mathcal{V}ar(\Gamma)$, em particular $y \notin \mathcal{V}ar(S)$.

Note que $\Lambda' = \Lambda \gamma \downarrow \cup \{x = S\}$ e portanto $\sigma_{\Lambda'} = \{y \mapsto T \gamma \downarrow \mid y = T \in \Lambda\} \cup \{x \mapsto S\}$. Como $\sigma_{\Lambda} = \{y \mapsto T \mid y = T \in \Lambda\}$ então: $\sigma_{\Lambda'} = \{y \mapsto y \sigma_{\Lambda} \gamma \downarrow \mid y \in \mathcal{D}om(\sigma_{\Lambda})\} \cup \{x \mapsto S\}$.

Por hipótese σ_{Λ} é idempotente então obtemos que para cada $y \in \mathcal{D}om(\sigma_{\Lambda})$ tem-se que $\mathcal{D}om(\sigma_{\Lambda}) \cap \mathcal{V}ar(y \sigma_{\Lambda}) = \emptyset$ e como $\mathcal{V}ar(y \sigma_{\Lambda} \gamma \downarrow) \subseteq (\mathcal{V}ar(y \sigma_{\Lambda}) \setminus \{x\}) \cup \mathcal{V}ar(S)$. pois $\gamma = \{x \mapsto S\}$, e pela afirmação temos que $\mathcal{D}om(\sigma_{\Lambda}) \cap \mathcal{V}ar(S) = \emptyset$. Além disso para cada $y \in \mathcal{D}om(\sigma_{\Lambda'}) \setminus \{x\} = \mathcal{D}om(\sigma_{\Lambda})$ temos $\mathcal{V}ar(y \sigma_{\Lambda'}) \cap \{x\} = \emptyset$. Assim,

$$\begin{aligned} (\mathcal{D}om(\sigma_{\Lambda'}) \setminus \{x\}) \cap \mathcal{V}ar(y \sigma_{\Lambda'}) &= \mathcal{D}om(\sigma_{\Lambda}) \cap \mathcal{V}ar(y \sigma_{\Lambda} \gamma \downarrow) \\ &\subseteq \mathcal{D}om(\sigma_{\Lambda}) \cap ((\mathcal{V}ar(y \sigma_{\Lambda})) \cup \mathcal{V}ar(S)) = \emptyset \end{aligned} \quad (3.7)$$

Portanto $\mathcal{D}om(\sigma_{\Lambda'}) \cap \mathcal{V}ar(y \sigma_{\Lambda'}) = \emptyset$ para cada $y \in \mathcal{D}om(\sigma_{\Lambda'}) \setminus \{x\}$ e como $x \sigma_{\Lambda'} = \mathcal{V}ar(S)$ então pela afirmação acima e por $x \notin \mathcal{V}ar(S)$ temos que $\mathcal{D}om(\sigma_{\Lambda'}) \cap \mathcal{V}ar(x \sigma_{\Lambda'}) = \mathcal{D}om(\sigma_{\Lambda'}) \cap \mathcal{V}ar(S) = \emptyset$, concluindo que para todo $y \in \mathcal{D}om(\sigma_{\Lambda'})$, $\mathcal{D}om(\sigma_{\Lambda'}) \cap \mathcal{V}ar(y \sigma_{\Lambda'}) = \emptyset$, e portanto $\sigma_{\Lambda'}$ é idempotente.

c) $\Gamma \parallel \Delta \parallel \Lambda \Longrightarrow_{N-dec} \Gamma' \parallel \Delta' \parallel \Lambda'$:

Temos $\Gamma = \tilde{\Gamma} \cup \{s \oplus t \oplus T\}$ e γ é um mgu idempotente de $s = ? t$, via unificação sintática, tal que $\mathcal{D}om(\gamma) \subseteq \mathcal{V}ar(s) \cup \mathcal{V}ar(t)$ e $\mathcal{V}ar(\mathcal{I}m(\gamma)) \subseteq \mathcal{V}ar(s) \cup \mathcal{V}ar(t) \subseteq \mathcal{V}ar(\Gamma)$.

Como provamos no item anterior que para cada $x = S \in \Lambda$, tem-se que $x \notin \mathcal{V}ar(\Gamma)$ e portanto para cada $x = S \in \Lambda$, $x \notin \mathcal{V}ar(\mathcal{I}m(\gamma))$, isto é, $\mathcal{D}om(\sigma_{\Lambda}) \cap \mathcal{V}ar(\mathcal{I}m(\gamma)) = \emptyset$. Por hipótese σ_{Λ} é idempotente, então $\mathcal{D}om(\sigma_{\Lambda}) \cap \mathcal{V}ar(\mathcal{I}m(\sigma_{\Lambda})) = \emptyset$, e portanto obtemos:

$$\mathcal{D}om(\sigma_{\Lambda}) \cap (\mathcal{V}ar(\mathcal{I}m(\gamma)) \cup \mathcal{V}ar(\sigma_{\Lambda})) = \emptyset \text{ e } \mathcal{D}om(\gamma) \cap \mathcal{V}ar(\mathcal{I}m(\gamma)) = \emptyset$$

Existem dois ramos na inferência, então analisaremos separadamente cada um:

- $\Gamma' = \Gamma, \Delta' = \Delta \dot{\cup} \{s \neq t\}$ e $\Lambda' = \Lambda$: Logo $\sigma_{\Lambda'} = \sigma_{\Lambda}$ e portanto pela hipótese de σ_{Λ} ser idempotente então $\sigma_{\Lambda'}$ é idempotente.
- $\Gamma' = \tilde{\Gamma}\gamma \downarrow, \Delta' = \Delta\gamma \downarrow$ e $\Lambda' = \Lambda\gamma \cup [\gamma]$:
Análogo ao caso da regra simplificação, com a diferença de que $[\gamma]$ pode incluir mais de uma variável no domínio, pelo mesmo raciocínio da regra *simplificação* obtemos que:

$$\sigma_{\Lambda'} := \{x \mapsto x\sigma_{\Lambda}\gamma \downarrow \mid x \in \mathcal{D}om(\sigma_{\Lambda})\} \cup \gamma$$

Portanto temos $\mathcal{D}om(\sigma_{\Lambda'}) = \mathcal{D}om(\sigma_{\Lambda}) \cup \mathcal{D}om(\gamma)$ e,

$$\mathcal{V}ar(\mathcal{I}m(\sigma_{\Lambda'})) \subseteq \left(\mathcal{V}ar(\mathcal{I}m(\sigma_{\Lambda})) \setminus \mathcal{D}om(\gamma) \right) \cup \mathcal{V}ar(\mathcal{I}m(\gamma))$$

Então podemos concluir que $\mathcal{D}om(\sigma_{\Lambda'}) \cap \mathcal{V}ar(\mathcal{I}m(\sigma_{\Lambda'})) = \emptyset$.

d) $\Gamma \parallel \Delta \parallel \Lambda \Longrightarrow_{Nul} \Gamma' \parallel \Delta' \parallel \Lambda'$: Temos que $\Lambda' = \Lambda$ e portanto por $\sigma_{\Lambda'}$ é idempotente.

□

Lema 3.20. Se $\Gamma \parallel \Delta \parallel \Lambda$ um estado válido de \mathcal{J}_{XORh} então σ_{Λ} é uma substituição idempotente.

Demonstração. Como $\Gamma \parallel \Delta \parallel \Lambda$ é um estado válido de \mathcal{J}_{XORh} então existe um estado inicial $\hat{\Gamma} \parallel \emptyset \parallel \emptyset$ e um $n \in \mathbb{N}$ tais que $\hat{\Gamma} \parallel \emptyset \parallel \emptyset \Longrightarrow_{\mathcal{J}_{XORh}}^n \Gamma \parallel \Delta \parallel \Lambda$.

Vamos provar por indução sobre $n \in \mathbb{N}$:

Hipótese de indução: Se $\Gamma' \parallel \Delta' \parallel \Lambda'$ é um estado válido de \mathcal{J}_{XORh} onde existe um estado inicial $\hat{\Gamma}' \parallel \emptyset \parallel \emptyset$ e $m < n$ tais que $\hat{\Gamma}' \parallel \emptyset \parallel \emptyset \Longrightarrow_{\mathcal{J}_{XORh}}^m \Gamma' \parallel \Delta' \parallel \Lambda'$. Então $\sigma_{\Lambda'}$ é uma substituição idempotente.

Caso base: Quando $n = 0$ temos que $\Gamma \parallel \Delta \parallel \Lambda$ é um estado inicial e portanto $\Lambda = \emptyset$, logo $\sigma_{\Lambda} = \emptyset$ que é a substituição identidade, logo idempotente.

Suponha agora que $n > 1$, portanto existe $\Gamma' \parallel \Delta' \parallel \Lambda'$ tal que

$$\hat{\Gamma} \parallel \emptyset \parallel \emptyset \Longrightarrow_{\mathcal{J}_{XORh}}^{n-1} \Gamma' \parallel \Delta' \parallel \Lambda' \Longrightarrow_{\mathcal{J}_{XORh}} \Gamma \parallel \Delta \parallel \Lambda$$

Como $n - 1 < n$ e pela hipótese de indução temos que $\Gamma' \parallel \Delta' \parallel \Lambda'$ é um estado válido de \mathcal{J}_{XORh} onde $\sigma_{\Lambda'}$ é idempotente e pelo Lema 3.19 σ_{Λ} é idempotente.

□

Teorema 3.4 (Correção de \mathcal{J}_{XORh}). *Sejam $\tilde{\Gamma}$ um problema de ACUNh-unificação em sua forma padronizada, $\Gamma := Purif(\tilde{\Gamma})$ e $L := \mathcal{J}_{XORh}(\Gamma||\emptyset||\emptyset)$. Então para cada $\sigma \in L$ temos que σ é um ACUNh-unificador idempotente de $\tilde{\Gamma}$.*

Demonstração. Seja $\sigma \in L$, então pela definição do algoritmo \mathcal{J}_{XORh} existe $\emptyset||\Delta||\Lambda$ um estado válido de \mathcal{J}_{XORh} tal que $\sigma = \sigma_\Lambda$ e $\Gamma||\emptyset||\emptyset \xRightarrow{*}_{\mathcal{J}_{XORh}} \emptyset||\Delta||\Lambda$.

Pelo Lema 3.20, σ é idempotente, logo para cada $x = S \in \Lambda$ temos

$$x\sigma = x\sigma\sigma = x\sigma_\Lambda\sigma =_{\oplus_h} S\sigma$$

Implicando que $\sigma \models \emptyset||\Lambda$ e pelo Lema 3.18 temos que $\sigma \models \Gamma||\emptyset$, isto é, para cada $T \in \Gamma$, tem-se que $T\sigma =_{\oplus_h} 0$ e portanto σ é um ACUNh-unificador de Γ . Pelo Teorema 3.2 temos que Γ é uma extensão conservativa de $\tilde{\Gamma}$ e como σ é um ACUNh-unificador idempotente de Γ então σ é um ACUNh-unificador idempotente de $\tilde{\Gamma}$. \square

3.2.3 Completude de \mathcal{J}_{XORh}

Nesta seção mostraremos que \mathcal{J}_{XORh} produz um *conjunto completo* de ACUNh-unificadores de um dado problema Γ em sua forma purificada. Para isso mostraremos que os ACUNh-unificadores de Γ são soluções dos estados finais gerados pelo algoritmo \mathcal{J}_{XORh} obtidos a partir do estado inicial $\Gamma||\emptyset||\emptyset$. Para isso utilizaremos a Definição 3.13 de extensão dirigida.

Lema 3.21. *Se $\Gamma||\Delta||\Lambda \xRightarrow{Triv} \Gamma'||\Delta'||\Lambda'$ então $\Gamma'||\Delta'||\Lambda'$ é uma extensão dirigida de $\Gamma||\Delta||\Lambda$.*

Demonstração. Como $\Gamma||\Delta||\Lambda \xRightarrow{Triv} \Gamma'||\Delta'||\Lambda'$, segue que $\Gamma = \tilde{\Gamma} \cup \{0\}$, $\Gamma' = \tilde{\Gamma}$, $\Delta' = \Delta$ e $\Lambda' = \Lambda$.

Seja uma substituição σ tal que $\sigma \models \Gamma||\Delta||\Lambda$, isto é, são validos:

- Para cada $T \in \Gamma \supset \Gamma'$, tem-se que $T\sigma =_{\oplus_h} 0$.
- Para cada $s \neq t \in \Delta = \Delta'$, tem-se que $s\sigma \neq_{\oplus_h} t\sigma$.
- Para cada $x = S \in \Lambda = \Lambda'$ tem-se que $x\sigma =_{\oplus_h} S\sigma$

Portanto $\sigma \models \Gamma'||\Delta'||\Lambda'$.

Tomando $\gamma = id$, a substituição identidade, temos que $Dom(\gamma) = \emptyset \subseteq Var(\Gamma', \Lambda') \setminus Var(\Gamma, \Lambda)$ e $\sigma\gamma = \sigma$ portanto $\sigma\gamma \models \Gamma'||\Delta'||\Lambda'$, equivalentemente, $\Gamma'||\Delta'||\Lambda'$ é uma extensão dirigida de $\Gamma||\Delta||\Lambda$. \square

Lema 3.22. Se $\Gamma \parallel \Delta \parallel \Lambda \implies_{Simp} \Gamma' \parallel \Delta' \parallel \Lambda'$ então $\Gamma' \parallel \Delta' \parallel \Lambda'$ é uma extensão dirigida de $\Gamma \parallel \Delta \parallel \Lambda$.

Demonstração. Como $\Gamma \parallel \Delta \parallel \Lambda \implies_{Simp} \Gamma' \parallel \Delta' \parallel \Lambda'$ então $\Gamma' \parallel \Delta' \parallel \Lambda'$, segue que, $\Gamma = \tilde{\Gamma} \cup \{x \oplus S\}$, $\gamma = \{x \mapsto S\}$, $\Gamma' = Purif(\Gamma\gamma \downarrow)$, $\Delta' = \Delta\gamma \downarrow$ e $\Lambda' = \Lambda\gamma \downarrow \cup \{x = S\}$.

Seja ϕ uma substituição tal que $\phi \models \Gamma \parallel \Delta \parallel \Lambda$. Como $x \oplus S \in \Gamma$ então temos que $(x \oplus S)\phi =_{\oplus_h} 0$, equivalentemente, $x\phi =_{\oplus_h} S\phi = x\gamma\phi$.

Tome uma variável $y \neq x$ temos que $y\gamma = y$ e portanto $y\gamma\phi = y\phi =_{\oplus_h} y\phi$, isto é, $\gamma\phi =_{\oplus_h} \phi$.

Tome $T \in \Gamma$ um termo qualquer, por hipótese $T\phi =_{\oplus_h} 0$.

Pelo Teorema 2.1 obtemos as seguintes igualdades:

$$(T\gamma \downarrow)\phi =_{\oplus_h} (T\gamma \downarrow)\phi \downarrow = T\gamma\phi \downarrow =_{\oplus_h} T\gamma\phi \quad (3.8)$$

Logo para cada $T \in \tilde{\Gamma}$, $(T\gamma \downarrow)\phi =_{\oplus_h} 0$, isto é, ϕ é um ACUNh-unificador de $\tilde{\Gamma}\gamma \downarrow$.

Como $\Gamma' = Purif(\tilde{\Gamma}\sigma \downarrow)$ segue do Teorema 3.2, que Γ' é uma extensão conservativa de $\tilde{\Gamma}\gamma \downarrow$ então existe uma substituição σ tal que $\phi\sigma$ é um ACUNh-unificador de Γ' e $Dom(\sigma) \subseteq \mathcal{V}ar(\Gamma') \setminus \mathcal{V}ar(\Gamma)$, isto é, $Dom(\sigma)$ contém apenas variáveis novas, e portanto podemos supor sem perda de generalidade que as variáveis não ocorrem em $\mathcal{V}ar(\Gamma) \cup \mathcal{V}ar(\Lambda) \cup \mathcal{V}ar(\mathcal{I}m(\phi)) \cup \mathcal{V}ar(\Delta)$ (\star).

1. Como $\phi\sigma$ é um ACUNh-unificador de Γ' , temos que para cada $T' \in \Gamma'$, $T'\phi\sigma =_{\oplus_h} 0$.
2. Tome $y = T' \in \Lambda'$ qualquer então, $y = T \in \Lambda$ onde $T' = T\gamma \downarrow$. Observe que $\phi \models \Gamma \parallel \Delta \parallel \Lambda$, implica em $y\phi =_{\oplus_h} T\phi$. Pela equação 3.8 temos: $y\phi\sigma =_{\oplus_h} T\phi\sigma =_{\oplus_h} T\gamma\phi\sigma =_{\oplus_h} (T\gamma \downarrow)\phi\sigma = T'\phi\sigma$.
3. Tome $s \neq t \in \Delta$, então $s\phi \neq_{\oplus_h} t\phi$.

Por (\star) temos $Dom(\gamma) \cap (\mathcal{V}ar(\Delta) \cup \mathcal{V}ar(\mathcal{I}m(\phi))) = \emptyset$, daí, $s\phi\sigma = s\phi$ e $t\phi\sigma = t\phi$, portanto $s\phi\sigma \neq_{\oplus_h} t\phi\sigma$. Utilizando a equação 3.8, obtemos $(s\gamma \downarrow)\phi\sigma =_{\oplus_h} s\phi\sigma$ e $(t\sigma \downarrow)\phi\sigma =_{\oplus_h} t\phi\sigma$.

Então $(s\sigma \downarrow)\phi\gamma \neq_{\oplus_h} (t\sigma \downarrow)\phi\gamma$, concluindo que para cada $s' \neq t' \in \Delta' = \Delta\sigma \downarrow$, tem-se que $s'\phi\gamma \neq_{\oplus_h} t'\phi\gamma$.

Por (1), (2) e (3) temos $\phi\gamma \models \Gamma' \parallel \Delta' \parallel \Lambda'$ e por (\star) temos $Dom(\gamma) \cap \mathcal{V}ar(\Lambda) = \emptyset$ então,

$$\begin{aligned} Dom(\gamma) &\subseteq \mathcal{V}ar(\Gamma') \setminus (\mathcal{V}ar(\Gamma) \cup \mathcal{V}ar(\Lambda)) \\ &\subseteq (\mathcal{V}ar(\Gamma') \cup \mathcal{V}ar(\Lambda')) \setminus (\mathcal{V}ar(\Gamma) \cup \mathcal{V}ar(\Lambda)) \subseteq \mathcal{V}ar(\Gamma', \Lambda') \setminus \mathcal{V}ar(\Gamma, \Lambda) \end{aligned}$$

Concluindo assim, que $\Gamma' \parallel \Delta' \parallel \Lambda'$ é um extensão dirigida de $\Gamma \parallel \Delta \parallel \Lambda$. □

Lema 3.23. Se $\Gamma \parallel \Delta \parallel \Lambda \implies_{N\text{-dec}} \Gamma \parallel \Delta' \parallel \Lambda' \vee \Gamma \parallel \Delta'' \parallel \Lambda$ e $\phi \models \Gamma \parallel \Delta \parallel \Lambda$ então $\phi \models \Gamma' \parallel \Delta' \parallel \Lambda'$ ou $\phi \models \Gamma \parallel \Delta'' \parallel \Lambda$

Demonstração. Por hipótese, $\Gamma = \tilde{\Gamma} \cup \{s \oplus t \oplus T\}$, $\Gamma' = \tilde{\Gamma}\sigma \downarrow \cup \{T\sigma \downarrow\}$, $\Delta' = \Delta\sigma \downarrow$, $\Lambda' = \Lambda\sigma \downarrow \cup [\sigma]$ e $\Delta'' = \Delta \dot{\cup} \{s \neq t\}$ com σ um mgu idempotente de $s =^? t$, via unificação sintática, tal que $\text{Dom}(\sigma), \text{Var}(\text{Im}(\sigma)) \subseteq \text{Var}(s) \cup \text{Var}(t) \subseteq \text{Var}(\Gamma)$ onde .

Suponha que $\phi \not\models \Gamma \parallel \Delta'' \parallel \Lambda$. É suficiente mostrar que $\phi \models \Gamma' \parallel \Delta' \parallel \Lambda'$.

Como $\Delta'' = \Delta \cup \{s \neq t\}$ então por $\phi \not\models \Gamma \parallel \Delta'' \parallel \Lambda$ e $\phi \models \Gamma \parallel \Delta \parallel \Lambda$ temos $s\phi =_{\oplus_h} t\phi$, porém s, t são termos puros não encabeçados por h , portanto se aparece algum símbolo de função \oplus ou h em $s\phi$ ou $t\phi$, este foi introduzido por ϕ . Por σ ser um mgu de $s =^? t$ existe uma substituição γ tal que $\sigma\gamma =_{\oplus_h} \phi$.

Como σ é idempotente, temos que

$$\sigma\phi =_{\oplus_h} \sigma\sigma\gamma = \sigma\gamma =_{\oplus_h} \phi \quad (3.9)$$

1. Seja $S' \in \Gamma' = \tilde{\Gamma}\sigma \downarrow \cup \{T\sigma \downarrow\}$:

- $S' = T\sigma \downarrow$: Defina $u := s\sigma = t\sigma$.

Por hipótese $(s \oplus t \oplus T)\phi =_{\oplus_h} 0$. Logo, pela Equação 3.9, $\sigma\phi =_{\oplus_h} \phi$, temos:

$$\begin{aligned} 0 =_{\oplus_h} (s \oplus t \oplus T)\phi &= (s \oplus t \oplus T)\sigma\phi \\ &= (s\sigma\phi \oplus t\sigma\phi \oplus T\sigma\phi = u\phi \oplus u\phi \oplus T\sigma\phi =_{\oplus_h} T\sigma\phi =_{\oplus_h} T\phi \end{aligned}$$

Em particular pelo teorema 2.1 para qualquer termo S tem-se que

$$(S\sigma \downarrow)\phi =_{\oplus_h} (S\sigma \downarrow)\phi \downarrow = S\sigma\phi \downarrow =_{\oplus_h} S\sigma\phi =_{\oplus_h} S\phi$$

Portanto $S'\phi = (T\sigma \downarrow)\phi =_{\oplus_h} T\phi =_{\oplus_h} 0$

- $S' \in \tilde{\Gamma}\sigma \downarrow$: Então existe $T \in \Gamma$ tal que $S' = T\sigma \downarrow$ e por hipótese $T\phi =_{\oplus_h} 0$, e portanto $S'\phi = (T\sigma \downarrow)\phi =_{\oplus_h} 0$

2. Tome $u' \neq v' \in \Delta' = \Delta\sigma \downarrow$ então existe $u \neq v \in \Delta$ tal que $u' = u\sigma \downarrow$ e $v' = v\sigma \downarrow$. Assim,

$$u'\phi = (u\sigma \downarrow)\phi =_{\oplus_h} u\phi \neq_{\oplus_h} v\phi =_{\oplus_h} (v\sigma \downarrow)\phi = v'\phi$$

e portanto $u'\phi \neq_{\oplus_h} v'\phi$.

3. Tome $x = S' \in \Lambda' = \Lambda\sigma \downarrow \cup [\sigma]$. Temos dois possíveis casos:

- se $x = S' \in \Lambda\sigma \downarrow$ então existe $x = S \in \Lambda$ tal que $S' = S\sigma \downarrow$. Por hipótese, temos que $x\phi =_{\oplus_h} S\phi =_{\oplus_h} (S\sigma \downarrow)\phi = S'\phi$.

Em ambos os casos concluímos que $x\phi =_{\oplus_h} S'\phi$

□

Para provarmos o análogo aos Lemas 3.21 e 3.22 para a regra de *nulificação* precisaremos definir a noção de *camadas* de um termo t em sua forma normal, que é a profundidade do termo ignorando o símbolo de função \oplus .

Definição 3.17 (Camadas). *Seja t um termo em sua forma normal então definimos $cmd(t)$ de forma indutiva como se segue:*

1. $cmd(t) = 0$ se, e somente se, t é uma constante ou variável.
2. $cmd(f(t_1, \dots, t_n)) = 1 + \max\{cmd(t_1), \dots, cmd(t_n)\}$ se, e somente se, f é um símbolo de função não interpretado e não constante.
3. $cmd(t_1 \oplus \dots \oplus t_n) = \max\{cmd(t_1), \dots, cmd(t_n)\}$
4. $cmd(h(t)) = 1 + \max\{cmd(t)\}$

Observação 3.6. *Seja t um termo qualquer, iremos abusar da notação e definiremos que o $cmd(t) := cmd(t \downarrow)$.*

Lema 3.24. *Se $\Gamma \parallel \Delta \parallel \Lambda \implies_{Nul} \Gamma' \parallel \Delta' \parallel \Lambda'$ então $\Gamma' \parallel \Delta' \parallel \Lambda'$ é uma extensão dirigida de $\Gamma \parallel \Delta \parallel \Lambda$.*

Demonstração. Por hipótese Temos que $\Gamma = \tilde{\Gamma} \cup \{S \oplus h(t)\}$, $\Gamma' = \tilde{\Gamma} \cup \{S, t\}$, $\Delta' = \Delta$ e $\Lambda' = \Lambda$, todas as variáveis de $\mathcal{V}ar(\Gamma) = \{x_1, \dots, x_n\}$ são variáveis presas e todo termo $S_i \in \Gamma = \{S_1, S_2, \dots, S_r\}$, tem-se que

$$S_i = \begin{cases} x_{i1} \oplus \dots \oplus x_{ik_i} & \text{ou} \\ x_{i1} \oplus \dots \oplus x_{ik_i} \oplus h(t_i) & \text{ou} \\ h(t_i) \end{cases}$$

Onde $x_{i1}, \dots, x_{ik_i} \in \mathcal{Var}(\Gamma) = \{x_1, \dots, x_n\}$, t_i um termo onde $\text{raíz}(t_i) \neq h$ e $k_i \geq 1$.

Afirmção: Se φ é uma substituição normalizada e básica, tal que $\varphi \models \Gamma \parallel \Delta \parallel \Lambda$ então para todo $j \in \{1, \dots, r\}$ onde $S_j = x_{j1} \oplus \dots \oplus x_{jk_j} \oplus h(t_j) \in \Gamma$ tem-se que $h(t_j\varphi) =_{\oplus_h} 0$.

Seja φ como na hipótese, então, $\varphi = \{x_1 \mapsto T_1, \dots, x_n \mapsto T_n, y_1 \mapsto S_1, \dots, y_m \mapsto S_m\}$. Podemos supor sem perda de generalidade que $\text{cmd}(T_1) \geq \dots \geq \text{cmd}(T_n)$.

Suponha por absurdo que exista algum $j \in \{1, \dots, r\}$ tal que $S_j = x_{j1} \oplus \dots \oplus x_{jk_j} \oplus h(t_j)$ e ao aplicar φ em t_j obtemos $h(t_j\varphi) \neq_{\oplus_h} 0$.

Afirmção: $\text{cmd}(T_1) > 0$. Suponha por absurdo que $\text{cmd}(T_1) = 0$ e então para cada $i \in \{1, \dots, n\}$ tem-se que $\text{cmd}(T_i) = 0$ e portanto cada T_i é um símbolo de função constante.

Seja $S_j =_{AC} x_{j1} \oplus \dots \oplus x_{jk_j} \oplus h(t_j) \in \Gamma$. Por hipótese $S_j\varphi =_{\oplus_h}$, isto é, $x_{j1}\varphi \oplus \dots \oplus x_{jk_j}\varphi \oplus h(t_j\varphi) =_{\oplus_h} 0$.

Pela definição de φ , temos $x_{ji}\varphi = T_{ji}$, segue que, $T_{j1} \oplus \dots \oplus T_{jk_j} \oplus h(t_j\varphi) =_{\oplus_h} 0$

Logo $h(t_j\varphi) =_{\oplus_h} 0$, pois não se anula com nenhum símbolo constante T_{ji} , que é uma contradição, pois supomos $h(t_j\varphi) \neq_{\oplus_h} 0$, portanto $\text{cmd}(T_1) > 0$.

Como x_1 é uma variável presa de Γ , existe um $i \in \{1, \dots, r\}$ tal que $S_i = x_{i1} \oplus \dots \oplus x_{ik_i} \oplus h(t_i) \in \Gamma$ com $x_1 \in \mathcal{Var}(t_i)$, então, $1 \leq \text{cmd}(T_1) = \text{cmd}(x_1\varphi) \leq \text{cmd}(t_i\varphi) < \text{cmd}(h(t_i\varphi))$.

Isto é, $\text{cmd}(h(t_i\varphi)) > 1$ então $h(t_i\varphi)$ não é uma variável nem uma constante, em particular, $h(t_i\varphi) \neq_{\oplus_h} 0$.

Por outro lado, pela hipótese, $S_i\varphi = \emptyset$, segue que, $x_{i1}\varphi \oplus \dots \oplus x_{ik_i}\varphi \oplus h(t_i\varphi) =_{\oplus_h} 0$.

Então existe um k tal que $x_{ik}\varphi = T_{ik} =_{\oplus_h} h(t_i\varphi) \oplus T'_{ik}$ pois $h(t_i\varphi) \neq_{\oplus_h} 0$. Calculando então $\text{cmd}()$ de cada parte, obtemos:

$$\text{cmd}(T_{ik}) = \text{máx}\{\text{cmd}(h(t_i\varphi)), \text{cmd}(T'_{ik})\} \geq \text{cmd}(h(t_i\varphi)) > \text{cmd}(T_1)$$

Que é uma contradição pois $\text{cmd}(T_1) \geq \text{cmd}(T_{ik})$, e portanto não existe um $j \in \{1, \dots, r\}$ tal que $h(t_j\varphi) \neq_{\oplus_h} 0$.

Note que $\phi \models \Gamma \parallel \Delta \parallel \Lambda$, então existe substituição básica α onde leva apenas em termos puros básicos não nulos com $\text{Dom}(\alpha) = \mathcal{Var}(\text{Im}(\phi))$ tal que $\phi\alpha \models \Gamma \parallel \Delta \parallel \Lambda$, basta instanciar de uma forma que para

cada variável $x \in Dom(\alpha)$ tem-se que $x\alpha = a_x$ seja um símbolo de função constante não nulo distinto para cada variável distinta. E portanto pela afirmação anterior que para cada $j \in \{1, \dots, r\}$, tal que $S_j = x_{j1} \oplus \dots \oplus x_{jk_j} \oplus h(t_j)$ tem-se que $h(t_j\phi\alpha) =_{\oplus_h} 0$, então $t_j\phi\alpha =_{\oplus} 0$, portanto $t_j\phi =_{\oplus_h} 0$ pois cada variável $w \in \mathcal{V}ar(\mathcal{I}m(\phi))$ $w\alpha$ vai em um símbolo de função constante e não nula.

Como $S \oplus h(t) \in \Gamma$ temos que $S\phi \oplus h(t\phi) =_{\oplus_h} 0$ e $h(t\phi) =_{\oplus_h} 0$, logo $S\phi =_{\oplus_h} 0$ e $t\phi =_{\oplus_h} 0$, isto é, para cada $S' \in \Gamma' = \tilde{\Gamma} \cup \{S, t\}$ tem-se que $S'\phi =_{\oplus_h} 0$ e com isso concluímos que $\phi \models \Gamma' \parallel \Delta \parallel \Lambda$ e portanto, $\phi \models \Gamma' \parallel \Delta' \parallel \Lambda'$. \square

Neste lema abaixo provaremos que os únicos estados finais de \mathcal{J}_{XORh} que possuem solução são os estados de solução, e juntamente com os lemas anteriores, provaremos que dado ϕ solução do estado inicial $\Gamma \parallel \emptyset \parallel \emptyset$ existe um γ tal que $\phi\gamma$ é uma solução de algum estado de solução obtido de $\Gamma \parallel \emptyset \parallel \emptyset$.

Lema 3.25. *Seja $\Gamma \parallel \Delta \parallel \Lambda$ um estado final de \mathcal{J}_{XORh} , se $\Gamma \neq \emptyset$ então não existe uma substituição ϕ tal que $\phi \models \Gamma \parallel \Delta \parallel \Lambda$.*

Demonstração. Como $\Gamma \parallel \Delta \parallel \Lambda$ é um estado final de \mathcal{J}_{XORh} então não é possível aplicar mais nenhuma regra de inferência então obtemos:

1. $0 \notin \Gamma$, pois caso contrário, seria possível aplicar *Trivial*.
2. Para toda variável $x \in \Gamma$ temos que x é uma variável presa de Γ , pois caso contrário, seria possível aplicar a regra *simplificação*
3. se $s \oplus t \oplus T \in \Gamma$ onde s, t são termos puros com $raíz(s) = raíz(t) \neq h$ então $s \neq t \in \Delta$, pois caso contrário, seria possível aplicar a regra *N-Decomposição*.
4. Existem termos S, t tais que t é um termo puro não variável com $raíz(t) \neq h$ e $t \oplus S \in \Gamma$, pois casos contrário, seria possível aplicar a regra *nulificação*.

Suponha por absurdo que exista uma substituição normalizada e básica ϕ tal que $\phi \models \Gamma \parallel \Delta \parallel \Lambda$, usaremos o mesmo raciocínio da demonstração do o Lema 3.24. Podemos supor sem perda de generalidade que,

$$\phi = \{x_1 \mapsto T_1, \dots, x_n \mapsto T_n, y_1 \mapsto S_1, \dots, y_m \mapsto S_m\}$$

onde $\mathcal{V}ar(\Gamma) = \{x_1, \dots, x_n\}$ e $cmd(T_1) \geq cmd(T_2) \geq \dots \geq cmd(T_n)$

Afirmação: $cmd(T_1) > 0$. Suponha que $cmd(T_1) = 0$ e portanto para cada $i \in \{1, \dots, n\}$ temos que $cmd(T_i) = 0$, portanto cada $i \in \{1, \dots, n\}$. T_i é uma constante.

Seja t um termo com as seguintes propriedades:

- a) t é um termo puro não variável,
- b) $raíz(t) \notin \{h\}$,
- c) Existe um termo S tal que $t \oplus S \in \Gamma$, e
- d) Se existe um termo t' com as propriedades (a), (b) e (c), então $cmd(t) \geq cmd(t')$.

Existe tal termo t pelo item (4) e sem perda de generalidade $t \oplus S =_{AC} x_{i_1} \oplus \dots \oplus x_{i_l} \oplus t \oplus T$, onde T não ocorre variáveis como argumento de soma. Por hipótese, temos as seguintes igualdades:

$$0 =_{\oplus_h} (t \oplus S)\phi =_{\oplus_h} (x_{i_1} \oplus \dots \oplus x_{i_l} \oplus t \oplus T)\phi =_{\oplus_h} x_{i_1}\phi \oplus \dots \oplus x_{i_l}\phi \oplus t\phi \oplus T\phi$$

Temos dois possíveis casos, t é uma constante ou t não é constante e $raíz(t) = f \neq h$.

- t é uma constante:

Como S é um termo em sua forma normal então $t \neq 0$, segue que t é uma constante não nula, em particular, $cmd(t) = 0$. Então existe alguma variável x_{i_k} onde $x_{i_k}\phi = t \oplus s$ para algum termo s .

Por hipótese, x_{i_k} é uma variável presa de Γ então existem termos $S' \in \Gamma$ e t' um termo puro e não variável tal que t' é um subtermo de S' com $x_{i_k} \in \mathcal{V}ar(t')$, portanto t' não é uma constante nem variável, implicando que $cmd(t') > 0 = cmd(t)$. Temos dois possíveis subcasos:

- $raíz(t') \neq h$ e $S' =_{AC} t' \oplus S''$:

Então t' é um termo com as propriedades (a), (b) e (c), implicando que $cmd(t) \geq cmd(t')$, que é uma contradição.

- $S' =_{AC} h(t'') \oplus S''$ e t' é um subtermo de $h(t'')$:

Como t' é um subtermo de $h(t'')$ onde $S'' \oplus h(t'') \in \Gamma$ implicando que $h(t'')\phi \neq_{\oplus_h} 0$ e $(S'' \oplus h(t''))\phi =_{\oplus_h} 0$ e portanto tem que existir alguma variável $x_i \in \mathcal{V}ar(\widehat{S})$ tal que $x_i\phi =_{AC} h(\widehat{t}\phi) \oplus T''$ que é uma contradição pois $x_i\phi = T_i$ uma constante.

- $t = f(t_1, \dots, t_r)$: E portanto nenhuma variável x_{i_k} de S unifica com t pois t não é uma constante, implicando que existe algum termo $t' = f(s_1, \dots, s_r)$ em T que unifica com t porém pelo item (3) $t \neq t' \in \Delta$ e portanto $t\phi \neq_{\oplus_h} t'\phi$, que é uma contradição.

Como em ambos os casos encontramos contradições então podemos concluir que de fato $cmd(T_1) > 0$, provando a afirmação.

Observe que x_1 é uma variável solta de Γ e portanto existem \widehat{S}, t tais que $t \oplus \widehat{S} \in \Gamma$, t é um termo puro e não é variável e $x \in \mathcal{Var}(t)$. Existem dois possíveis casos, $raíz(t) = h$ ou $raíz(t) \neq h$:

- $raíz(t) \neq h$:

Então $t = f(t_1, \dots, t_r)$ e sem perda de generalidade podemos supor $\widehat{S} \oplus t =_{AC} x_{i_1} \oplus \dots \oplus x_{i_l} \oplus t \oplus T$.

Por hipótese temos $\phi \models \Gamma \parallel \Delta \parallel \Lambda$ então $(\widehat{S} \oplus t)\phi =_{\oplus_h} 0$, isto é, $x_{i_1}\phi \oplus \dots \oplus x_{i_l}\phi \oplus t\phi \oplus T\phi =_{\oplus_h} 0$.

Também por hipótese não é possível aplicar nenhuma regra de inferência, portanto não existe um termo $t' = f(s_1, \dots, s_r)$ em T tal que t' unifica com t , pelo mesmo argumento que usamos na afirmação, e por conseguinte deve existir alguma variável x_{i_k} tal que $x_{i_k}\phi =_{\oplus_h} t\phi \oplus T'$, implicando que $cmd(x_{i_k}\phi) = \max\{cmd(t\phi), cmd(T')\}$, e portanto $cmd(T_{i_k}) = cmd(x_{i_k}\phi) \geq cmd(t\phi)$.

Por outro lado, $x_1 \in \mathcal{Var}(t)$ e portanto $T_1 = x_1\phi$ é um subtermo de $t\phi = f(t_1\phi, \dots, t_r\phi)$, logo obtemos que $cmd(T_1) < cmd(t\phi) \leq cmd(T_{i_k})$, que é uma contradição.

- $t = h(t_i)$:

Dessa forma x_1 é uma variável ocorrendo em t_i e portanto $0 < cmd(T_1) = cmd(x_1\phi) \leq cmd(t_i\phi)$ e portanto t_i não é uma constante nem variável nem soma de constantes e variáveis, em particular $t_i\phi \neq_{\oplus_h} 0$, implicando que $h(t_i\phi) \neq_{\oplus_h} 0$.

Porém $(\widehat{S} \oplus h(t_i)) =_{\oplus_h} 0$, e como todos os termos de Γ estão em suas formas puras, temos que ocorre apenas um símbolo de função h , assim deve existir um x_{i_k} em \widehat{S} tal que $x_{i_k}\phi =_{\oplus_h} h(t_i\phi) \oplus T'$ e assim de forma análoga ao item anterior obtemos uma contradição.

E como em ambos os casos obtemos uma contradição temos que não existe ϕ substituição normalizada e básica tal que $\phi \models \Gamma \parallel \Delta \parallel \Lambda$, e portanto pelo mesmo argumento do Lema 3.24, não existe uma substituição ϕ tal que $\phi \models \Gamma \parallel \Delta \parallel \Lambda$. □

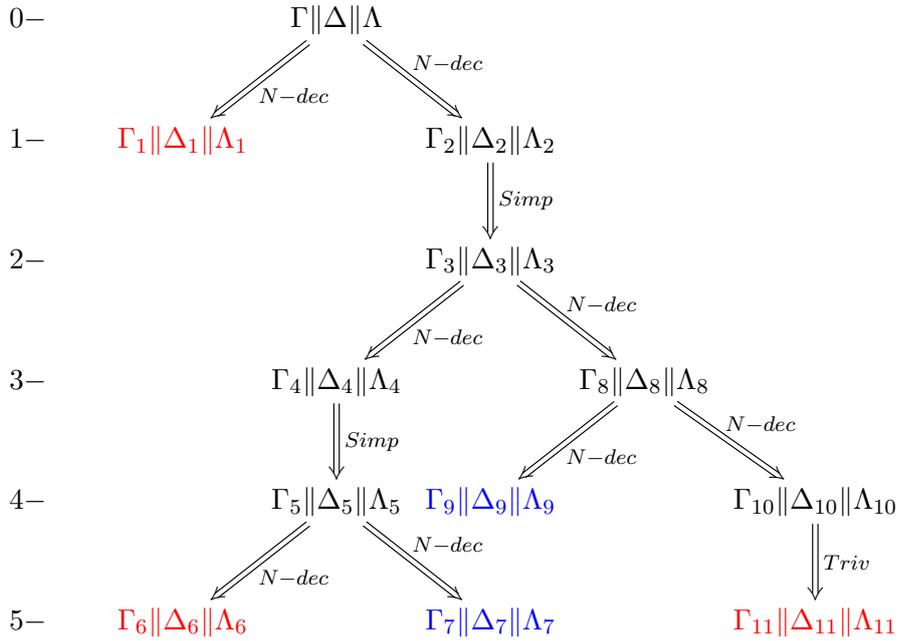
Para demonstração do Lema 3.26, utilizaremos a seguinte definição:

Definição 3.18. *Seja $\Gamma \parallel \Delta \parallel \Lambda$ um estado válido de \mathcal{J}_{XORh} , e a árvore de execução de \mathcal{J}_{XORh} , como no exemplo 3.6 na página 84, a partir do estado $\Gamma \parallel \Delta \parallel \Lambda$, então definimos:*

- Se $\Gamma \parallel \Delta \parallel \Lambda$ for um estado final, então: $\Gamma \parallel \Delta \parallel \Lambda \Longrightarrow_{\mathcal{J}_{XORh}}^{\leq 1} \Gamma \parallel \Delta \parallel \Lambda$.
- Se $\Gamma \parallel \Delta \parallel \Lambda \Longrightarrow_{\mathcal{J}_{XORh}} \bigvee_{i \in I} \Gamma_i \parallel \Delta_i \parallel \Lambda_i$, então: $\Gamma \parallel \Delta \parallel \Lambda \Longrightarrow_{\mathcal{J}_{XORh}}^{\leq 1} \bigvee_{i \in I} \Gamma_i \parallel \Delta_i \parallel \Lambda_i$.
- Se $\Gamma \parallel \Delta \parallel \Lambda \Longrightarrow_{\mathcal{J}_{XORh}}^{\leq m} \bigvee_{i \in I} \Gamma_i \parallel \Delta_i \parallel \Lambda_i$, e
 - Para cada $i \in I$ temos $\Gamma_i \parallel \Delta_i \parallel \Lambda_i \Longrightarrow_{\mathcal{J}_{XORh}}^{\leq 1} \bigvee_{k \in J_i} \Gamma_{k_i} \parallel \Delta_{k_i} \parallel \Lambda_{k_i}$
 - e o conjunto $\{\Gamma_j \parallel \Delta_j \parallel \Lambda_j\}_{j \in J} := \{\bigvee_{k \in J_i} \Gamma_{k_i} \parallel \Delta_{k_i} \parallel \Lambda_{k_i} \mid i \in I\}$

Então $\Gamma \parallel \Delta \parallel \Lambda \Longrightarrow_{\mathcal{J}_{XORh}}^{\leq m+1} \bigvee_{j \in J} \Gamma_j \parallel \Delta_j \parallel \Lambda_j$

Exemplo 3.7. *Seja Γ um estado válido de \mathcal{J}_{XORh} , suponha que obtemos a seguinte árvore de execução de \mathcal{J}_{XORh} a partir de $\Gamma \parallel \Delta \parallel \Lambda$:*



$\Gamma \parallel \Delta \parallel \Lambda \Longrightarrow_{\mathcal{J}_{XORh}}^{\leq m} \bigvee_{i \in I} \Gamma_i \parallel \Delta_i \parallel \Lambda_i$ quer dizer que, $\bigvee_{i \in I} \Gamma_i \parallel \Delta_i \parallel \Lambda_i$ são todos os encontrados na profun-

didade m da árvore e todos os estados finais obtidos em qualquer profundidade menor que m . Então,

$$\begin{aligned}\Gamma \parallel \Delta \parallel \Lambda &\Longrightarrow_{\mathcal{J}_{XORh}}^{\leq 3} \Gamma_1 \parallel \Delta_1 \parallel \Lambda_1 \vee \Gamma_4 \parallel \Delta_4 \parallel \Lambda_4 \vee \Gamma_8 \parallel \Delta_8 \parallel \Lambda_8 \\ \Gamma_1 \parallel \Delta_1 \parallel \Lambda_1 &\Longrightarrow_{\mathcal{J}_{XORh}}^{\leq 1} \Gamma_1 \parallel \Delta_1 \parallel \Lambda_1 \text{ e } \Gamma_4 \parallel \Delta_4 \parallel \Lambda_4 \Longrightarrow_{\mathcal{J}_{XORh}}^{\leq 1} \Gamma_5 \parallel \Delta_5 \parallel \Lambda_5 \\ \Gamma_8 \parallel \Delta_8 \parallel \Lambda_8 &\Longrightarrow_{\mathcal{J}_{XORh}}^{\leq 1} \Gamma_9 \parallel \Delta_9 \parallel \Lambda_9 \vee \Gamma_{10} \parallel \Delta_{10} \parallel \Lambda_{10}\end{aligned}$$

E também, $\Gamma \parallel \Delta \parallel \Lambda \Longrightarrow_{\mathcal{J}_{XORh}}^{\leq 4} \Gamma_1 \parallel \Delta_1 \parallel \Lambda_1 \vee \Gamma_5 \parallel \Delta_5 \parallel \Lambda_5 \vee \Gamma_9 \parallel \Delta_9 \parallel \Lambda_9 \vee \Gamma_{10} \parallel \Delta_{10} \parallel \Lambda_{10}$.

Lema 3.26. *Sejam $\Gamma \parallel \Delta \parallel \Lambda$ estado válido \mathcal{J}_{XORh} , $m \in \mathbb{N}$ e $\{\Gamma_i \parallel \Delta_i \parallel \Lambda_i\}_{i \in I}$ tais que,*

$$\Gamma \parallel \Delta \parallel \Lambda \Longrightarrow_{\mathcal{J}_{XORh}}^{\leq m} \bigvee_{i \in I} \Gamma_i \parallel \Delta_i \parallel \Lambda_i$$

Se $\phi \models \Gamma \parallel \Delta \parallel \Lambda$ então existem $i \in I$ e uma substituição γ_i tais que $\phi \gamma_i \models \Gamma_i \parallel \Delta_i \parallel \Lambda_i$ e $\text{Dom}(\gamma_i) \subseteq \text{Var}(\Gamma_i, \Lambda_i) \setminus \text{Var}(\Gamma, \Lambda)$.

Demonstração. Este lema será demonstrado por indução sobre $m \geq 1$.

Hipótese de indução: Suponha verdadeiro o teorema para algum $m \geq 1$.

Base da indução: Quando $m = 1$, temos que duas possibilidades:

- Se $\Gamma \parallel \Delta \parallel \Lambda$ for um estado final, então: $\Gamma \parallel \Delta \parallel \Lambda \Longrightarrow_{\mathcal{J}_{XORh}}^{\leq 1} \Gamma \parallel \Delta \parallel \Lambda$. Portanto o resultado do teorema é trivial, pois para cada solução σ de $\Gamma \parallel \Delta \parallel \Lambda$, podemos tomar $\gamma = \text{id}$, a substituição identidade, e portanto $\sigma \gamma = \sigma \models \Gamma \parallel \Delta \parallel \Lambda$ e $\text{Dom}(\gamma) = \emptyset = \text{Var}(\Gamma, \Lambda) \setminus \text{Var}(\Gamma, \Lambda)$
- Se $\Gamma \parallel \Delta \parallel \Lambda \Longrightarrow_{\mathcal{J}_{XORh}} \bigvee_{i \in I} \Gamma_i \parallel \Delta_i \parallel \Lambda_i$, então $\Gamma \parallel \Delta \parallel \Lambda \Longrightarrow_{\mathcal{J}_{XORh}}^{\leq 1} \bigvee_{i \in I} \Gamma_i \parallel \Delta_i \parallel \Lambda_i$.

Então pelos Lemas 3.21, 3.22, 3.23 e 3.24 o resultado segue.

Passo indutivo: Suponha $\Gamma \parallel \Delta \parallel \Lambda$ estado válido \mathcal{J}_{XORh} , $m \in \mathbb{N}$ e $\{\Gamma_i \parallel \Delta_i \parallel \Lambda_i\}_{i \in I}$ tais que,

$$\Gamma \parallel \Delta \parallel \Lambda \Longrightarrow_{\mathcal{J}_{XORh}}^{\leq m} \bigvee_{i \in I} \Gamma_i \parallel \Delta_i \parallel \Lambda_i$$

Portanto tomando o conjunto $\{\Gamma_j \parallel \Delta_j \parallel \Lambda_j\}_{j \in J}$ como na Definição 3.18, temos que para cada $i \in I$, com $\Gamma_i \parallel \Delta_i \parallel \Lambda_i \Longrightarrow_{\mathcal{J}_{XORh}}^{\leq 1} \bigvee_{k_i \in J_i} \Gamma_{k_i} \parallel \Delta_{k_i} \parallel \Lambda_{k_i}$ então $\{\Gamma_{k_i} \parallel \Delta_{k_i} \parallel \Lambda_{k_i}\}_{i \in I} \subseteq \{\Gamma_j \parallel \Delta_j \parallel \Lambda_j\}_{j \in J}$. E temos: $\Gamma \parallel \Delta \parallel \Lambda \Longrightarrow_{\mathcal{J}_{XORh}}^{\leq m+1} \bigvee_{j \in J} \Gamma_j \parallel \Delta_j \parallel \Lambda_j$.

Tome $\sigma \models \Gamma \parallel \Delta \parallel \Lambda$ então pela hipótese de indução, existem $i \in I$ e uma substituição γ_i tal que $\sigma\gamma_i \models \Gamma_i \parallel \Delta_i \parallel \Lambda_i$ e $\text{Dom}(\gamma_i) \subseteq \text{Var}(\Gamma_i, \Lambda_i) \setminus \text{Var}(\Gamma, \Lambda)$ Pelo caso base da indução, existe um $k_i \in J_i$ e um substituição γ'_i tais que $\sigma\gamma_i\gamma'_i \models \Gamma_{k_i} \parallel \Delta_{k_i} \parallel \Lambda_{k_i}$, porém $\Gamma_{k_i} \parallel \Delta_{k_i} \parallel \Lambda_{k_i} \in \{\Gamma_j \parallel \Delta_j \parallel \Lambda_j\}_{j \in J}$ e portanto existe um $j \in J$ onde $\Gamma_j \parallel \Delta_j \parallel \Lambda_j = \Gamma_{k_i} \parallel \Delta_{k_i} \parallel \Lambda_{k_i}$ e portanto o resultado segue pois $\text{Var}(\Gamma_i, \Lambda_i) \subseteq \text{Var}(\Gamma_{k_i}, \Lambda_{k_i})$, implicando que $\text{Dom}(\gamma_i\gamma'_i) \subseteq \text{Var}(\Gamma_{k_i}, \Lambda_{k_i}) \setminus \text{Var}(\Gamma, \Lambda)$.

□

Teorema 3.5 (Completeness de \mathcal{J}_{XORh}). *Seja Γ um problema de ACUNh-unificação em sua forma purificada e $L := \mathcal{J}_{XORh}(\Gamma \parallel \emptyset \parallel \emptyset)$. Se ϕ é um ACUNh-unificador de Γ então, existe uma substituição $\sigma \in L$ tal que $\sigma|_{\text{Var}(\Gamma)} \lesssim_{\oplus_h} \phi|_{\text{Var}(\Gamma)}$.*

Demonstração. Sejam Γ , ϕ e L como na hipótese, pelo Teorema 3.3 da terminação de \mathcal{J}_{XORh} existe um $n \in \mathbb{N}$ tal que se $\Gamma \parallel \emptyset \parallel \emptyset \xRightarrow{\mathcal{J}_{XORh}^m} \Gamma' \parallel \Delta' \parallel \Lambda'$ implica que $m \leq n$. Portanto tomando a família $\{\Gamma_i \parallel \Delta_i \parallel \Lambda_i\}_{i \in I}$ de estados tal que, $\Gamma \parallel \emptyset \parallel \emptyset \xRightarrow{\mathcal{J}_{XORh}^n} \bigvee_{i \in I} \Gamma_i \parallel \Delta_i \parallel \Lambda_i$.

Portanto para cada $i \in I$, $\Gamma_i \parallel \Delta_i \parallel \Lambda_i$ é um estado final de \mathcal{J}_{XORh} , e pelo Lema 3.26 temos que existem $i \in I$ e uma substituição γ tal que $\phi\gamma \models \Gamma_i \parallel \Delta_i \parallel \Lambda_i$ onde $\text{Var}(\gamma) \subseteq \text{Var}(\Gamma_i, \Lambda_i) \setminus \text{Var}(\Gamma)$, portanto o estado final $\Gamma_i \parallel \Delta_i \parallel \Lambda_i$ possui uma solução, logo pelo Lema 3.25 garantimos que $\Gamma_i = \emptyset$, implicando que $\text{Dom}(\gamma) \subseteq \text{Var}(\Lambda_i) \setminus \text{Var}(\Gamma)$.

Assim fazendo $\sigma := \sigma_{\Lambda_i} = \{x \mapsto S \mid x = S \in \Lambda_i\}$, implica que $\sigma \in L$, pois $\Gamma_i \parallel \Delta_i \parallel \Lambda_i$ é um estado final e $\Gamma_i = \emptyset$, note que as variáveis que ocorrem no $\text{Dom}(\gamma)$ são apenas variáveis novas inseridas pelo algoritmo e portanto podemos tomar todas de tal forma que $\text{Dom}(\gamma) \cap \text{Var}(\text{Im}(\phi)) = \emptyset$.

Note que $\phi\gamma \models \emptyset \parallel \Delta_i \parallel \Lambda_i$ e portanto para cada $x = S \in \Lambda_i$, temos que $x\phi\gamma =_{\oplus_h} S\phi\gamma$ e $x\sigma = S$ então $x\phi\gamma =_{\oplus_h} x\sigma\phi\gamma$, para cada $x \in \text{Dom}(\sigma)$, e se $x \notin \text{Dom}(\sigma)$ temos que $x\sigma = x$ implica que $x\sigma\phi\gamma = x\phi\gamma$ e portanto $x\phi\gamma =_{\oplus_h} x\sigma\phi\gamma$ para toda variável x , em particular para as variáveis $x \in \text{Var}(\Gamma)$ então podemos concluir que $\phi\gamma|_{\text{Var}(\Gamma)} =_{\oplus_h} \sigma\phi\gamma|_{\text{Var}(\Gamma)}$.

E observando que dado $x \in \text{Var}(\Gamma)$ então $x \notin \text{Var}(\Lambda_i) \setminus \text{Var}(\Gamma) = \text{Dom}(\gamma)$ e portanto $x\gamma = x$, por outro lado se $x \in \text{Var}(\Gamma) \cap \text{Dom}(\phi)$ então $x\phi\gamma = x\phi$, pois $\text{Dom}(\gamma) \cap \text{Var}(\text{Im}(\phi)) = \emptyset$, então $\phi|_{\text{Var}(\Gamma)} = \phi\gamma|_{\text{Var}(\Gamma)}$.

Logo provamos que $\phi|_{\text{Var}(\Gamma)} =_{\oplus_h} \sigma\phi\gamma|_{\text{Var}(\Gamma)}$, e portanto obtemos que existe $\sigma \in L$ tal que: $\sigma|_{\text{Var}(\Gamma)} \lesssim_{\oplus_h} \phi|_{\text{Var}(\Gamma)}$.

□

Então com os resultados demonstrados até aqui, podemos enunciar e demonstrar o Teorema mais importante deste capítulo, que diz que para todo problema Γ de ACUN-unificação, existe um conjunto finito L de substituições que é um conjunto completo de ACUNh-unificadores para Γ e além disso da uma forma construtível de como obter tal conjunto.

Teorema 3.6. *Seja Γ um problema de ACUNh-unificação, então existe um conjunto finito L que é um conjunto completo de ACUNh-unificadores de Γ .*

Demonstração. Seja Γ um problema de ACUNh-unificação, sem perda de generalidade, suponha $\Gamma = \{t_1 =? t'_1, \dots, t_n =? t'_n\}$

Tome o conjunto $\Gamma' := \{(t_i \oplus t'_i) \downarrow =? 0 \mid t_i =? t'_i \in \Gamma\}$, isto é, a forma padronizada de Γ . Portanto pela Proposição 2.1 da padronização e Proposição 2.2 da normalização, temos que Γ e Γ' possuem os mesmo ACUNh-unificadores, logo L é um conjunto completo de ACUNh-unificadores de Γ se, e somente se, L é um conjunto completo de ACUNh-unificadores de Γ' .

Sejam $\widehat{\Gamma} := Purif(\Gamma')$ que pelo Teorema 3.2 é uma extensão conservativa de Γ' e conjunto $\widehat{L} := \mathcal{J}_{XORh}(\widehat{\Gamma} \parallel \emptyset \parallel \emptyset)$, que é de fato um conjunto finito pois \mathcal{J}_{XORh} é terminante pelo Teorema 3.3, implicando que tem um conjunto finito de estados finais sempre.

Se $\widehat{L} = \emptyset$ então todo estado final de $\widehat{\Gamma} \parallel \emptyset \parallel \emptyset$ é um estado de falha e portanto $\widehat{\Gamma}$ não possui ACUNh-unificador, pois casos contrário se existe σ ACUNh-unificador de $\widehat{\Gamma}$, pelo Teorema 3.5 da completude de \mathcal{J}_{XORh} existe $\sigma_\Lambda \in \widehat{L} = \emptyset$ uma contradição. Portanto Γ' não possui ACUNh-unificadores, pois $\widehat{\Gamma}$ não possui ACUNh-unificadores e é uma extensão conservativa de Γ' , e dessa forma Γ também não possui ACUNh-unificadores pois Γ' é sua forma padronizada. Então por vacuidade $\widehat{L} = \emptyset$ é um conjunto completo de ACUNh-unificadores de Γ .

Se $\widehat{L} \neq \emptyset$ então pelo Teorema 3.4 da correção de \mathcal{J}_{XORh} , para cada $\sigma \in \widehat{L}$, σ é um ACUNh-unificador de $\widehat{\Gamma}$ idempotente e pelo Teorema 3.5 da completude de \mathcal{J}_{XORh} , para cada ϕ ACUNh-unificador de $\widehat{\Gamma}$ existe uma substituição $\sigma \in \widehat{L}$ tal que $\sigma|_{\mathcal{V}ar(\widehat{\Gamma})} \lesssim_{\oplus_h} \phi|_{\mathcal{V}ar(\widehat{\Gamma})}$, equivalentemente, \widehat{L} é um conjunto completo de ACUNh-unificadores de $\widehat{\Gamma}$. Então $\widehat{\Gamma}$ é uma extensão conservativa de Γ' e \widehat{L} é um conjunto completo de ACUNh-unificadores para $\widehat{\Gamma}$, então pela Proposição 1.6 encontrada na página 32, temos que o conjunto $L := \{\sigma|_{\mathcal{V}ar(\Gamma')} \mid \sigma \in \widehat{L}\}$ é um conjunto completo de ACUNh-unificadores para Γ' , equivalentemente, L é um conjunto completo de ACUNh-unificadores de Γ . \square

Corolário 3.3. *Seja Γ problema de XOR/XORh-unificação elementar com constantes, então existe um conjunto, unitário ou vazio, L que é um conjunto completo de XOR/XORh-unificadores de Γ .*

Demonstração. A prova é bem simples, como Γ é um problema de XOR/XORh-unificação elementar com constantes, e portanto os únicos símbolos de função não constantes que ocorrem em Γ são $\oplus/\oplus, h$, portanto não é possível aplicar nenhuma regra *N-decomposição*, sobrando apenas as regras determinísticas, isto é, existe apenas um único estado final obtido no algoritmo \mathcal{J}_{XORh} , sendo L conjunto completo de ACUNh-unificadores de Γ , então $L = \emptyset$ ou L é unitário. \square

Capítulo 4

Unificação Assimétrica

Iremos abordar o problema de encontrar um conjunto completo de unificadores \mathcal{C} para o problema de E' -unificação $s \stackrel{?}{=}_{E'} t$ com t em sua forma normal com relação à $\rightarrow_{\mathcal{R}, E}$, tal que para todo $\sigma \in \mathcal{C}$, $s\sigma \stackrel{?}{=}_{E'} t\sigma$ e $t\sigma$ está em sua forma normal onde $(\Sigma'_{E'}, \mathcal{R}, E)$ é uma decomposição de E' . Um novo paradigma de unificação surge para comportar essas técnicas utilizadas em ferramentas de análise de protocolos de criptografia que aplicam unificação módulo teorias equacionais. A unificação assimétrica se baseia em:

- Decomposição $(\Sigma_E, \mathcal{R}, E)$ de uma teoria equacional em $E' = E'' \dot{\cup} E$, onde é possível orientar cada equação de E'' , obtendo o sistema de reescrita \mathcal{R} convergente módulo E .
- Redução de Γ um problema de E' -unificação em um conjunto de problemas $s \stackrel{?}{=} t$ onde o termo t é \mathcal{R}, E -irredutível e se σ é um unificador de $s \stackrel{?}{=} t$, $t\sigma$ é \mathcal{R}, E -irredutível.

Intuitivamente, um problema de *unificação assimétrica* Γ é um problema de unificação sobre as formas normais de cada equação em Γ com relação ao sistema reescrita da decomposição, e os *unificadores assimétricos* de Γ são unificadores de Γ , que quando aplicados na forma normal do lado direito de cada equação em Γ , mantém-se em sua forma normal.

Neste capítulo vamos apresentar o estudo desenvolvido por Liu em [18] para computar um conjunto de ACUN-unificadores assimétricos, para Γ um problema de ACUN-unificação, a partir de um conjunto completo de ACUN-unificadores padrões de Γ , obtido pelo algoritmo \mathcal{J}_{XORh} descrito na seção 3.2 do capítulo 3. Mais especificamente, dado um conjunto de equações Γ e um ACUN-unificador *padrão* σ de Γ , vamos construir um conjunto L_σ de ACUN-unificadores assimétricos que são instâncias de σ . Para

isto apresentaremos o algoritmo \mathcal{J}_{AXO} que retorna uma lista de E' -unificadores de unificadores L_σ para um dado problema de E' -unificação.

Dada uma decomposição (Σ, \mathcal{R}, E) da teoria equacional E' e um problema de E' -unificação assimétrica $\Gamma = \{t_1 =^? \widehat{t}_1, \dots, t_n =^? \widehat{t}_n\}$, o algoritmo consiste dos seguintes passos:

1. Computar um conjunto completo e finito $\mathcal{U}_{E'}(\Gamma)$ de E' -unificadores de Γ , usando um algoritmo de unificação finitária para E' . Se $\mathcal{U}_{E'}(\Gamma)$ for vazio, então não há E' -unificadores assimétricos de Γ .
2. Para cada $\sigma \in \mathcal{U}_{E'}(\Gamma)$, deve-se verificar para cada $t_i =^? \widehat{t}_i \in \Gamma$, se o termo $(\widehat{t}_i \downarrow_{\mathcal{R}, E})\sigma$ está em sua forma normal. Todos os unificadores que cumprirem as condições acima serão unificadores assimétricos.
3. Se existir uma substituição $\sigma \in \mathcal{U}_{E'}(\Gamma)$ tal que para algum problema de unificação $t_i =^? \widehat{t}_i \in \Gamma$, o termo $(\widehat{t}_i \downarrow_{\mathcal{R}, E})\sigma$ não está em sua forma normal, então devemos computar um $\mathcal{R} \dot{\cup} E$ -unificador assimétrico equivalente a σ se possível.
4. Se ambos os passos anteriores falharem, implica que cada unificador σ de Γ e seus equivalentes, não são unificadores assimétricos de Γ em sua forma geral. Porém podemos obter instâncias de σ , que não equivalentes a σ , que são unificadores assimétricos, obtidos por instanciar variáveis apropriadas em σ . Este passo é muito custoso, então deverá ser utilizado em ultimo caso. Para cada tal instância obtida dessa forma, deveser repetido os passos (2) e (3).

Agora iremos aplicar essa abordagem para a teoria equacional ACUN, os passos (1) e (2) consistem em verificar se dentre os ACUN-unificadores padrões de Γ existem ACUN-unificadores assimétricos equivalentes a cada um deles.

A partir disso iremos desenvolver um método para obter um ACUN-unificador assimétrico a partir de um ACUN-unificador padrão.

4.1 Preliminares

Sejam Σ uma assinatura e E' um conjunto de Σ -identidades. Suponha que $E' = E'' \dot{\cup} E$ e que exista um sistema de reescrita \mathcal{R} para E'' , de tal forma que (Σ, \mathcal{R}, E) é uma *decomposição* de E' , que eventualmente denotaremos E' pela união $\mathcal{R} \dot{\cup} E$. As definições a seguir fazem uso da Definição 1.38 de

decomposição de uma teoria equacional, denotaremos por simplicidade, a relação $\rightarrow_{\mathcal{R},E}$ da decomposição (Σ, \mathcal{R}, E) por \rightarrow .

Definição 4.1 (Unificador Padrão). *Sejam E' um conjunto de Σ -identidades tal que (Σ, \mathcal{R}, E) é uma decomposição de E' e $\Gamma = \{t_1 =^? \hat{t}_1, \dots, t_n =^? \hat{t}_n\}$ um conjunto de equações. Uma substituição σ é um E' -unificador padrão de Γ se, e somente se, para cada equação $t_i =^? \hat{t}_i \in \Gamma$, tem-se que $(t_i \downarrow)\sigma \downarrow =_E (\hat{t}_i \downarrow)\sigma \downarrow$.*

Teorema 4.1. *Seja Γ um problema de ACUNh-unificação e \rightarrow a relação de reescrita ACUNh módulo AC. σ é um ACUNh-unificador de Γ se, e somente se, σ é um ACUNh-unificador padrão de Γ .*

Demonstração. Este teorema é uma consequência direta da Proposição 2.2 □

A definição a seguir trata do caso em que para cada equação $t_i =^? \hat{t}_i \in \Gamma$, tem-se que, $(\hat{t}_i \downarrow)\sigma$ é irreduzível, e σ um unificador padrão de Γ .

Definição 4.2 (Unificação Assimétrica). *Sejam E' um conjunto de Σ -identidades tal que (Σ, \mathcal{R}, E) é uma decomposição de E' e $\Gamma = \{t_1 =^? \hat{t}_1, \dots, t_n =^? \hat{t}_n\}$ um problema de E' -unificação e σ um E' -unificador padrão de Γ . Dizemos que σ é um E' -unificador assimétrico de Γ se, e somente se, para cada equação $t_i =^? \hat{t}_i \in \Gamma$ tem-se que $(t_i \downarrow)\sigma \downarrow =_E (\hat{t}_i \downarrow)\sigma$. Um conjunto $\mathcal{UA}_{E'}(\Gamma)$ é um conjunto completo de E' -unificadores assimétricos de Γ , desde que possua as propriedades abaixo:*

(i) $\forall \sigma \in \mathcal{UA}_{E'}(\Gamma)$, σ é um E' -unificador assimétrico idempotente de Γ .

(ii) Para todo E' -unificador assimétrico θ de Γ , $\exists \sigma \in \mathcal{UA}_{E'}(\Gamma)$. $\sigma|_{\text{var}(\Gamma)} \lesssim_E \theta|_{\text{var}(\Gamma)}$.

Notação: $\Gamma = \{t_1 =^\downarrow \hat{t}_1, \dots, t_n =^\downarrow \hat{t}_n\}$ denota um problema de unificação assimétrica.

Na sequência, a menos que seja dito o contrário, em cada equação $t_i =^\downarrow \hat{t}_i$ de Γ o lado direito está em sua forma normal, isto é, \hat{t}_i é irreduzível w.r.t \mathcal{R} .

Exemplo 4.1. *Seja $\Gamma = \{f(y \oplus a) =^\downarrow f(x \oplus z)\}$ um problema de ACUN-unificação, pelo algoritmo \mathcal{J}_{XORh} temos o E -unificador mais geral $\sigma = \{x \mapsto v \oplus z, y \mapsto v \oplus a\}$ de Γ , porém $f(x \oplus z)\sigma = f(x\sigma \oplus z\sigma) = f(v \oplus z \oplus z)$, que é redutível no sistema de reescrita \mathcal{R}_\oplus módulo AC.*

Mas fazendo $\theta = \{v \mapsto v' \oplus z\}$ e aplicando em σ e normalizando sua imagem, obtemos $\sigma\theta = \{x \oplus v', y \mapsto v' \oplus z \oplus a\}$.

Então $\sigma\theta$ é um ACUN-unificador de Γ com $f(x \oplus z)\sigma\theta = f(v' \oplus z)$, que está em sua forma normal com relação ao sistema de reescrita \mathcal{R}_{\oplus} módulo AC. Portanto $\sigma\theta$ é um ACUN-unificador assimétrico de Γ .

4.2 Unificação assimétrica módulo ACUN

Nesta seção vamos apresentar um método para solubilidade de problemas para ACUN-unificação assimétrica, desenvolvido por Liu em [18], para isso dado uma assinatura $\Sigma \supseteq \Sigma_{XOR}$ utilizaremos a decomposição $(\Sigma, \mathcal{R}_{\oplus}, AC)$ da teoria equacional ACUN, apresentada no capítulo 2. Neste capítulo utilizaremos a teoria equacional ACUN, a menos que mencionado o contrário, então quando relacionado com a teoria equacional ACUN mencionaremos apenas unificação, unificador assimétrico, unificador, etc.

Definição 4.3 (Termo Simples, Termo Soma). *Seja s um termo, s é dito um termo soma se, e somente se, existem $n \in \mathbb{N}$ e termos t_1, \dots, t_n tais que $s \downarrow = t_1 \oplus \dots \oplus t_n$, onde $n \geq 2$ e para todo $i \in \{1, \dots, n\}$ tem-se que $\text{raiz}(t_i) \neq \oplus$, caso contrário s é dito termo simples. Diremos que um termo simples $t \in_{\oplus} S$ se, e somente se, S está em sua forma normal e $S =_{AC} t \oplus S'$, isto é, t é um átomo de S .*

Definição 4.4 (Restrição). *Uma restrição é um par da forma (v, s) onde v é uma variável e s é um termo simples.*

Definição 4.5. *Dado um conjunto de restrições e uma substituição θ , define-se o conjunto $\Upsilon\theta$ da seguinte forma*

$$\Upsilon\theta = \{(v_1, s_1\theta \downarrow), \dots, (v_n, s_n\theta \downarrow)\}$$

Caso $s_i\theta \downarrow$ não seja um termo simples, isto é, $s_i\theta \downarrow =_{AC} t_1 \oplus \dots \oplus t_n$ com t_i termo simples para cada $i = 1, \dots, n$. Então substituímos o par $(v_i, t_1 \oplus \dots \oplus t_n)$ pelos pares $(v_i, t_1), \dots, (v_i, t_n)$ em $\Upsilon\theta$.

Notações:

- $\Upsilon \cup \{(v, s)\} = \Upsilon \cup (v, s)$
- $\Upsilon[\frac{\hat{v}}{v}] = \{(y, t) \in \Upsilon \mid y \neq v\} \cup \{(\hat{v}, t) \mid (v, t) \in \Upsilon\}$
- $\Upsilon[\frac{v_{12}}{v_1, v_2}] = (\Upsilon[\frac{v_{12}}{v_1}])[\frac{v_{12}}{v_2}]$

- $\Upsilon[\frac{v'_1}{v_1}, \frac{v'_2}{v_2}, \frac{v_{12}}{v_1, v_2}] = \Upsilon[\frac{v'_1}{v_1}] \cup \Upsilon[\frac{v'_2}{v_2}] \cup \Upsilon[\frac{v_{12}}{v_1, v_2}]$
- $\mathcal{V}ar(\Upsilon) := \bigcup_{(v,t) \in \Upsilon} \{v\} \cup \mathcal{V}ar(t)$

Definição 4.6 (Conjunto de inequações). *Seja Δ um conjunto de pares (s, t) , onde $ratz(s) = ratz(t)$ ($s \downarrow \oplus t \downarrow$) $\downarrow \neq_{AC}^? 0$, é chamado de conjunto de inequações. Sejam $\Delta = \{(s_1, t_1), \dots, (s_n, t_n)\}$ e θ uma substituição, então definimos,*

$$\Delta\theta = \{(s_1\theta \downarrow, t_1\theta \downarrow), \dots, (s_n\theta \downarrow, t_n\theta \downarrow)\}.$$

Notação: $\mathcal{V}ar(\Delta) := \bigcup_{(s,t) \in \Delta} (\mathcal{V}ar(s) \cup \mathcal{V}ar(t))$

Definição 4.7 (Violação, Satisfação). *Sejam Υ um conjunto de restrições, Δ um conjunto de inequações e σ uma substituição.*

i) *Dizemos que σ viola $(v, s) \in \Upsilon$ se, e somente se, possui as seguintes propriedades*

- $v\sigma \downarrow \neq_{AC} 0$ e $s\sigma \downarrow \neq_{AC} 0$.
- $v\sigma \downarrow \oplus s\sigma \downarrow$ é redutível.

Caso contrário é dito que σ satisfaz (v, s) . Uma substituição σ satisfaz Υ se, e somente se, σ satisfaz todo $(s, t) \in \Upsilon$.

ii) *Dizemos que σ viola $(s, t) \in \Delta$ se, e somente se, $(s\sigma \downarrow \oplus t\sigma \downarrow) \downarrow =_{AC} 0$, caso contrário, dizemos que σ satisfaz (s, t) . Uma substituição σ satisfaz Δ se, e somente se, σ satisfaz todo $(s, t) \in \Delta$.*

Definição 4.8 (Variáveis originais, Variáveis suporte). *Seja Γ um problema de unificação assimétrica. As variáveis que ocorrem em Γ serão chamadas de variáveis originais e as que não ocorrem em Γ de variáveis suporte.*

Definição 4.9 (Conflito). *Seja σ um unificador de Γ e s, t termos simples. Dizemos que uma variável original x está em conflito com o termo simples t em σ , desde que as seguintes condições se cumpram:*

- Existe uma designação $[x \mapsto t \oplus T] \in \sigma$.
- Existe $u = \downarrow v[x \oplus s]_p \in \Gamma$, com $p \in \mathcal{P}os(v)$.

(iii) $s\sigma \downarrow_{=AC} t \oplus S$, onde S é um termo que pode ser vazio.

Observação 4.1. Observe que na definição de conflito, a partir do item (iii) obtemos $u\sigma =_{AC} (v\sigma)[x\sigma \oplus s\sigma]_p =_{AC} (v\sigma)[t \oplus t \oplus S]_p$, que é redutível.

Definição 4.10 (Instância de $(\Gamma, \sigma, \Upsilon, \Delta)$). Sejam Γ um problema de unificação assimétrica, σ um unificador de Γ , Υ um conjunto de restrições e Δ um conjunto de inequações. Dada uma substituição δ , dizemos que $\delta \in \text{Asym}(\Gamma, \sigma, \Upsilon, \Delta)$ se, e somente se,

(i) δ é um unificador assimétrico de Γ .

(ii) $\exists \theta$ substituição. $\delta = \sigma\theta|_{\text{Var}(\Gamma)}$.

(iii) $\sigma\theta$ satisfaz $\Upsilon\theta$ e $\Delta\theta$.

O conjunto $\text{Inst}(\Gamma, \sigma, \Upsilon, \Delta)$ é o conjunto das substituições $\delta \in \text{Asym}(\Gamma, \sigma, \Upsilon, \theta)$ tais que $\delta = \sigma\theta|_{\text{Var}(\Gamma)}$ e $\sigma\theta$ é idempotente.

Vamos provar algumas proposições que utilizaremos para provar que o algoritmo é correto e completo, dizendo exatamente que é suficiente considerarmos apenas substituições idempotentes, sem perder a generalidade das soluções.

Proposição 4.1. Seja $\delta \in \text{Inst}(\Gamma, \sigma, \Upsilon, \Delta)$ onde $\delta = \sigma\theta|_{\text{Var}(\Gamma)}$ e $\sigma\theta$ é idempotente. Se $\text{Var}(\Upsilon) \cap \text{Dom}(\sigma) = \emptyset$ então, $\sigma\theta$ satisfaz Υ .

Demonstração. Suponha Υ e δ como na hipótese então, para cada $(v, t) \in \Upsilon$ tem-se que $t\sigma = v$, assim podemos concluir que $\Upsilon\sigma\theta = \Upsilon\theta$.

Como $\delta \in \text{Inst}(\Gamma, \sigma, \Upsilon, \Delta)$, então existe θ tal que $\delta = \sigma\theta|_{\text{Var}(\Gamma)}$, $\sigma\theta$ é idempotente e satisfaz $\Upsilon\theta$. Queremos provar que $\sigma\theta$ satisfaz Υ , então se $v\sigma\theta \downarrow_{=AC} 0$ ou $t\sigma\theta \downarrow_{=AC} 0$ pela definição de violação, temos que $\sigma\theta$ satisfaz $(v, t) \in \Upsilon$.

Suponha que $v\sigma\theta \not\downarrow_{=AC} 0$ e $t\sigma\theta \not\downarrow_{=AC} 0$ então basta provar que $v\sigma\theta \downarrow \oplus t\sigma\theta \downarrow$ é irredutível.

Então, para cada $(v, t) \in \Upsilon$ existe $n \geq 1$ e termos simples t_1, \dots, t_n tais que $t\sigma\theta \downarrow_{=AC} t_1 \oplus \dots \oplus t_n$, e portanto $(v, t_i) \in \Upsilon\sigma\theta = \Upsilon\theta$ para cada $i \in \{1, \dots, n\}$. Como $\sigma\theta$ é idempotente e $\text{Var}(t_i) \subseteq \text{Var}(t\sigma\theta)$ temos $t_i\sigma\theta = t_i$.

De fato, como $t\sigma\theta \downarrow \neq 0$, temos que cada $t_i \neq 0$ e como $\sigma\theta$ satisfaz $\Upsilon\sigma\theta$, por hipótese temos que $v\sigma\theta \downarrow \oplus t_i\sigma\theta \downarrow$ é irredutível. Porém $t_i\sigma\theta = t_i$, assim para cada $i \in \{1, \dots, n\}$, $v\sigma\theta \downarrow \oplus t_i$ é irredutível, e portanto, $v\sigma\theta \downarrow \oplus t_1 \oplus \dots \oplus t_n =_{AC} v\sigma\theta \downarrow \oplus t\sigma\theta \downarrow$ é irredutível. Portando conclui-se que em todos os casos $\sigma\theta$ satisfaz $(v, t) \in \Upsilon$ então provamos que $\sigma\theta$ satisfaz Υ . \square

Proposição 4.2. *Seja $\delta \in \text{Inst}(\Gamma, \sigma, \Upsilon, \Delta)$ onde $\delta = \sigma\gamma|_{\text{Var}(\Gamma)}$ e $\sigma\gamma$ é idempotente. Se $\text{Var}(\Delta) \cap \text{Dom}(\sigma) = \emptyset$ então, $\sigma\gamma$ satisfaz Δ .*

Demonstração. Sejam δ e Δ como na hipótese. Então, $s\sigma = s$, $t\sigma = t$ e $\Delta\sigma\gamma = \Delta\gamma$.

Como $\sigma\gamma$ satisfaz $\Delta\gamma$ então $\sigma\gamma$ satisfaz $\Delta\sigma\gamma$, e como, para todo $(s, t) \in \Delta$, $(s\sigma\gamma \downarrow, t\sigma\gamma \downarrow) \in \Delta\sigma\gamma$, então $(s\sigma\gamma\sigma\gamma \downarrow \oplus t\sigma\gamma\sigma\gamma \downarrow) \downarrow \neq 0$. Como $\sigma\gamma$ é idempotente, temos $(s\sigma\gamma \downarrow \oplus t\sigma\gamma \downarrow) \downarrow \neq 0$, implicando que $\sigma\gamma$ satisfaz Δ . \square

Proposição 4.3. *Seja $\sigma\gamma$ um unificador assimétrico de Γ , idempotente que satisfaz Υ e Δ . Se $\text{Var}(\Upsilon, \Delta) \cap \text{Dom}(\sigma) = \emptyset$ então, $\sigma\gamma|_{\text{Var}(\Gamma)} \in \text{Inst}(\Gamma, \sigma, \Upsilon, \Delta)$*

Demonstração. Seja $\sigma\gamma$ como na hipótese, então basta provar que $\sigma\gamma$ satisfaz $\Upsilon\gamma$ e $\Delta\gamma$.

Tome $(v, t') \in \Upsilon\gamma$ qualquer, então existe $(v, t) \in \Upsilon$ tal que $t\gamma \downarrow =_{AC} t' \oplus T$, como por hipótese $\text{Var}(\Upsilon, \Delta) \cap \text{Dom}(\sigma) = \emptyset$ segue que $t\sigma = t$. Portanto $t\sigma\gamma \downarrow =_{AC} t' \oplus T$, e então $\text{Var}(t') \subseteq \text{Var}(t\sigma\gamma)$ e além disso, como $\sigma\gamma$ é idempotente, temos que $t'\sigma\gamma = t'$. Se $v\sigma\gamma \downarrow =_{AC} 0$ ou $t'\sigma\gamma \downarrow =_{AC} 0$ então obtemos que $\sigma\gamma$ satisfaz (v, t') . Suponha que $v\sigma\gamma \downarrow \neq_E 0$ e $t'\sigma\gamma \downarrow \neq_{AC} 0$ então $t\sigma\gamma \downarrow \neq_{AC} 0$ e como $\sigma\gamma$ satisfaz Υ tem-se que $v\sigma\gamma \downarrow \oplus t\sigma\gamma \downarrow$ é irredutível, implicando que $v\sigma\gamma \downarrow \oplus t' \oplus T$ é irredutível e por conseguinte $v\sigma\gamma \downarrow \oplus t'$ é irredutível, assim por $t'\sigma\gamma \downarrow = t'$ tem-se $v\sigma\gamma \downarrow \oplus t'\sigma\gamma \downarrow$ é irredutível, como queríamos demonstrar.

Tome $(s, t) \in \Delta$, então $(s\gamma, t\gamma) \in \Delta\gamma$. Como por hipótese $\text{Var}(\Upsilon, \Delta) \cap \text{Dom}(\sigma) = \emptyset$ temos que $s\sigma = s$ e $t\sigma = t$, implicando que $s\sigma\gamma \downarrow \oplus t\sigma\gamma \downarrow =_{AC} s\sigma\gamma\sigma\gamma \downarrow \oplus t\sigma\gamma\sigma\gamma \downarrow =_{AC} s\gamma\sigma\gamma \downarrow \oplus t\gamma\sigma\gamma \downarrow$, então $(s\sigma\gamma \downarrow \oplus t\sigma\gamma \downarrow) \downarrow =_{AC} (s\gamma\sigma\gamma \downarrow \oplus t\gamma\sigma\gamma \downarrow) \downarrow$ e como $\sigma\gamma$ satisfaz Δ tem-se que $(s\sigma\gamma \downarrow \oplus t\sigma\gamma \downarrow) \downarrow \neq 0$, implicando que $(s\gamma\sigma\gamma \downarrow \oplus t\gamma\sigma\gamma \downarrow) \downarrow \neq 0$. Logo $\sigma\gamma$ satisfaz $\Delta\gamma$. \square

Proposição 4.4. *Seja t um termo em sua forma normal e α um renomeamento de t então $t\alpha$ está em sua forma normal.*

Demonstração. Suponha por absurdo que $t\alpha \rightarrow t'$. Como α^{-1} é uma substituição, temos que $t\alpha\alpha^{-1} \rightarrow t'\alpha$ e $t\alpha\alpha^{-1} = t$ pelo Corolário 1.1.

Portanto $t \rightarrow t'\alpha^{-1}$ que é uma contradição pois por hipótese supomos t em sua forma normal. \square

Proposição 4.5. *Sejam δ uma substituição, α um renomeamento de variáveis de δ livre em $W \subset \mathcal{V}$ e t um termo onde $\mathcal{V}ar(t) \subseteq W$. Se $t\delta\alpha \rightarrow t'$ então $t\delta \rightarrow t'\alpha^{-1}$.*

Demonstração. Sejam t, δ, α e W como na hipótese, como α é um renomeamento de variáveis de δ livre de $W \subset \mathcal{V}$ então para todo $x \in \mathcal{D}om(\delta)$, tem-se que $x\delta\alpha^{-1} = x\delta$.

Tome $v \in \mathcal{V}ar(t) \setminus \mathcal{D}om(\delta)$, então $v \in W \setminus \mathcal{D}om(\delta)$, logo $v\delta = v$ e $v\alpha\alpha^{-1} = v$ pois α é livre de $W \subset \mathcal{V}$. Portanto $t\delta\alpha\alpha^{-1} = t\delta$.

Suponha que $t\delta\alpha \rightarrow t'$, como α^{-1} é uma substituição temos que $t\delta\alpha\alpha^{-1} \rightarrow t'\alpha^{-1}$, e o resultado segue. \square

Corolário 4.1. *Sejam δ uma substituição, α um renomeamento de variáveis de δ livre de $W \subset \mathcal{V}$ e t um termo onde $\mathcal{V}ar(t) \subseteq W$. Se $t\delta$ está em sua forma normal então $t\delta\alpha$ está em sua forma normal.*

Demonstração. Esse corolário é a contra-positiva da Proposição 4.5. \square

Proposição 4.6. *Seja Γ um problema de unificação assimétrica, δ um unificador assimétrico de Γ e α um renomeamento de variáveis de δ livre de $W \subset \mathcal{V}$. Se $\mathcal{V}ar(\Gamma) \subseteq W$ então $\delta\alpha$ é um unificador assimétrico de Γ .*

Demonstração. Tome $u = \downarrow u' \in \Gamma$ então $(u \downarrow)\delta =_{AC} (u')\delta$, pois δ é um unificador assimétrico de Γ , note que $\mathcal{V}ar(u') \subseteq \mathcal{V}ar(\Gamma) \subseteq W$ e pelo corolário 4.1 $u'\delta\alpha$ está em sua forma normal e como $\delta\alpha$ é um unificador de Γ temos que $\delta\alpha$ é um unificador assimétrico de Γ . \square

Proposição 4.7. *Seja δ uma substituição satisfazendo Υ e Δ , e α um renomeamento de variáveis de δ livre de $W \subset \mathcal{V}$. Se $\mathcal{V}ar(\Upsilon, \Delta) \subseteq W$ então $\delta\alpha$ satisfaz Υ e Δ .*

Demonstração. Tome $(v, t) \in \Upsilon$, suponha sem perda de generalidade que $v\delta \neq 0$ e $t\delta \neq 0$, como por hipótese δ satisfaz Υ implica que $(v\delta \downarrow \oplus t\delta \downarrow) \downarrow =_{AC} v\delta \downarrow \oplus t\delta \downarrow$ então, $(v\delta \downarrow \oplus t\delta \downarrow)\alpha$ é irreduzível e portanto $(v\delta \downarrow)\alpha \oplus (t\delta \downarrow)\alpha$ é irreduzível. Como $(v\delta \downarrow)\alpha = v\delta\alpha \downarrow$ e $(t\delta \downarrow)\alpha = t\delta\alpha \downarrow$ então $v\delta\alpha \downarrow \oplus t\delta\alpha \downarrow$ é irreduzível.

A prova é análoga para $(s, t) \in \Delta$. □

A seguinte proposição estabelece um critério mais simples para pertinência no conjunto \mathcal{Inst} .

Proposição 4.8. *Sejam $\sigma\gamma$ uma substituição, Υ um conjunto de restrições, Δ um conjunto de inequações e Γ um problema de unificação assimétrica tais que $\mathcal{Var}(\Upsilon, \Delta) \cap \mathcal{Dom}(\sigma) = \emptyset$. Então $\sigma\gamma|_{\mathcal{Var}(\Gamma)} \in \mathcal{Inst}(\Gamma, \sigma, \Upsilon, \Delta)$ se, e somente se, $\sigma\gamma$ é um unificador assimétrico idempotente de Γ que satisfaz Υ e Δ .*

Demonstração. As proposições 4.1, 4.2 e 4.3 garante que, sob suas hipóteses que $\sigma\gamma|_{\mathcal{Var}(\Gamma)} \in \mathcal{Inst}(\Gamma, \sigma, \Upsilon, \Delta)$ se, e somente se, $\sigma\gamma$ satisfaz Υ e Δ , e $\sigma\gamma|_{\mathcal{Var}(\Gamma)}$ é um unificador assimétrico idempotente de Γ . □

Teorema 4.2. *Sejam Γ, Υ, Δ e σ uma substituição tais que $\mathcal{Var}(\Upsilon, \Delta) \cap \mathcal{Dom}(\sigma) = \emptyset$ Se existe uma substituição γ tal que $\sigma\gamma$ é um unificador assimétrico de Γ e $\sigma\gamma$ satisfaz Υ e Δ então existe α um renomeamento de variáveis de $\sigma\gamma$ tal que $\sigma\gamma\alpha|_{\mathcal{Var}(\Gamma)} \in \mathcal{Inst}(\Gamma, \sigma, \Upsilon, \Delta)$*

Demonstração. Tome $W := \mathcal{Var}(\Gamma, \Upsilon, \Delta) \cup \mathcal{Dom}(\sigma\gamma) \cup \mathcal{Var}(\mathcal{Im}(\sigma\gamma))$.

Supondo $\{x_1, \dots, x_n\} = \mathcal{Dom}(\sigma\gamma) \cap \mathcal{Var}(\mathcal{Im}(\sigma\gamma))$ e um renomeamento de variáveis $\alpha = \{x_1 \mapsto y_1, \dots, x_n \mapsto y_n\}$ onde $\{y_1, \dots, y_n\} \subset \mathcal{V} \setminus W$ então α é um renomeamento de variáveis de $\sigma\gamma$ livre de W , e $\sigma\gamma\alpha$ é idempotente. E pelas proposições 4.6 e 4.7 obtemos que $\sigma\gamma\alpha$ é um unificador assimétrico idempotente de Γ que satisfaz Υ e Δ , portanto pela Proposição 4.8 temos que $\sigma\gamma\alpha|_{\mathcal{Var}(\Gamma)} \in \mathcal{Inst}(\Gamma, \sigma, \Upsilon, \Delta)$. □

Vamos mostrar agora que todo unificador assimétrico de Γ que é uma instância de σ é um renomeamento de algum $\delta \in \mathcal{Inst}(\Gamma, \sigma, \emptyset, \emptyset)$, equivalentemente, é suficiente trabalharmos apenas com os unificadores assimétricos idempotentes.

Definição 4.11. *Sejam A, B conjuntos de unificadores Γ , dizemos que $A \subseteq_{\alpha} B$ se, e somente se, para todo $\sigma \in A$, Existe α um renomeamento de variáveis de σ tal que $\sigma\alpha|_{\mathcal{Var}(\Gamma)} \in B$. Definimos, $A =_{\alpha} B \Leftrightarrow A \subseteq_{\alpha} B$ e $B \subseteq_{\alpha} A$*

Proposição 4.9. $Asym(\Gamma, \sigma, \emptyset, \emptyset) =_{\alpha} \mathcal{Inst}(\Gamma, \sigma, \emptyset, \emptyset)$

Demonstração. (\subseteq_{α}) Tome $\delta \in Asym(\Gamma, \sigma, \emptyset, \emptyset)$ tal que $\delta = \sigma\gamma|_{\mathcal{Var}(\Gamma)}$. Se $\sigma\gamma$ for idempotente então, pela definição de \mathcal{Inst} , temos $\sigma\gamma|_{\mathcal{Var}(\Gamma)} \in \mathcal{Inst}(\Gamma, \sigma, \emptyset, \emptyset)$.

Suponha que $\sigma\gamma$ não seja idempotente, então existem n número natural não nulo e $\{x_1, \dots, x_n\} = \text{Dom}(\sigma\gamma) \cap \text{Var}(\text{Im}(\sigma\gamma))$.

Considere $W := \text{Var}(\Gamma) \cup \text{Dom}(\sigma\gamma) \cup \text{Var}(\text{Im}(\sigma\gamma))$, $\{y_1, \dots, y_n\} \subset \mathcal{V} \setminus W$ e a substituição $\alpha = \{x_i \mapsto y_i \mid i = 1, \dots, n\}$. Então α é um renomeamento de variáveis de $\sigma\gamma$ livre de $W \supseteq \text{Var}(\Gamma)$. Como $\sigma\gamma$ é um unificador assimétrico de Γ então, pela Proposição 4.6, $\sigma\gamma\alpha$ é um unificador assimétrico de Γ , logo $\delta\alpha|_{\text{Var}(\Gamma)} = \sigma\gamma\alpha|_{\text{Var}(\Gamma)} \in \text{Asym}(\Gamma, \sigma, \emptyset, \emptyset)$. Como $\sigma\gamma\alpha$ é idempotente, temos $\delta\alpha|_{\text{Var}(\Gamma)} \in \text{Inst}(\Gamma, \sigma, \emptyset, \emptyset)$, e portanto $\text{Asym}(\Gamma, \sigma, \emptyset, \emptyset) \subseteq_{\alpha} \text{Inst}(\Gamma, \sigma, \emptyset, \emptyset)$.

(\supseteq_{α}) Basta tomar a identidade como renomeamento, então é direto a prova.

Assim $\text{Asym}(\Gamma, \sigma, \emptyset, \emptyset) =_{\alpha} \text{Inst}(\Gamma, \sigma, \emptyset, \emptyset)$. □

4.3 Um algoritmo para *ACUN*–unificação assimétrica

Nesta seção apresentaremos os algoritmo \mathcal{J}_{AXO} , proposto por Liu em [18] para solubilidade de problemas de *ACUN*-unificação assimétrica.

Dado um problema de *ACUN*-unificação assimétrica Γ e $\sigma \in \mathcal{U}_{ACUN}$, com \mathcal{U}_{ACUN} um conjunto completo de *ACUN*-unificadores padrões de Γ , o algoritmo \mathcal{J}_{AXO} , computa um unificador assimétrico para Γ que é equivalente a σ (se possível), caso não for possível encontrar um unificador assimétrico equivalente a σ , o algoritmo tentará encontrar um conjunto L_{σ} de unificadores assimétricos de Γ que são instâncias de σ , com a propriedade de que para todo λ unificador assimétrico de Γ que é instância de σ , existe um $\delta \in L_{\sigma}$ tal que $\delta|_{\text{Var}(\Gamma)} \lesssim_{\oplus} \lambda|_{\text{Var}(\Gamma)}$

\mathcal{J}_{AXO} consiste da aplicação exaustiva e consecutiva das regras *Separação* (Sep), *Ramificação* (Ram) e *Instanciação* (Inst), que serão descritas no decorrer desta seção. O algoritmo opera em triplas da forma $\sigma \parallel \Upsilon \parallel \Delta$, que serão chamadas de *estados*, e tais que σ é um *ACUN*-unificador padrão de Γ , Υ é um conjunto de restrições e Δ um conjunto de inequações. Denotaremos por

$$\sigma \parallel \Upsilon \parallel \Delta \Longrightarrow_{\mathcal{J}_{AXO}} \sigma_1 \parallel \Upsilon_1 \parallel \Delta_1 \vee \dots \vee \sigma_n \parallel \Upsilon_n \parallel \Delta_n \quad (4.1)$$

um passo de execução do algoritmo \mathcal{J}_{AXO} , isto é, a aplicação de uma das regras que compõem o algoritmo. Abusando da notação de $\Longrightarrow_{\mathcal{J}_{AXO}}$, na redução 4.1, diremos que para cada $i \in \{1, \dots, n\}$, $\sigma \parallel \Upsilon \parallel \Delta \Longrightarrow_{\mathcal{J}_{AXO}} \sigma_i \parallel \Upsilon_i \parallel \Delta_i$.

Quando quisermos explicitar qual regra foi utilizada, adotaremos a relação $\Rightarrow_{[R]}$, com $R \in \{\text{Sep}, \text{Ram}, \text{Inst}\}$.

Definição 4.12. Dado \mathcal{U}_{ACUN} um conjunto completo de ACUN-unificadores para Γ e $\sigma \in \mathcal{U}_{ACUN}$, definiremos um estado válido de \mathcal{J}_{AXO} por:

- $\sigma \parallel \emptyset \parallel \emptyset$ é um estado válido de \mathcal{J}_{AXO} , que será chamado por estado inicial.
- $\sigma' \parallel \Upsilon' \parallel \Delta'$ é um estado válido se, e somente se, existe $n \in \mathbb{N}$ tal que $\sigma' \parallel \Upsilon' \parallel \Delta'$ é obtido de $\sigma \parallel \emptyset \parallel \emptyset$ por n aplicações das regras de inferência de \mathcal{J}_{AXO} .
- Se $\sigma' \parallel \Upsilon' \parallel \Delta'$ é um estado válido de \mathcal{J}_{AXO} tal que nenhuma regra de \mathcal{J}_{AXO} é aplicável, dizemos que $\sigma' \parallel \Upsilon' \parallel \Delta'$ é um estado final, quando σ' for um unificador assimétrico, denotaremos o estado final $\sigma' \parallel \Upsilon' \parallel \Delta'$ como estado de solução, caso contrário, diremos que $\sigma' \parallel \Upsilon' \parallel \Delta'$ é um estado de falha.

4.3.1 Regras de \mathcal{J}_{AXO}

\mathcal{J}_{AXO} - Separação

Separação [Sep]: esta regra tem como objetivo retirar as variáveis *originais* $Im(\sigma)$ e as substituir por variáveis de *suporte*, pois o método de remover conflitos fará uso de variáveis *suporte*, assim com o objetivo de não alterar as variáveis *originais* precisamos remove-las da imagem e adicioná-las ao domínio.

Separação:

$$\frac{\sigma \parallel \Upsilon \parallel \Delta}{\sigma\theta \parallel \Upsilon\theta \parallel \Delta\theta} \text{ Sep}$$

Condições:

- Existe uma designação $[x \mapsto y \oplus S \oplus T] \in \sigma$ onde $x, y \in \mathcal{V}ar(\Gamma)$ e $y \notin \mathcal{V}ar(S)$
- $\theta = \{y \mapsto v \oplus S\}$ e v é uma variável de suporte nova.

Observação 4.2. Os termos T, S podem ser tomados de forma conveniente, desde que assegurando as condições da regra separação.

\mathcal{J}_{AXO} - Ramificação

Ramificação [Ram]: Esta regra consiste em detectar um conflito com alguma variável original x de Γ e tentar removê-lo usando uma variável suporte. A regra de ramificação divide-se em três casos, dependendo do tipo de conflito, a dizer, *não-variável*, *variável* e *auxiliar*.

- **Não-Variável [NRam]:** Esse tipo de ramificação será usado quando alguma variável original x tiver um conflito com um termo s , simples e não-variável, em σ .

Ramificação Não-Variável:

$$\frac{\sigma \parallel \Upsilon \parallel \Delta}{\sigma \theta \parallel \Upsilon' \theta \parallel \Delta \theta \quad \vee \quad \sigma \parallel \Upsilon'' \parallel \Delta} \text{NRam}$$

Condições:

- Existe uma designação $[x \mapsto v \oplus s \oplus S] \in \sigma$ tal que $v \notin \mathcal{V}ar(\Gamma)$, $x \in \mathcal{V}ar(\Gamma)$ e $v \notin \mathcal{V}ar(s)$.
- s é um termo simples, não-variável, x está em conflito com s em σ e $(v, s) \notin \Upsilon$.
- $\theta = \{v \mapsto v' \oplus s\}$ e v' é uma variável nova.
- $\Upsilon' = \Upsilon[\frac{v'}{v}] \cup (v', s)$ e $\Upsilon'' = \Upsilon \cup (v, s)$

- **Variável [VRam]:** Esta regra será aplicada quando existir um conflito entre duas variáveis originais x e y , isto é, quando existir $u =^\downarrow v \in \Gamma$, tal que $x \oplus y$ é um subtermo de v e as designações de x e y em σ tem uma variável suporte em comum.

Ramificação Variável:

$$\frac{\sigma \parallel \Upsilon \parallel \Delta}{\sigma \theta \parallel \Upsilon' \theta \parallel \Delta \theta \quad \vee \quad \sigma \parallel \Upsilon'' \parallel \Delta} \text{VRam}$$

Condições:

- Existem as designações $[x \mapsto v_i \oplus v_j \oplus S]$, $[y \mapsto v_i \oplus S'] \in \sigma$ onde $v_i, v_j \notin \mathcal{V}ar(\Gamma)$ e $x, y \in \mathcal{V}ar(\Gamma)$

- Existe $u =\downarrow u' \in \Gamma$ onde $x \oplus y$ é subtermo de u' .
- $(v_i, v_j), (v_j, v_i) \notin \Upsilon$
- $\theta = \{v_i \mapsto v'_i \oplus v_{ij}, v_j \mapsto v'_j \oplus v_{ij}\}$, onde v'_i, v'_j, v_{ij} são variáveis de suporte novas.
- $\Upsilon' = \Upsilon[\frac{v'_i}{v_i}, \frac{v'_j}{v_j}, \frac{v_{ij}}{v_i, v_j}] \cup A_i^j$, onde o conjunto A_i^j é definido por:

$$A_i^j := \{(v'_i, v_{ij}), (v'_j, v_{ij}), (v_{ij}, v'_i), (v_{ij}, v'_j), (v'_i, v'_j), (v_{ij}, v'_i)\}$$

- $\Upsilon'' = \Upsilon \cup \{(v_i, v_j), (v_j, v_i)\}$

- **Auxiliar:** Esse tipo de ramificação será utilizado quando existir um conflito entre duas variáveis originais x e y e um termo simples s , isto é, quando $x \oplus y$ é um subtermo de v para $u =\downarrow v \in \Gamma$, tal que $x\sigma =_{AC} s \oplus T$ e $y\sigma =_{AC} s \oplus T'$ e portanto $(x \oplus y)\sigma$ é redutível.

Ramificação Auxiliar:

$$\frac{\sigma \parallel \Upsilon \parallel \Delta}{\sigma \theta \parallel \Upsilon' \theta \parallel \Delta \theta \vee \sigma \parallel \Upsilon'' \parallel \Delta} \text{ARam}$$

Condições:

- Existem designações $[y \mapsto v \oplus S'], [x \mapsto v \oplus s \oplus S] \in \sigma$ onde $v \notin \mathcal{Var}(\Gamma)$ e $x, y \in \mathcal{Var}(\Gamma)$
- s é um termo simples e não-variável onde $v \notin \mathcal{Var}(s)$
- Existe uma equação assimétrica $u =\downarrow u' \in \Gamma$ onde $x \oplus y$ é subtermo de u' .
- $(v, s) \notin \Upsilon$
- $\theta = \{v \mapsto v' \oplus s\}$ onde, v' é uma variável de suporte nova.
- $\Upsilon' = \Upsilon[\frac{v'}{v}]$ e $\Upsilon'' = \Upsilon \cup (v, s)$

Observação 4.3. Note que para a regra ramificação há várias possíveis escolhas de variáveis suporte v na designação do $x \in \text{Dom}(\sigma)$, então o ramo à esquerda é definido pela escolha da variável suporte, e o lado direito é eliminar a escolha da variável suporte no ramo. A ramificação variável e a ramificação auxiliar não eliminam o conflito, apenas preparam σ para a regra de instanciação.

Exemplo 4.2. Seja $\Gamma = \{y \oplus z =^\downarrow x \oplus a, y \oplus a \oplus b =^\downarrow w \oplus a \oplus y\}$ um problema de unificação de unificação assimétrica. Observe que ao aplicar o algoritmo \mathcal{J}_{XORh} sobre Γ , obtemos o seguinte unificador padrão: $\sigma = \{x \mapsto y \oplus a \oplus z, w \mapsto b\}$. Pelos teoremas de correção e completude de \mathcal{J}_{XORh} , σ é um unificador idempotente e mais geral de Γ . Porém σ não é um unificador assimétrico de Γ , pois $y \oplus z =^\downarrow x \oplus a \in \Gamma$ e $x\sigma =_{AC} a \oplus (y \oplus z)$ então x tem um conflito com a em σ .

Vamos aplicar as regras de [Sep] e [Ram] sobre o estado inicial $\sigma \parallel \emptyset \parallel \emptyset$ para tentar transformar σ em um unificador assimétrico de Γ .

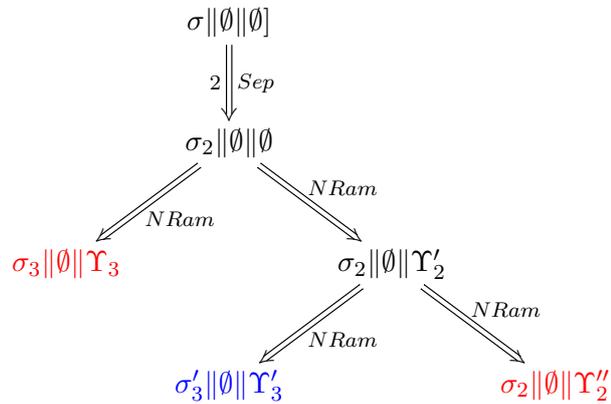
1. $\sigma \parallel \emptyset \parallel \emptyset$: como existem y, z variáveis originais na designação $[x \mapsto y \oplus a \oplus z] \in \sigma$, então aplicando [Sep] duas vezes obtemos: $\sigma \parallel \emptyset \parallel \emptyset \xRightarrow{2}_{Sep} \sigma_2 \parallel \emptyset \parallel \emptyset$ com, $\sigma_2 = \{x \mapsto v_1 \oplus a \oplus v_2, y \mapsto v_1, z \mapsto v_2, w \mapsto b\}$.
2. $\sigma_2 \parallel \emptyset \parallel \emptyset$: como x está em conflito com a em σ_2 , e v_1 é uma variável suporte na designação $[x \mapsto v_1 \oplus a \oplus v_2] \in \sigma_2$, podemos aplicar [NRam], obtendo: $\sigma_2 \parallel \emptyset \parallel \emptyset \xRightarrow{NRam} \sigma_3 \parallel \emptyset \parallel \Upsilon_3 \vee \sigma_2 \parallel \emptyset \parallel \Upsilon'_2$, com $\Upsilon_3 = \{(v'_1, a)\}$, $\Upsilon'_2 = \{(v_1, a)\}$, $\sigma_3 = \sigma_2 \theta_3 \downarrow$ e $\theta_3 = \{v_1 \mapsto v'_1 \oplus a\}$ e $\sigma_3 = \sigma_2 \theta_3 \downarrow = \{x \mapsto v'_1 \oplus v_2, y \mapsto v'_1 \oplus a, v_1 \mapsto v'_1 \oplus a, z \mapsto v_2, w \mapsto b\}$.
3. $\sigma_3 \parallel \emptyset \parallel \Upsilon_3$: note que $y \oplus a \oplus b =^\downarrow w \oplus a \oplus y \in \Gamma$ e $y\sigma_3 =_{AC} a \oplus v'_1$, logo y tem um conflito com a em σ_3 , porém a única variável suporte na designação $[y \mapsto v'_1 \oplus a] \in \sigma_3$ é v'_1 . Como $(v'_1, a) \in \Upsilon_3$, não é possível aplicar [Sep] ou [Ram]. Mais ainda $\sigma_3 \parallel \emptyset \parallel \Upsilon_3$ é um estado final e y tem um conflito com σ_3 , então σ_3 não é um unificador assimétrico de Γ .
4. $\sigma_2 \parallel \emptyset \parallel \Upsilon'_2$: x tem um conflito com a em σ_2 e $(v_1, a) \in \Upsilon'_2$, portanto não podemos aplicar [NRam] com a variável suporte v_1 , mas podemos aplicar com a variável suporte v_2 . Então, $\sigma_2 \parallel \emptyset \parallel \Upsilon'_2 \xRightarrow{NRam} \sigma'_3 \parallel \emptyset \parallel \Upsilon'_3 \vee \sigma_2 \parallel \emptyset \parallel \Upsilon''_2$ com $\Upsilon'_3 = \{(v_1, a), (v'_2, a)\}$, $\Upsilon''_2 = \{(v_1, a), (v_2, a)\}$, $\sigma'_3 = \sigma_2 \theta'_3 \downarrow$ e $\theta'_3 = \{v_2 \mapsto v'_2 \oplus a\}$ $\sigma'_3 = \{x \mapsto v_1 \oplus v'_2, y \mapsto v_1, z \mapsto v'_2 \oplus a, w \mapsto b\}$
5. $\sigma'_3 \parallel \emptyset \parallel \Upsilon'_3$:

Note que σ'_3 é um unificador assimétrico de Γ , bastando testar o lado direito em cada equação em Γ , de fato,

- $(x \oplus a)\sigma'_3 = v_1 \oplus v'_2 \oplus a$
- $(w \oplus a \oplus y)\sigma'_3 = b \oplus a \oplus v_1$

6. $\sigma_2 \parallel \emptyset \parallel \Upsilon''_2$: Note que x tem um conflito com a em σ_2 , porém $(v_1, a), (v_2, a) \in \Upsilon''_2$ e portanto não é possível aplicar a regra ramificação não variável. Mais ainda não é possível aplicar nenhuma regra e portanto $\sigma_2 \parallel \emptyset \parallel \Upsilon''_2$ é um estado final

Representando essas aplicações de regras como uma árvore de estados, obtemos a seguinte árvore. Os estados colorido são estados finais, em vermelho os estados de falha e os azuis os estados de solução.



Instanciação (Inst): Estas regras serão utilizadas apenas quando não for possível mais aplicar as regras de ramificação e separação. O principal objetivo desta regra é remover conflitos entre termos simples s, t que são *ACUN*-unificáveis e remover variáveis suporte que estão em conflito. Esta regra é dividida em duas:

- **Decomposição:** Esta regra será utilizada quando houver conflitos entre termos simples s, t que tem o mesmo símbolo raiz, resultando em um conjunto completo L de unificadores para $s =^? t$ (Algoritmo Capítulo 3) Para cada unificador $\theta \in L$ é criado um novo ramo, tornando esta regra não determinística em relação às ramificações.

Decomposição:

$$\frac{\sigma \parallel \Upsilon \parallel \Delta}{\bigvee_{i=1}^n \sigma_i \parallel \Upsilon_i \parallel \Delta_i \bigvee \sigma \parallel \Upsilon \parallel \Delta'} \text{Dec}$$

Condições:

- Existe a designação $[x \mapsto s \oplus t \oplus S] \in \sigma$, onde s, t são termos simples, não-variáveis com $\text{raíz}(s) = \text{raíz}(t)$
- x tem um conflito com s em Γ e $(s, t) \notin \Delta$
- $\{\theta_1, \dots, \theta_n\}$ é um conjunto completo de ACUN-unificadores da equação $s =^? t$.
- $\sigma_i := \sigma\theta_i$, $\Upsilon_i := \Upsilon\theta_i$ e $\Delta_i := \Delta\theta_i$ para cada $i \in \{1, \dots, n\}$
- $\Delta' = \Delta \cup (s, t)$

- **Eliminação:** Esta regra será utilizada quando houver conflitos entre variáveis $x, y \in \text{Var}(\Gamma)$ e uma variável suporte v , simplesmente instanciando v para 0.

Eliminação

$$\frac{\sigma \parallel \Upsilon \parallel \Delta}{\sigma\theta \parallel \Upsilon\theta \parallel \Delta\theta} \text{Elim}$$

Condições:

- Existe designações $[x \mapsto v \oplus S], [y \mapsto v \oplus S'] \in \sigma$.
- S, S' são termos não vazios e v é uma variável suporte.
- Existe a equação $u =^\downarrow u' \in \Gamma$, tal que $x \oplus y$ é subtermo de v' .
- $\theta = \{v \mapsto 0\}$

Vamos definir agora o algoritmo \mathcal{J}_{AXO} para as etapas (3) e (4) que descrevemos na introdução

deste capítulo. Para isso utilizaremos uma pilha ¹ P para corrigir o problema da regra de inferência *decomposição* ser não determinística na quantidade de ramos gerados. Uma lista L será utilizada para armazenar os estados finais relevantes, isto é, os estados finais que tem \mathcal{Inst} não vazio.

Algoritmo 2: \mathcal{J}_{AXO}

Data: Um problema de unificação Γ , um estado inicial $\hat{\sigma} \parallel \emptyset \parallel \emptyset$ sobre Γ

Result: Lista L de estados finais de Γ

```

1 inicialização:  $P \leftarrow \text{new pilha}()$ ,  $L \leftarrow \text{new Lista}()$ ;
2  $P.\text{push}(\hat{\sigma} \parallel \emptyset \parallel \emptyset)$ ;
3 while  $P \neq \emptyset$  do
4    $\sigma \parallel \Upsilon \parallel \Delta \leftarrow P.\text{pop}()$ ;
5   if  $\sigma \parallel \Upsilon \parallel \Delta \implies_{\mathcal{J}_{AXO}} \bigvee_{i=1}^n \sigma_i \parallel \Upsilon_i \parallel \Delta_i$  then
6     for  $i = 1 \dots n$  do
7        $P.\text{push}(\sigma_i \parallel \Upsilon_i \parallel \Delta_i)$ ;
8     end
9   else
10    if Para cada  $u = \downarrow u' \in \Gamma$ ,  $u'\sigma$  é irreduzível then
11       $L.\text{add}(\sigma \parallel \Upsilon \parallel \Delta)$ 
12    end
13  end
14 end
15 return  $L$ 

```

Vamos enunciar o seguinte teorema da terminação deste algoritmo, pela sua complexidade técnica decidimos por apenas citar a demonstração que foi realizada Liu [18].

Teorema 4.3 (Terminação de \mathcal{J}_{AXO}). \mathcal{J}_{AXO} é terminante, isto é, em algum momento de sua execução a pilha P tem apenas estados finais.

Demonstração. Liu em sua tese [18], constrói uma medida μ dos estados válidos de \mathcal{J}_{AXO} para \mathbb{N}^6 , em que a cada aplicação de uma regra de inferência de \mathcal{J}_{AXO} a medida μ decresce com relação a relação noetheriana $>_{lex}$ de \mathbb{N}^6 .

¹Método *First-in Last-out* para inserção e remoção na pilha P

Para as regras *decomposição* e *ramificação variável* a prova em que a medida decresce tem um grau elevado de complexidade. \square

Teorema 4.4 (Correção de \mathcal{J}_{AXO}). *Se $L := \mathcal{J}_{AXO}(\Gamma, \sigma \parallel \emptyset \parallel \emptyset)$ então para cada $\sigma_i \parallel \Upsilon_i \parallel \Delta_i \in L$ temos que σ_i é um ACUN-unificador assimétrico de Γ que é uma instância de σ .*

Demonstração. A prova segue dos resultados estabelecidos no capítulo 5 e do algoritmo \mathcal{J}_{AXO} , pois escolhemos apenas os estados que σ_i é um ACUN-unificador assimétrico, e σ_i é uma instância de σ pela definição das regras de inferência de \mathcal{J}_{AXO} . \square

Teorema 4.5 (Completude de \mathcal{J}_{AXO}). *Se $L := \{\sigma_i \parallel \Upsilon_i \parallel \Delta_i\} = \mathcal{J}_{AXO}(\Gamma, \sigma \parallel \emptyset \parallel \emptyset)$ e δ um unificador assimétrico de Γ que é uma instância de σ então existe um estado $\sigma_i \parallel \Upsilon_i \parallel \Delta_i \in L$ tal que $\sigma_i \upharpoonright_{\text{var}(\Gamma)} \lesssim_{\oplus} \delta \upharpoonright_{\text{var}(\Gamma)}$*

Demonstração. A prova completa está no capítulo 5. \square

Exemplo 4.3. *Vamos aplicar o algoritmo \mathcal{J}_{AXO} no problema Γ com um ACUN-mgu σ obtido pelo algoritmo \mathcal{J}_{XORh} , isto é, $\Gamma = \{x \oplus y \oplus z =^\downarrow a, x \oplus z =^\downarrow x \oplus z, x \oplus a =^\downarrow x \oplus a, a \oplus f(b) =^\downarrow w \oplus f(y)\}$ em que $\sigma = \{x \mapsto y \oplus z \oplus a, w \mapsto a \oplus f(b) \oplus f(y)\}$. Assim obtemos o estado inicial, $\sigma \parallel \emptyset \parallel \emptyset$.*

1. $\sigma \parallel \emptyset \parallel \emptyset$: *observe que z é uma variável original e $z \in_{\oplus} x\sigma$, aplicando regra [Sep] com $\theta_1 = \{z \mapsto v_1\}$, obtemos $\sigma_1 \parallel \Upsilon_1 \parallel \Delta_1$, com $\Upsilon_1 = \emptyset$, $\Delta_1 = \emptyset$ e, $\sigma_1 = \sigma\theta_1 = \{x \mapsto v_1 \oplus y \oplus a, z \mapsto v_1, w \mapsto a \oplus f(b) \oplus f(y)\}$.*

$$\sigma \parallel \emptyset \parallel \emptyset \xrightarrow{\text{Sep}} \sigma_1 \parallel \emptyset \parallel \emptyset$$

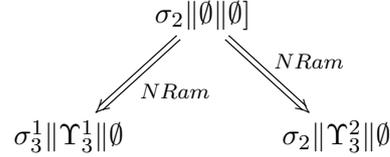
2. $\sigma_1 \parallel \emptyset \parallel \emptyset$: *$z \in_{\oplus} x\sigma_1$ e z uma variável original, então de forma análoga ao item 2 temos, $\Upsilon_2 = \emptyset$, $\Delta_2 = \emptyset$ e, $\sigma_2 \{x \mapsto v_1 \oplus v_2 \oplus a, z \mapsto v_1, y \mapsto v_2, w \mapsto f(b) \oplus f(v_2)\}$. Logo,*

$$\sigma_1 \parallel \emptyset \parallel \emptyset \xrightarrow{[\text{Sep}]} \sigma_2 \parallel \emptyset \parallel \emptyset$$

3. $\sigma_2 \parallel \emptyset \parallel \emptyset$: *x tem um conflito com a em σ_2 , pois a equação $x \oplus a =^\downarrow x \oplus a \in \Gamma$ e $x\sigma_2 =_{AC} a \oplus (v_1 \oplus v_2)$, então vamos aplicar a regra [NRam] escolhendo a variável suporte v_1 e $\theta_3^1 = \{v_1 \mapsto v_3 \oplus a\}$,*

obtendo dois estados $\sigma_3^1 \parallel \Upsilon_3^1 \parallel \Delta_3^1$ e $\sigma_3^2 \parallel \Upsilon_3^2 \parallel \Delta_3^2$, com, $\Upsilon_3^1 = \{(v_3, a)\}$, $\Delta_3^1 = \emptyset$, $\Upsilon_3^2 = \{(v_1, a)\}$, $\Delta_3^2 = \emptyset$, $\sigma_3^2 = \sigma_2$ e,

$$\sigma_3^1 = \sigma_2 \theta_3^1 = \{x \mapsto v_3 \oplus v_2, z \mapsto v_3 \oplus a, y \mapsto v_2, w \mapsto a \oplus f(b) \oplus f(v_2)\}$$



Vamos colocar $\sigma_2 \parallel \Upsilon_3^2 \parallel \emptyset$ na pilha P , isto é, $P = \{\sigma_2 \parallel \Upsilon_3^2 \parallel \emptyset\}$

4. $\sigma_3^1 \parallel \Upsilon_3^1 \parallel \emptyset$:

Como $x \oplus z = \downarrow x \oplus z \in \Gamma$ e $[x \mapsto v_2 \oplus v_3], [z \mapsto v_2] \in \sigma$ e $(v_2, v_3) \notin \Upsilon_3^1$ podemos aplicar a regra ramificação variável, com $\theta_4^1 = \{v_2 \mapsto v'_2 \oplus v_{23}, v_3 \mapsto v'_3 \oplus v_{23}\}$, obtendo dois estados $\sigma_4^1 \parallel \Upsilon_4^1 \parallel \Delta_4^1, \sigma_4^2 \parallel \Upsilon_4^2 \parallel \Delta_4^2$.

Assim, $\Upsilon_4^1 = \Upsilon_3^1 \theta_4^1 = \{(v'_3, a), (v_{23}, a)\} \cup A_2^3$, $\Upsilon_4^2 = \{(v_1, a), (v_2, v_3), (v_3, v_2)\}$, $\Delta_4^1 = \emptyset$, $\Delta_4^2 = \emptyset$, $\sigma_4^2 = \sigma_3^1$, e $\sigma_4^1 = \sigma_3^1 \theta_4^1$

$$\sigma_4^1 = \{x \mapsto v'_3 \oplus v'_2, z \mapsto v'_3 \oplus v_{23} \oplus a, y \mapsto v'_2 \oplus v_{23}, w \mapsto a \oplus f(b) \oplus f(v'_2 \oplus v_{23})\}$$

$$\sigma_3^1 \parallel \Upsilon_3^1 \parallel \emptyset \xrightarrow{VRam} \sigma_3^1 \parallel \Upsilon_4^2 \parallel \emptyset$$

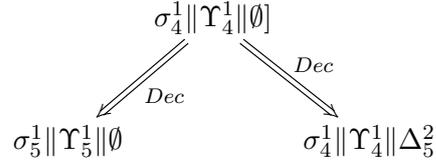
Vamos colocar $\sigma_3^1 \parallel \Upsilon_4^2 \parallel \emptyset$ na pilha, e portanto temos, $P = \{\sigma_3^1 \parallel \Upsilon_4^2 \parallel \emptyset, \sigma_2 \parallel \Upsilon_3^2 \parallel \emptyset\}$

5. $\sigma_4^1 \parallel \Upsilon_4^1 \parallel \emptyset$:

Observe que não é possível mais aplicar nenhuma regra de ramificação e portanto podemos aplicar a regra decomposição pois $a \oplus f(b) = \downarrow w \oplus f(y) \in \Gamma$ com $f(y) \sigma_4^1 = f(v'_2 \oplus v_{23})$ e portanto w tem um conflito com $f(v'_2 \oplus v_{23})$ em σ_4^1 . Seja $\theta_5^1 = \{v'_2 \mapsto v_{23} \oplus b\}$, θ_5^1 é um ACUN-unificador mais geral de $f(b) = ? f(v'_2 \oplus v_{23})$. Obtemos dois novos estados, $\sigma_5^1 \parallel \Upsilon_5^1 \parallel \emptyset, \sigma_5^2 \parallel \Upsilon_5^2 \parallel \Delta_5^2$, com $\sigma_5^1 = \sigma_4^1 \theta_5^1$, $\sigma_5^2 = \sigma_4^1$, $\Delta_5^2 = \{f(b) \neq f(v'_2 \oplus v_{23})\}$, $\Upsilon_5^2 = \Upsilon_4^1$ e,

$$\Upsilon_5^1 = \Upsilon_4^1 \theta_5^1 = \left\{ \begin{array}{ccccc} (v'_3, a) & (v_{23}, a) & (v'_2, v_{23}) & (v_{23}, b) & (v_{23}, v_{23}) \\ (v'_2, v'_3) & (v'_3, b) & (v'_3, v_{23}) & (v'_3, v_{23}) & (v_{23}, v'_3) \end{array} \right\} \quad (4.2)$$

$$\sigma_5^1 = \{x \mapsto v'_3 \oplus v_{23} \oplus b, y \mapsto b, z \mapsto v'_3 \oplus v_{23} \oplus a, w \mapsto a\}$$



Obtendo a pilha $P = \{\sigma_4^1 \parallel \Upsilon_4^1 \parallel \Delta_5^2, \sigma_3^1 \parallel \Upsilon_4^2 \parallel \emptyset, \sigma_2 \parallel \Upsilon_3^2 \parallel \emptyset\}$

6. $\sigma_5^1 \parallel \Upsilon_5^1 \parallel \emptyset$: vamos aplicar única regra possível [Elim] sobre a variável v'_3 , logo sendo $\theta_6 = \{v'_3 \mapsto 0\}$ temos $\sigma_6 = \sigma_5^1 \theta_6$, $\Upsilon_6 = \Upsilon_5^1 \theta_6$ e o estado $\sigma_6 \parallel \Upsilon_6 \parallel \emptyset$, então: $\sigma_6 = \{x \mapsto v_{23} \oplus b, z \mapsto v_{23} \oplus a, y \mapsto b, w \mapsto a\}$ e

$$\Upsilon_6 = \left\{ \begin{array}{ccccc} (v'_3, a) & (v_{23}, a) & (v'_2, v_{23}) & (v_{23}, b) & (v_{23}, v_{23}) \\ (v'_2, 0) & (v'_3, b) & (v'_3, v_{23}) & (v'_3, v_{23}) & (v_{23}, 0) \end{array} \right\}$$

Logo, $\sigma_5^1 \parallel \Upsilon_5^1 \parallel \emptyset \xrightarrow{\text{Elim}} \sigma_6 \parallel \Upsilon_6 \parallel \emptyset$.

Tomando $\sigma_7 = \{x \mapsto b, z \mapsto a, y \mapsto b, w \mapsto a\}$ e

$$\Upsilon_7 = \left\{ \begin{array}{ccccc} (v'_3, a) & (v_{23}, a) & (v'_2, 0) & (v_{23}, b) & (v_{23}, 0) \\ (v'_2, 0) & (v'_3, b) & (v'_3, 0) & (v'_3, 0) & (v_{23}, 0) \end{array} \right\}$$

obtemos, $\sigma_6 \parallel \Upsilon_6 \parallel \emptyset \xrightarrow{\text{Elim}} \sigma_7 \parallel \Upsilon_7 \parallel \emptyset$.

Ainda temos a pilha $P = \{\sigma_4^1 \parallel \Upsilon_4^1 \parallel \Delta_5^2, \sigma_3^1 \parallel \Upsilon_4^2 \parallel \emptyset, \sigma_2 \parallel \Upsilon_3^2 \parallel \emptyset\}$, esses estados da pilha podem ainda gerar novos estados de solução.

Observe que de fato σ_7 é idempotente e um unificador assimétrico de Γ que não é equivalente a σ pois usamos as regras de decomposição e a eliminação

Capítulo 5

Correção e Completude de \mathcal{J}_{AXO}

Este capítulo consiste de demonstrações de lemas e proposições técnicas necessárias para prova de correção e completude do algoritmo \mathcal{J}_{AXO} . Muitas dessas provas são inéditas e/ou alternativas às provas abordadas em [18].

5.1 Idempotência das Soluções e Regularidade dos Estados Válidos de \mathcal{J}_{AXO}

Nesta seção provaremos resultados importantes sobre os estados válidos de \mathcal{J}_{AXO} para um problema de ACUN-unificação Γ , dentre eles, garantir que cada estado válido $\sigma \parallel \Upsilon \parallel \Delta$, σ seja idempotente e $Dom(\sigma) \cap Var(\Upsilon, \Delta) = \emptyset$, pois precisamos que as soluções de \mathcal{J}_{AXO} sejam idempotentes e para provarmos a correção e completude, iremos utilizar o Teorema 4.2, que é uma simplificação para pertinência no conjunto $Inst$.

Lema 5.1. *Seja $\sigma \parallel \Upsilon \parallel \Delta$ um estado válido de \mathcal{J}_{AXO} .*

1. *Se $\sigma \parallel \Upsilon \parallel \Delta \implies_{Sep} \sigma\theta \parallel \Upsilon\theta \parallel \Delta\theta$ então $\sigma|_{Var(\Gamma)} \approx_{AC} \sigma\theta|_{Var(\Gamma)}$.*
2. *Se $\sigma \parallel \Upsilon \parallel \Delta \implies_{Sep} \sigma\theta \parallel \Upsilon\theta \parallel \Delta\theta$ e σ for idempotente então $\sigma\theta$ é idempotente.*

Demonstração. 1. Por hipótese, $\theta = \{y \mapsto v \oplus S\}$, onde v é uma variável nova. Defina a substituição α da seguinte forma: $\alpha := \{v \mapsto y \oplus S\}$.

Observe que $\theta\alpha|_{\mathcal{V}\setminus\{v\}} = id_{\mathcal{V}}$, já que para uma variável $w \notin \{y, v\}$ temos que $w\theta\alpha \downarrow = w$ e para y temos $y\theta\alpha \downarrow =_{AC} (v \oplus S)\alpha \downarrow =_{AC} (y \oplus S \oplus S) \downarrow = y$.

Logo, por v ser uma variável nova, obtemos que $v \notin \mathcal{V}ar(\mathcal{I}m(\sigma))$ e então, para todo $x \in \mathcal{V}ar(\Gamma)$ temos $x\sigma\theta\alpha \downarrow =_{AC} x\sigma \downarrow$. Assim $\sigma\theta|_{\mathcal{V}ar(\Gamma)} \lesssim_{AC} \sigma|_{\mathcal{V}ar(\Gamma)}$, donde segue que $\sigma|_{\mathcal{V}ar(\Gamma)} \approx_{AC} \sigma\theta|_{\mathcal{V}ar(\Gamma)}$.

2. Por hipótese $\theta = \{y \mapsto v \oplus S\}$ onde v é uma variável nova. Vamos mostrar que $\sigma\theta = \theta\sigma\theta$:

- Tome $w \in \mathcal{V} \setminus \{y\}$, então $w\theta = w$, ou ainda, $w\theta\sigma\theta = w\sigma\theta$.
- Para y temos: $y\theta\sigma\theta = (v \oplus S)\sigma\theta = v\sigma\theta \oplus S\sigma\theta$.

Como σ é idempotente e S é um subtermo de $x\sigma \in \mathcal{I}m(\sigma)$ temos $S\sigma = S$. Pelas condições da regra de separação: v é uma variável nova, o que implica que $v\sigma\theta = v$; e $y \notin \mathcal{V}ar(S)$ o que implica que $S\theta = S$. Assim $y\theta\sigma\theta = v \oplus S = y\sigma\theta$,

Logo, $\sigma\theta\sigma\theta = \sigma\sigma\theta = \sigma\theta$.

□

Lema 5.2. *Seja $\sigma \parallel \Upsilon \parallel \Delta$ um estado válido.*

1. *Se $\sigma \parallel \Upsilon \parallel \Delta \implies_{NRam} \sigma\theta \parallel \Upsilon'\theta \parallel \Delta\theta \vee \sigma \parallel \Upsilon'' \parallel \Delta$ então $\sigma|_{\mathcal{V}ar(\Gamma)} \approx_{AC} \sigma\theta|_{\mathcal{V}ar(\Gamma)}$.*
2. *Se $\sigma \parallel \Upsilon \parallel \Delta \implies_{NRam} \sigma\theta \parallel \Upsilon'\theta \parallel \Delta\theta \vee \sigma \parallel \Upsilon'' \parallel \Delta$ e σ for idempotente então $\sigma\theta$ é idempotente.*

Demonstração. 1. Por hipótese, $\theta = \{v \mapsto v' \oplus s\}$, onde v' é uma variável nova em $\sigma \parallel \Upsilon \parallel \Delta$. Defina $\alpha = \{v' \mapsto v \oplus S\}$. Analogamente ao Lema 5.1, pode-se provar que $\sigma\theta|_{\mathcal{V}ar(\Gamma)} \approx_{AC} \sigma|_{\mathcal{V}ar(\Gamma)}$.

2. Por hipótese, $\theta = \{v \mapsto v' \oplus s\}$, onde v' é uma variável nova em $\sigma \parallel \Upsilon \parallel \Delta$. Vamos provar que $\theta\sigma\theta = \sigma\theta$.

De fato, como $v \notin \mathcal{V}ar(s)$, σ é idempotente e v, s são subtermos de $x\sigma \in \mathcal{V}ar(\mathcal{I}m(\sigma))$ e v' é uma variável nova, obtemos: $v\theta\sigma\theta \downarrow = (v' \oplus s)\sigma\theta \downarrow = v'\sigma\theta \oplus s\sigma\theta = v' \oplus s = v\sigma\theta$.

Para qualquer outra variável $w \neq v$ obtemos $w\theta = w$ e então $w\theta\sigma\theta = w\sigma\theta$.

Logo, para w uma variável qualquer temos que $w\sigma\theta\sigma\theta = w\sigma\sigma\theta = w\sigma\theta$, e o resultado segue.

□

Lema 5.3. *Seja $\sigma \parallel \Upsilon \parallel \Delta$ um estado válido de \mathcal{J}_{AXO}*

1. *Se $\sigma \parallel \Upsilon \parallel \Delta \implies_{VRam} \sigma \theta \parallel \Upsilon' \theta \parallel \Delta \theta \vee \sigma \parallel \Upsilon'' \parallel \Delta$, então $\sigma|_{\mathcal{V}ar(\Gamma)} \approx_{AC} \sigma \theta|_{\mathcal{V}ar(\Gamma)}$.*
2. *Se $\sigma \parallel \Upsilon \parallel \Delta \implies_{VRam} \sigma \theta \parallel \Upsilon' \theta \parallel \Delta \theta \vee \sigma \parallel \Upsilon'' \parallel \Delta$ e σ é idempotente então $\sigma \theta$ é idempotente.*

Demonstração. 1. Por hipótese, $\theta = \{v_1 \mapsto v'_1 \oplus v_{12}, v_2 \mapsto v'_2 \oplus v_{12}\}$. Considere a substituição

$$\alpha := \{v'_1 \mapsto v_1 \oplus v_{12}, v'_2 \mapsto v_2 \oplus v_{12}\}, \text{ então } \theta \alpha = \{v'_1 \mapsto v_1 \oplus v_{12}, v'_2 \mapsto v_2 \oplus v_{12}\}.$$

Como v'_1, v'_2, v'_{12} são variáveis novas, para cada $w \in \mathcal{V}ar(\Gamma)$, tem-se que $v'_1, v'_2, v'_{12} \notin \mathcal{V}ar(w\sigma)$, o que implica que $w\sigma\theta\alpha \downarrow_{AC} w\sigma \downarrow$. Assim obtemos $\sigma\theta|_{\mathcal{V}ar(\Gamma)} \approx_{AC} \sigma|_{\mathcal{V}ar(\Gamma)}$.

2. Por hipótese, $\theta = \{v_1 \mapsto v'_1 \oplus v_{12}, v_2 \mapsto v'_2 \oplus v_{12}\}$. Vamos mostrar que $\theta\sigma\theta = \sigma\theta$:

Por hipótese σ é idempotente, $v_1, v_2 \in \mathcal{V}ar(\mathcal{I}m(\sigma))$ e v'_1, v'_2, v_{12} são variáveis novas então $v'_1, v'_2, v_{12} \notin \mathcal{D}om(\sigma)$. Observe que

$$v_1\theta\sigma\theta \downarrow = (v'_1 \oplus v_{12})\sigma\theta \downarrow = v'_1 \oplus v_{12} = v_1\theta \downarrow = v_1\sigma\theta \downarrow$$

$$v_2\theta\sigma\theta \downarrow = (v'_2 \oplus v_{12})\sigma\theta \downarrow = v'_2 \oplus v_{12} = v_2\theta \downarrow = v_2\sigma\theta \downarrow$$

Seja $w \neq v_1, v_2$ uma variável, então $w\theta = w$, o que implica que, $w\theta\sigma\theta = w\sigma\theta$ e o resultado segue. □

Lema 5.4. 1. *Se $\sigma \parallel \Upsilon \parallel \Delta \implies_{Raux} \sigma \theta \parallel \Upsilon' \theta \parallel \Delta \theta \vee \sigma \parallel \Upsilon'' \parallel \Delta$ então $\sigma|_{\mathcal{V}ar(\Gamma)} \approx_{AC} \sigma \theta|_{\mathcal{V}ar(\Gamma)}$.*

2. *Se $\sigma \parallel \Upsilon \parallel \Delta \implies_{Raux} \sigma \theta \parallel \Upsilon' \theta \parallel \Delta \theta \vee \sigma \parallel \Upsilon'' \parallel \Delta$ e σ for idempotente então $\sigma \theta$ é idempotente.*

Demonstração. Análogo ao caso da ramificação não variável. □

Lema 5.5. *Se $\sigma \parallel \Upsilon \parallel \Delta \implies_{Dec} \bigvee_{i=1}^n \sigma_i \parallel \Upsilon_i \parallel \Delta_i \vee \sigma \parallel \Upsilon \parallel \Delta'$ e σ é idempotente então, para cada $i \in \{1, \dots, n\}$ tem-se que σ_i é idempotente.*

Demonstração. Seja $\{\theta_1, \dots, \theta_n\}$ um conjunto completo de ACUN-unificadores de $s =^? t$, podemos supor sem perda de generalidade que, para cada $i \in \{1, \dots, n\}$ temos que $\mathcal{V}ar(\mathcal{I}m(\theta_i)) \cap \mathcal{D}om(\sigma) = \emptyset$.

Vamos mostrar que $x\theta_i\sigma\theta_i \downarrow = x\sigma\theta_i \downarrow$:

- Tome $x \in \text{Dom}(\theta_i)$. Como $\text{Dom}(\theta_i) \subseteq \text{Var}(s) \cup \text{Var}(t) \subseteq \text{Var}(\mathcal{I}m(\sigma))$ e σ é idempotente, temos que $x\sigma\theta_i \downarrow = x\theta_i \downarrow = x\theta_i\sigma \downarrow$.

Aplicando θ_i de ambos os lados, temos $x\theta_i\sigma\theta_i \downarrow = x\sigma\theta_i\theta_i \downarrow$, e por θ_i ser idempotente, obtemos $x\theta_i\sigma\theta_i \downarrow = x\sigma\theta_i \downarrow$.

- se $x \notin \text{Dom}(\theta_i)$ então $x\theta_i = x$ e, portanto $x\theta_i\sigma\theta_i \downarrow = x\sigma\theta_i \downarrow$.

Portanto $\sigma\theta_i\sigma\theta_i = \sigma\sigma\theta_i = \sigma\theta_i$. □

Lema 5.6. Se $\sigma \parallel \Upsilon \parallel \Delta \xRightarrow{Elim} \sigma\theta \parallel \Upsilon\theta \parallel \Delta\theta$ e σ é idempotente, então $\sigma\theta$ é idempotente.

Demonstração. É trivial pois $\theta = \{v \mapsto 0\}$ e portanto $\sigma\theta$ é a substituição σ removendo todas as ocorrências da variável v na $\mathcal{I}m(\sigma)$, portanto $\sigma\theta$ continua idempotente. □

Teorema 5.1 (Idempotência). Se $\sigma \parallel \Upsilon \parallel \Delta$ é um estado válido de \mathcal{J}_{AXO} então σ é idempotente.

Demonstração. Vamos provar por indução sobre a quantidade de regras de inferências de \mathcal{J}_{AXO} que foram utilizadas.

Hipótese de indução: Seja $\sigma \parallel \Upsilon \parallel \Delta$ obtido com $n \geq 0$ aplicações de regras de inferência sobre um estado inicial, então σ é idempotente.

Base da indução: $n = 0$.

O estado inicial $\sigma \parallel \emptyset \parallel \emptyset$ é o único estado válido obtido por zero aplicações de regras de \mathcal{J}_{AXO} , onde $\sigma \in \mathcal{U}_{ACUN}$ e \mathcal{U}_{ACUN} é um conjunto completo de unificadores de Γ , então σ é idempotente.

Passo Indutivo. seja $\sigma' \parallel \Upsilon' \parallel \Delta'$ um estado válido obtido com $n + 1$ aplicações das regras de \mathcal{J}_{AXO} sobre um estado inicial. Então existe $\sigma \parallel \Upsilon \parallel \Delta$ obtido com n aplicações das regras tal que $\sigma \parallel \Upsilon \parallel \Delta \xRightarrow{\mathcal{J}_{AXO}} \sigma' \parallel \Upsilon' \parallel \Delta'$ e portanto, por HI, σ é idempotente. Pelos Lemas 5.1 a 5.5, σ' é idempotente. □

Teorema 5.2 (Regularidade). Se $\sigma \parallel \Upsilon \parallel \Delta$ é um estado válido de \mathcal{J}_{AXO} então $\text{Dom}(\sigma) \cap \text{Var}(\Upsilon, \Delta) = \emptyset$.

Demonstração. Como $\sigma \parallel \Upsilon \parallel \Delta$ é um estado válido, existe um estado inicial $\hat{\sigma} \parallel \emptyset \parallel \emptyset$ e um número natural $n \in \mathbb{N}$ tal que $\hat{\sigma} \parallel \emptyset \parallel \emptyset \xRightarrow{\mathcal{J}_{AXO}}^n \sigma \parallel \Upsilon \parallel \Delta$, vamos provar por indução sobre $n \in \mathbb{N}$.

Hipótese de indução: Seja $\sigma \parallel \Upsilon \parallel \Delta$ obtido com $n \geq 0$ aplicações de regras de inferência sobre o estado inicial $\hat{\sigma} \parallel \emptyset \parallel \emptyset$, então $\text{Dom}(\sigma) \cap \text{Var}(\Upsilon, \Delta) = \emptyset$.

Base da indução: Os únicos estados válidos obtidos com 0 aplicações de regras são o estados iniciais, e o resultado segue trivialmente.

Passo Indutivo. Suponha que $\hat{\sigma} \parallel \emptyset \parallel \emptyset \xRightarrow{\mathcal{J}_{AXO}^{n+1}} \sigma_1 \parallel \Upsilon_1 \parallel \Delta_1$. Portanto existe um estado $\sigma \parallel \Upsilon \parallel \Delta$ tal que, $\hat{\sigma} \parallel \emptyset \parallel \emptyset \xRightarrow{\mathcal{J}_{AXO}^n} \sigma \parallel \Upsilon \parallel \Delta \xRightarrow{\mathcal{J}_{AXO}} \sigma_1 \parallel \Upsilon_1 \parallel \Delta_1$. Por HI, $\text{Dom}(\sigma) \cap \text{Var}(\Upsilon, \Delta) = \emptyset$. Observe que em cada regra de inferência, considerando os ramos não triviais, temos $\sigma_1 = \sigma\theta$, onde θ é uma substituição idempotente com $\text{Dom}(\theta) \subseteq \text{Var}(\text{Im}(\sigma))$ e $\text{Var}(\text{Im}(\theta)) \cap \text{Dom}(\sigma) = \emptyset$, pois σ é idempotente e as variáveis ocorrendo em $\text{Var}(\text{Im}(\theta))$ são variáveis novas no estado $\sigma \parallel \Upsilon \parallel \Delta$ ou são variáveis ocorrendo em $\text{Var}(\text{Im}(\sigma))$, pela própria definição das regras.

Nas regras [Sep] e [Inst], temos que $\Upsilon_1 = \Upsilon\theta$ e $\Delta_1 = \Delta\theta$ e como:

$$\text{Var}(\Upsilon\theta) \subseteq (\text{Var}(\Upsilon) \setminus \text{Dom}(\theta)) \cup \text{Var}(\text{Im}(\theta))$$

$$\text{Var}(\Delta\theta) \subseteq (\text{Var}(\Delta) \setminus \text{Dom}(\theta)) \cup \text{Var}(\text{Im}(\theta))$$

Temos as seguintes inclusões:

$$\text{Dom}(\sigma\theta) \cap \text{Var}(\Upsilon\theta) \subseteq \text{Dom}(\sigma\theta) \cap [(\text{Var}(\Upsilon) \setminus \text{Dom}(\theta)) \cup \text{Var}(\text{Im}(\theta))]$$

$$\subseteq (\text{Dom}(\sigma) \cup \text{Dom}(\theta)) \cap [(\text{Var}(\Upsilon) \setminus \text{Dom}(\theta)) \cup \text{Var}(\text{Im}(\theta))]$$

$$\text{Dom}(\sigma\theta) \cap \text{Var}(\Delta\theta) \subseteq \text{Dom}(\sigma\theta) \cap [(\text{Var}(\Delta) \setminus \text{Dom}(\theta)) \cup \text{Var}(\text{Im}(\theta))]$$

$$\subseteq (\text{Dom}(\sigma) \cup \text{Dom}(\theta)) \cap [(\text{Var}(\Delta) \setminus \text{Dom}(\theta)) \cup \text{Var}(\text{Im}(\theta))]$$

Portanto unindo os conjuntos das inclusões acima obtemos:

$$\text{Dom}(\sigma\theta) \cap \text{Var}(\Upsilon\theta, \Delta\theta) \subseteq \text{Dom}(\sigma\theta) \cap [(\text{Var}(\Upsilon, \Delta) \setminus \text{Dom}(\theta)) \cup \text{Var}(\text{Im}(\theta))]$$

$$\subseteq (\text{Dom}(\sigma) \cup \text{Dom}(\theta)) \cap [(\text{Var}(\Upsilon, \Delta) \setminus \text{Dom}(\theta)) \cup \text{Var}(\text{Im}(\theta))] = \emptyset$$

Os ramos triviais são os que $\sigma_1 = \sigma$, e portanto, o resultado é trivial pois $\Upsilon_1 = \Upsilon$ e $\Delta_1 = \Delta \cup (s, t)$ onde s, t são subtermos de algum termo de $\text{Im}(\sigma)$.

Para a regra *ramificação* a demonstração é análoga, com a única diferença que Υ_1 tem algumas variáveis novas.

□

Lema 5.7. *Seja $\sigma \parallel \Upsilon \parallel \Delta$ um estado válido de \mathcal{J}_{AXO} . Se existir $u =^\downarrow u'[s \oplus t]_p \in \Gamma$, tal que $p \in \text{Pos}(u')$, s, t são termos simples não variáveis onde $t\sigma =_{\oplus} s\sigma$ então $\text{Inst}(\Gamma, \sigma, \Upsilon, \Delta) = \emptyset$.*

Demonstração. Note que $u'\sigma$ é redutível, pois $s\sigma \oplus t\sigma$ é redutível.

Tome γ uma substituição qualquer, por s, t serem termos simples e não variáveis então $s\sigma, t\sigma$ são termos simples e não variáveis. Portanto $(s\sigma\gamma \oplus t\sigma\gamma) \downarrow_{=AC} (s\sigma \oplus t\sigma)\gamma \downarrow = 0\gamma = 0$, isto é, $s\sigma\gamma \oplus t\sigma\gamma$ é redutível, implicando que $u'\sigma\gamma$ é redutível, e então $\sigma\gamma$ não é um unificador assimétrico de Γ , equivalentemente, $\sigma\gamma|_{\text{Var}(\Gamma)} \notin \text{Inst}(\Gamma, \sigma, \Upsilon, \Delta)$ e assim $\text{Inst}(\Gamma, \sigma, \Upsilon, \Delta) = \emptyset$. \square

Lema 5.8. *Seja $\sigma \parallel \Upsilon \parallel \Delta$ um estado válido de \mathcal{J}_{AXO} . Então σ satisfaz Υ e Δ .*

Demonstração. Pelo Teorema 5.2 temos $\text{Dom}(\sigma) \cap \text{Var}(\Upsilon, \Delta) = \emptyset$.

- Tome $(v, t) \in \Upsilon$, então $v = v\sigma$ e $t = t\sigma$. Observe que se $v = 0$ ou $t = 0$ temos que $v\sigma = 0$ ou $t\sigma = 0$ e portanto σ satisfaz (v, t) . Suponha que $v \neq 0$ e $t \neq 0$, então $v \oplus t$ está em sua forma normal e portanto $v\sigma \downarrow \oplus t\sigma \downarrow$ está em sua forma normal, obtendo que σ satisfaz (v, t) .
- Tome $(s, t) \in \Delta$, então temos que $s\sigma = s$, $t\sigma = t$ e $s \oplus t$ está em sua forma normal e portanto $(s \oplus t) \downarrow \neq 0$, equivalentemente, $(s\sigma \oplus t\sigma) \downarrow \neq 0$ e portanto σ satisfaz Δ .

Portanto σ satisfaz Υ e Δ . \square

Lema 5.9. *Seja $\sigma \parallel \Upsilon \parallel \Delta$ um estado final de \mathcal{J}_{AXO} . Se σ não é um unificador assimétrico de Γ satisfazendo as seguintes condições:*

1. Existe $[x \mapsto s \oplus T] \in \sigma|_{\text{Var}(\Gamma)}$
2. Existe $u =^\downarrow u'[x \oplus t]_p \in \Gamma$, onde $p \in \text{Pos}(u')$
3. s, t são termos simples não variáveis tais que $t\sigma \downarrow_{=AC} s$

Então valem as seguintes afirmações:

- a. Para cada $v \in_{\oplus} T$, tem-se que $(v, s) \in \Upsilon$ ou $v \in \text{Var}(s)$.
- b. Para cada termos simples $t' \in_{\oplus} T$ tal que $\text{raíz}(t') = \text{raíz}(s)$, então $(s, t') \in \Delta$

Demonstração. Vamos supor σ como na hipótese, portanto x tem um conflito com s em σ .

- a. Tome $v \in_{\oplus} T$ uma variável suporte. Suponha por absurdo que $(v, s) \notin \Upsilon$ e $v \notin \mathcal{V}ar(s)$ então podemos aplicar a regra de inferência *ramificação não variável* (NRam), que é uma contradição pois $\sigma \parallel \Upsilon \parallel \Delta$ é um estado final de \mathcal{J}_{AXO} .
- b. Tome $t' \in_{\oplus} T$ um termo simples e não variável com $raíz(t') = raíz(s)$. Suponha por absurdo, que $(s, t') \notin \Delta$, então podemos aplicar a regra de *decomposição* (Dec), que é uma contradição pois $\sigma \parallel \Upsilon \parallel \Delta$ é um estado final de \mathcal{J}_{AXO} .

□

Lema 5.10. *Seja $\sigma \parallel \Upsilon \parallel \Delta$ um estado final de \mathcal{J}_{AXO} . Se σ não é um unificador assimétrico de Γ satisfazendo as seguintes condições:*

1. *Existem $[x \mapsto s \oplus T] \in \sigma|_{\mathcal{V}ar(\Gamma)}$*
2. *Existe $u =_{\downarrow} u'[x \oplus y]_p \in \Gamma$, onde $p \in \mathcal{P}os(u')$*
3. *s é um termos simples e $y \in \mathcal{V}ar(\Gamma)$ tal que $y\sigma \downarrow =_E s \oplus S$*

Então vale as seguintes afirmações:

- a. *Para cada $v \in_{\oplus} S \oplus T$, $(v, s) \in \Upsilon$ ou $v \in \mathcal{V}ar(s)$.*
- b. *Para cada termo simples não variável $t \in_{\oplus} S \oplus T$ tal que $raíz(t) = raíz(s)$, então $(s, t) \in \Delta$*
- c. *Se $s = v$ uma variável suporte então T é um termo vazio ou S é um termo vazio, isto é, $x\sigma = v$ ou $y\sigma = v$.*

Demonstração. Vamos supor σ como na hipótese, portanto x, y tem um conflito com s em σ . Sem perda de generalidade, vamos analisar apenas para $v \in_{\oplus} T$ e $t \in_{\oplus} T$

1. s é um termo simples não variável:
 - a. Tome $v \in_{\oplus} T$ uma variável suporte. Suponha por absurdo que $(v, s) \notin \Upsilon$ e $v \notin \mathcal{V}ar(s)$ então podemos aplicar a regra *ramificação auxiliar* (ARam), que é uma contradição pois $\sigma \parallel \Upsilon \parallel \Delta$ é um estado final de \mathcal{J}_{AXO} .

b. Tome $t \in_{\oplus} T$ um termo simples e não variável, com $raíz(t) = raíz(s)$. Suponha por absurdo, que $(s, t) \notin \Delta$ então podemos aplicar a regra *decomposição*(Dec) que é uma contradição pois $\sigma \parallel \Upsilon \parallel \Delta$ é um estado final de \mathcal{J}_{AXO} .

2. $s = v$ é uma variável:

Então v não é uma variável original, pois caso $v \in \mathcal{Var}(\Gamma)$ temos que é possível aplicar a regra *separação*, que é uma contradição, então v é uma variável suporte.

a. Suponha por absurdo que exista uma variável suporte $v_2 \in_{\oplus} T$ tal que $(v, v_2) \notin \Upsilon$ e $v \neq v_2$, isto é, $(v, v_2) \notin \Upsilon$ e $v \notin \mathcal{Var}(v_2) = \{v_2\}$. Portanto é possível aplicar a regra *ramificação variável*, que é uma contradição, então $v = v_2$ ou $(v, v_2) \in \Upsilon$. Como $v \oplus T$ está em sua forma normal, temos que $v \neq v_2$ logo $(v, v_2) \in \Upsilon$ para toda variável suporte $v_2 \in_{\oplus} T$

c. Suponha por absurdo S e T não são termos não vazios, como $\sigma \parallel \Upsilon \parallel \Delta$ é um estado final, em particular não é possível mais aplicar a regra *ramificação*. Portanto podemos aplicar a regra *instanciação* do tipo *eliminação*, que é uma contradição, portanto S é um termo vazio ou T é um termo vazio.

□

Lema 5.11. *Seja $\sigma \parallel \Upsilon \parallel \Delta$ um estado final de \mathcal{J}_{AXO} . Se existe uma equação assimétrica $u =^{\downarrow} u' \in \Gamma$ tal que $u'\sigma$ é redutível então $\mathcal{Inst}(\Gamma, \sigma, \Upsilon, \Delta) = \emptyset$.*

Demonstração. Suponha por absurdo, que exista um $\delta \in \mathcal{Inst}(\Gamma, \sigma, \Upsilon, \Delta)$, então δ é um unificador assimétrico de Γ e existe uma substituição γ tal que $\delta = \sigma\gamma|_{\mathcal{Var}(\Gamma)}$ com $\sigma\gamma$ é idempotente satisfazendo Υ e Δ .

Por hipótese existe $u =^{\downarrow} u' \in \Gamma$ tal que $u'\sigma$ é redutível, portanto existem uma posição $p \in \mathcal{Pos}(u')$ e termos simples s, s' tais que $u' = u'[s' \oplus t']_p$ e $s\sigma \oplus s'\sigma$ é redutível.

Como supomos que $\mathcal{Inst}(\Gamma, \sigma, \Upsilon, \Delta) \neq 0$, pelo Lema 5.7 temos que s ou s' é uma variável, portanto existem dois possíveis casos.

1. Se s é um termos simples não variável e $s' = x \in \mathcal{Var}(\Gamma)$, então:

Neste caso temos $u =^{\downarrow} u'[x \oplus s]_p \in \Gamma$, $[x \mapsto t \oplus T] \in \sigma|_{\mathcal{Var}(\Gamma)}$ e $s\sigma =_{\oplus} t$. E como σ não é

um unificador assimétrico de Γ , que satisfaz as condições 1, 2 e 3 do Lema 5.9, portanto vale as afirmações *a* e *b* do Lema 5.9.

Note que $\sigma\gamma$ é uma substituição idempotente que satisfaz Υ , Δ e $\sigma\gamma$ é um unificador assimétrico de Γ , portanto $x\sigma\gamma \oplus s\sigma\gamma =_{\oplus} x\sigma\gamma \oplus t\gamma$ é irreduzível, implicando que $t\gamma \notin_{\oplus} x\sigma\gamma$.

Porém $x\sigma\gamma = (t \oplus T)\gamma \downarrow = (t\gamma \oplus T\gamma) \downarrow = (t\sigma\gamma \oplus T\sigma\gamma) \downarrow$, e como $t\sigma\gamma \notin_{\oplus} x\sigma\gamma$ então tem que existir algum termo simples $t' \in_{\oplus} T$ tal que $t'\sigma\gamma \downarrow =_{AC} t\sigma\gamma \oplus T'$. Existem dois possíveis casos:

- $t' = v \in_{\oplus} T$ uma variável suporte:
Pelo Lema 5.9, $(v, t) \in \Upsilon$ ou $v \in \mathcal{V}ar(t)$ e como $v\sigma\gamma =_{AC} t\sigma\gamma \oplus T'$ temos que $v \notin \mathcal{V}ar(t)$, logo $(v, t) \in \Upsilon$, que é uma contradição pois $v\sigma\gamma \downarrow \oplus t\sigma\gamma \downarrow$ é redutível e $\sigma\gamma$ satisfaz Υ .
- t' é não variável: Então novamente pelo Lema 5.9 temos que $(t, t') \in \Delta$ que é uma contradição pois $t\sigma\gamma \downarrow =_{AC} t'\sigma\gamma \downarrow$ e $\sigma\gamma$ satisfaz Δ .

2. Se $s, s' \in \mathcal{V}ar(\Gamma)$ de uma forma análoga obtemos que seria possível aplicar uma das regras *VRam*, *ARam*, *Dec* ou *Elim*, e pelo Lema 5.10 obtemos uma contradição.

Logo, $\mathcal{I}nst(\Gamma, \sigma, \Upsilon, \Delta) = \emptyset$. □

5.2 Correção e Completude

Neste capítulo iremos provar primeiro que a cada aplicação de regras de inferência de \mathcal{J}_{AXO} sobre um estado válido as soluções do estado não se perdem, onde se $\sigma \parallel \Upsilon \parallel \Delta$ é um estado válido então dizemos que suas soluções são $\mathcal{I}nst(\Gamma, \sigma, \Upsilon, \Delta)$.

Lema 5.12. *Se $\sigma \parallel \Upsilon \parallel \Delta \implies_{Sep} \sigma\theta \parallel \Upsilon\theta \parallel \Delta\theta$, então $\mathcal{I}nst(\Gamma, \sigma, \Upsilon, \Delta) \subseteq_{\alpha} \mathcal{I}nst(\Gamma, \sigma\theta, \Upsilon\theta, \Delta\theta)$.*

Demonstração. Suponha $\sigma \parallel \Upsilon \parallel \Delta \implies_{Sep} \sigma\theta \parallel \Upsilon\theta \parallel \Delta\theta$ então existe $[x \mapsto y \oplus S \oplus T] \in \sigma$ com $\theta = \{y \mapsto v \oplus S\}$ exatamente como na definição.

Tome $\delta \in \mathcal{I}nst(\Gamma, \sigma, \Upsilon, \Delta)$, logo existe γ tal que $\delta = \sigma\gamma|_{\mathcal{V}ar(\Gamma)}$, $\sigma\gamma$ é idempotente e $\sigma\gamma$ satisfaz Υ e Δ . Seja $\phi := \{v \mapsto y \oplus S\}$ daí temos $\theta\phi = \{v \mapsto y \oplus S\}$.

Afirmação: $\sigma\theta\phi\gamma|_{\mathcal{V} \setminus \{v\}} =_{AC} \sigma\gamma|_{\mathcal{V} \setminus \{v\}}$.

Como v é uma variável nova então $v \notin \mathcal{V}ar(\mathcal{I}m(\sigma))$ então para todo $w \in \mathcal{V} \setminus \{v\}$ temos que

$v \notin \mathcal{V}ar(w\sigma)$, assim $w\sigma\theta\phi =_{AC} w\sigma$, implicando que, $w\sigma\theta\phi\gamma =_{AC} w\sigma\gamma$. Logo, $\sigma\theta\phi\gamma|_{\mathcal{V}\setminus\{v\}} =_{AC} \sigma\gamma|_{\mathcal{V}\setminus\{v\}}$.

Definindo por simplicidade, $\sigma_1 := \sigma\theta$ e $\gamma_1 := \phi\gamma$, então pela afirmação acima $\sigma_1\gamma_1|_{\mathcal{V}\setminus\{v\}} =_{AC} \sigma\gamma|_{\mathcal{V}\setminus\{v\}}$ e por $v \notin \mathcal{V}ar(\Gamma)$ temos $\delta =_{AC} \sigma_1\gamma_1|_{\mathcal{V}ar(\Gamma)}$.

Agora basta provarmos que $\sigma_1\gamma_1$ satisfaz $\Upsilon\theta$ e $\Delta\theta$. No Lema 5.1, provamos que se σ é idempotente então $\sigma\theta$ é idempotente e para provarmos isso provamos que $\theta\sigma\theta = \sigma\theta$, então $\theta\sigma\theta\phi\gamma =_{AC} \theta\sigma_1\gamma_1 =_{AC} \sigma_1\gamma_1$, concluindo que, $\theta\sigma_1\gamma_1|_{\mathcal{V}\setminus\{v\}} =_{AC} \sigma_1\gamma_1|_{\mathcal{V}\setminus\{v\}} =_{AC} \sigma\gamma|_{\mathcal{V}\setminus\{v\}}$.

i) Sendo $(u, t) \in \Upsilon$ onde t é um termo simples não-variável e $u\sigma\gamma \neq 0$, temos que $(u, t\theta) \in \Upsilon\theta$. Como $v \notin \mathcal{V}ar(t)$ e $u \neq v$ então pelo resultado acima obtemos que, $u\sigma_1\gamma_1 =_{AC} u\sigma\gamma$ e $t\theta\sigma_1\gamma_1 =_{AC} t\sigma\gamma$. Assim aplicando \oplus as partes obtemos: $u\sigma_1\gamma_1 \downarrow \oplus t\theta\sigma_1\gamma_1 \downarrow =_{AC} u\sigma\gamma \downarrow \oplus t\sigma\gamma \downarrow$. Como por hipótese, $\sigma\gamma$ satisfaz Υ então $u\sigma\gamma \downarrow \oplus t\sigma\gamma \downarrow$ é irredutível, então temos que $u\sigma_1\gamma_1 \downarrow \oplus t\theta\sigma_1\gamma_1 \downarrow$ é irredutível, logo $\sigma_1\gamma_1$ satisfaz $(u, t\theta) \in \Upsilon\theta$.

ii) Sendo $(u, w) \in \Upsilon$ onde w é uma variável suporte, temos que $w \neq y$ logo $w\theta = w$ e portanto $(u, w) \in \Upsilon\theta$. Por outro lado, v é variável nova, logo $u \neq v$ e $w \neq v$, temos $u\sigma_1\gamma_1 =_{AC} u\sigma\gamma$ e $w\sigma_1\gamma_1 =_{AC} w\sigma\gamma$. Assim aplicando \oplus em ambas as partes: $u\sigma_1\gamma_1 \downarrow \oplus w\sigma_1\gamma_1 \downarrow =_{AC} u\sigma\gamma \downarrow \oplus w\sigma\gamma \downarrow$. Como por hipótese, $\sigma\gamma$ satisfaz Υ temos que $u\sigma\gamma \downarrow \oplus w\sigma\gamma \downarrow$ é irredutível, implicando que $u\sigma_1\gamma_1 \downarrow \oplus w\sigma_1\gamma_1 \downarrow$ é irredutível e portanto $\sigma_1\gamma_1$ satisfaz $(u, w) \in \Upsilon\theta$.

Assim concluímos que $\sigma_1\gamma_1$ satisfaz $\Upsilon\theta$.

Tome $(s, t) \in \Delta$ então $(s\theta, t\theta) \in \Delta\theta$, como v é uma variável nova, temos que $v \notin \mathcal{V}ar(t) \cup \mathcal{V}ar(s)$ e portanto pela afirmação acima, $s\theta\sigma_1\gamma_1 =_{AC} s\sigma\gamma$ e $t\theta\sigma_1\gamma_1 =_{AC} t\sigma\gamma$ e aplicando \oplus em ambas as partes obtemos: $s\theta\sigma_1\gamma_1 \downarrow \oplus t\theta\sigma_1\gamma_1 \downarrow =_{AC} s\sigma\gamma \downarrow \oplus t\sigma\gamma \downarrow$.

Por hipótese $\sigma\gamma$ satisfaz Δ então $(s\sigma\gamma \downarrow \oplus t\sigma\gamma \downarrow) \downarrow \neq 0$ implicando que, $(s\theta\sigma_1\gamma_1 \downarrow \oplus t\theta\sigma_1\gamma_1 \downarrow) \downarrow \neq 0$. Logo $\sigma_1\gamma_1$ satisfaz $(s\theta, t\theta) \in \Delta\theta$, por conseguinte, $\sigma_1\gamma_1$ satisfaz $\Delta\theta$.

Então pelo Teorema 4.2, existe um renomeamento de variáveis α tal que $\delta\alpha|_{\mathcal{V}ar(\Gamma)} = \sigma_1\gamma_1\alpha|_{\mathcal{V}ar(\Gamma)} \in \mathcal{I}nst(\Gamma, \sigma\theta, \Upsilon\theta, \Delta\theta)$. E portanto $\mathcal{I}nst(\Gamma, \sigma, \Upsilon, \Delta) \subseteq_{\alpha} \mathcal{I}nst(\Gamma, \sigma\theta, \Upsilon\theta, \Delta\theta)$.

□

Lema 5.13. Se $\sigma \parallel \Upsilon \parallel \Delta \implies_{NRam} \sigma\theta \parallel \Upsilon'\theta \parallel \Delta\theta \vee \sigma \parallel \Upsilon'' \parallel \Delta$, então

$$\mathcal{I}nst(\Gamma, \sigma, \Upsilon, \Delta) \subseteq_{\alpha} \mathcal{I}nst(\Gamma, \sigma\theta, \Upsilon'\theta, \Delta\theta) \cup \mathcal{I}nst(\Gamma, \sigma, \Upsilon'', \Delta)$$

Demonstração. Tome $\delta \in \text{Inst}(\Gamma, \sigma, \Upsilon, \Delta)$, então δ é um unificador assimétrico de Γ , existe uma substituição γ tal que, $\delta = \sigma\gamma|_{\text{Var}(\Gamma)}$ e, $\sigma\gamma$ é idempotente satisfazendo Υ e Δ .

Se $\sigma\gamma$ não viola (v, s) então δ satisfaz Υ'' , logo $\sigma\gamma \in \text{Inst}(\Gamma, \sigma, \Upsilon'', \Delta)$, e portanto $\sigma\gamma \in \text{Inst}(\Gamma, \sigma\theta, \Upsilon'\theta, \Delta\theta) \cup \text{Inst}(\Gamma, \sigma, \Upsilon'', \Delta)$.

Suponha que $\sigma\gamma$ viole (v, s) então, $v\sigma\gamma \neq 0$, $v\sigma\gamma \downarrow =_{AC} s' \oplus S'$ e $s\sigma\gamma \downarrow =_{AC} s'$. Definindo $\phi = \{v' \mapsto v \oplus s\}$ então $\theta\phi = \{v' \mapsto v \oplus s\}$, com isso vamos provar a seguinte afirmação:

Afirmação: $\sigma\theta\phi\gamma|_{\mathcal{V}\setminus\{v'\}} =_{AC} \sigma\gamma|_{\mathcal{V}\setminus\{v'\}}$ e $v'\sigma\theta\phi\gamma =_{AC} S'$.

Como v' é variável nova então $v'\sigma = v'$ então temos:

$$\begin{aligned} v'\sigma\theta\phi\gamma \downarrow &=_{AC} v'\theta\phi\gamma \downarrow =_{AC} (v \oplus s)\gamma \downarrow \\ &=_{AC} (v\gamma \downarrow \oplus s\gamma \downarrow) \downarrow =_{AC} (s' \oplus S' \oplus s') \downarrow =_{AC} S' \end{aligned}$$

se $w \neq v'$ então $v' \notin \text{Var}(w\sigma)$ então $w\sigma\theta\phi =_{AC} w\sigma$, implicando que $w\sigma\theta\phi\gamma =_{AC} w\sigma\gamma$. Logo $\sigma\theta\phi\gamma|_{\mathcal{V}\setminus\{v'\}} = \sigma\gamma|_{\mathcal{V}\setminus\{v'\}}$. Tome por simplicidade $\sigma_1 = \sigma\theta$ e $\gamma_1 = \phi\gamma$, então obtemos que $\sigma_1\gamma_1|_{\mathcal{V}\setminus\{v'\}} =_{AC} \sigma\gamma|_{\mathcal{V}\setminus\{v'\}}$ e $v'\sigma_1\gamma_1 =_{AC} S'$. Note que σ é idempotente então $\sigma\theta$ também é idempotente e $\theta\sigma\theta =_{AC} \sigma\theta$, por conseguinte, $\theta\sigma_1\gamma_1|_{\mathcal{V}\setminus\{v'\}} =_{AC} \sigma\gamma|_{\mathcal{V}\setminus\{v'\}}$.

Vamos provar que $\sigma_1\gamma_1$ satisfaz $\Upsilon'\theta$ e $\Delta\theta$.

Afirmação: $\sigma_1\gamma_1$ satisfaz $\Upsilon'\theta$

i) Supondo que $(w, t) \in \Upsilon$, $w \neq v$ e $t \neq v$, então $(w, t\theta) \in \Upsilon'\theta$. Como $w\sigma_1\gamma_1 =_{AC} w\sigma\gamma$ e $t\theta\sigma_1\gamma_1 =_{AC} t\sigma\gamma$ então temos, $w\sigma_1\gamma_1 \downarrow \oplus t\theta\sigma_1\gamma_1 \downarrow =_{AC} w\sigma\gamma \downarrow \oplus t\sigma\gamma \downarrow$, e como $\sigma\gamma$ satisfaz Υ temos $w\sigma\gamma \downarrow \oplus t\sigma\gamma \downarrow$ irredutível, Logo $w\sigma_1\gamma_1 \downarrow \oplus t\theta\sigma_1\gamma_1 \downarrow$ é irredutível.

ii) Supondo que $(v, t) \in \Upsilon$, onde t é um termo simples não variável, logo $(v', t\theta) \in \Upsilon'\theta$.

Pela afirmação $v'\sigma_1\gamma_1 =_{AC} S'$ e $t\theta\sigma_1\gamma_1 =_{AC} t\sigma\gamma$ então basta provar $S' \oplus t\sigma\gamma \downarrow$ é irredutível.

De fato, por hipótese temos que $\sigma\gamma$ satisfaz Υ então $v\sigma\gamma \downarrow \oplus t\sigma\gamma \downarrow$ é irredutível e portanto, $s' \oplus S' \oplus t\sigma\gamma \downarrow$ é irredutível, por conseguinte, $S' \oplus t\sigma\gamma \downarrow$ é irredutível como queríamos demonstrar.

iii) Supondo que (v, w) pertença a Υ com $w \neq v$ uma variável, então $(v', w) \in \Upsilon'\theta$.

Como $v'\sigma_1\gamma_1 \downarrow =_{AC} S'$ e $w\sigma_1\gamma_1 \downarrow =_{AC} w\sigma\gamma \downarrow$, e pela hipótese temos $\sigma\gamma$ satisfaz Υ , então $\sigma\gamma$ não viola (v, w) , isto é, $v\sigma\gamma \downarrow \oplus w\sigma\gamma \downarrow$ é irredutível, no entanto, $v\sigma\gamma \downarrow =_{AC} s' \oplus S'$. Assim concluímos que $s' \oplus S' \oplus w\sigma\gamma \downarrow$ é irredutível, e por conseguinte, $v'\sigma_1\gamma_1 \downarrow \oplus w\sigma_1\gamma_1 \downarrow =_{AC} S' \oplus w\sigma\gamma$ que pelo

resultado acima é irreduzível, Logo $v'\sigma_1\gamma_1 \downarrow \oplus w\sigma_1\gamma_1 \downarrow$ é irreduzível, implicando que $\sigma_1\gamma_1$ satisfaz (v', w) .

iv) Supondo que $(w, v) \in \Upsilon$ onde w é uma variável suporte, então $(w, v) \in \Upsilon'$ e $(w, v'), (w, s) \in \Upsilon'\theta$ e como analisado no item anterior de forma totalmente análoga concluimos que $\sigma_1\gamma_1$ satisfaz (w, v') e (w, s) .

v) Sendo que $(v', s) \in \Upsilon'$ pela própria definição implica que $(v', s\theta) \in \Upsilon'\theta$. Como $v'\sigma_1\gamma_1 \downarrow =_{AC} S'$ e pela afirmação anterior $s\theta\sigma_1\gamma_1 \downarrow =_{AC} s\sigma\gamma \downarrow =_{AC} s'$, temos:

$$v'\sigma_1\gamma_1 \downarrow \oplus s\theta\sigma_1\gamma_1 \downarrow =_{AC} S' \oplus s' =_{AC} v\sigma\gamma \downarrow$$

Assim $v'\sigma_1\gamma_1 \downarrow \oplus s\theta\sigma_1\gamma_1 \downarrow$ é irreduzível, e por conseguinte, $\sigma_1\gamma_1$ satisfaz $(v', s\theta) \in \Upsilon'\theta$.

Logo, pelos itens acima, fica provado que $\sigma_1\gamma_1$ satisfaz $\Upsilon'\theta$.

Afirmação: $\sigma_1\gamma_1$ satisfaz $\Delta\theta$

Suponha $(r, t) \in \Delta$, então $(r\theta, t\theta) \in \Delta\theta$. Como v' é uma variável nova, $v' \notin \mathcal{V}ar(r) \cup \mathcal{V}ar(t)$, logo obtemos que:

$$r\theta\sigma_1\gamma_1 \downarrow =_{AC} r\sigma\gamma \downarrow \text{ e } t\theta\sigma_1\gamma_1 \downarrow =_{AC} t\sigma\gamma \downarrow$$

Assim $(r\theta\sigma_1\gamma_1 \downarrow \oplus t\theta\sigma_1\gamma_1 \downarrow) \downarrow =_{AC} (r\sigma\gamma \downarrow \oplus t\sigma\gamma \downarrow) \downarrow \neq 0$, implicando que, $\sigma_1\gamma_1$ satisfaz $(r\theta, t\theta) \in \Delta\theta$ e portanto $\sigma_1\gamma_1$ satisfaz $\Delta\theta$.

Assim pelas afirmações anteriores, $\sigma\theta\gamma_1 = \sigma_1\gamma_1$ satisfaz $\Upsilon'\theta$ e $\Delta\theta$, então pelo Teorema 4.2 existe um renomeamento de variáveis α tal que, $\sigma_1\gamma_1\alpha|_{\mathcal{V}ar(\Gamma)} \in \mathcal{I}nst(\Gamma, \sigma\theta, \Upsilon'\theta, \Delta\theta)$. Como $\delta =_{AC} \sigma\gamma|_{\mathcal{V}ar(\Gamma)} =_{AC} \sigma_1\gamma_1|_{\mathcal{V}ar(\Gamma)}$, então $\delta\alpha|_{\mathcal{V}ar(\Gamma)} =_{AC} \sigma_1\gamma_1\alpha|_{\mathcal{V}ar(\Gamma)}$ é um unificador assimétrico.

Portanto temos, $\delta\alpha|_{\mathcal{V}ar(\Gamma)} \in \mathcal{I}nst(\Gamma, \sigma\theta, \Upsilon'\theta, \Delta\theta)$, que por conseguinte,

$$\mathcal{I}nst(\Gamma, \sigma, \Upsilon, \Delta) \subseteq_{\alpha} \mathcal{I}nst(\Gamma, \sigma\theta, \Upsilon'\theta, \Delta\theta) \cup \mathcal{I}nst(\Gamma, \sigma, \Upsilon \cup (v, s), \Delta)$$

□

Lema 5.14. Se $\sigma \parallel \Upsilon \parallel \Delta \implies_{V\text{Ram}} \sigma\theta \parallel \Upsilon'\theta \parallel \Delta\theta \vee \sigma \parallel \Upsilon'' \parallel \Delta$ então

$$\mathcal{I}nst(\Gamma, \sigma, \Upsilon, \Delta) \subseteq_{\alpha} \mathcal{I}nst(\Gamma, \sigma\theta, \Upsilon'\theta, \Delta\theta) \cup \mathcal{I}nst(\Gamma, \sigma, \Upsilon'', \Delta)$$

Demonstração. Tome $\delta \in \text{Inst}(\Gamma, \sigma, \Upsilon, \Delta)$, daí $\delta = \sigma\gamma|_{\mathcal{V}ar(\Gamma)}$ e $\sigma\gamma$ é idempotente satisfazendo $\Upsilon e \Delta$. Observe que podemos supor γ idempotente sem prejuízo da generalidade. De fato, sendo α um renomeamento das variáveis de γ livre de $W = \mathcal{V}ar(\Gamma) \cup \mathcal{V}ar(\sigma\|\Upsilon\|\Delta)$ tal que $\gamma\alpha$ é idempotente, então $\sigma\gamma\alpha$ continua idempotente, pois se $x \in \mathcal{V} \setminus \text{Dom}(\alpha)$ temos $x\alpha\sigma = x\sigma$ e por outro lado $x\alpha\sigma = x\alpha$, então para qualquer $x \in \mathcal{V}$, $x\sigma\gamma\alpha\sigma\gamma\alpha =_{AC} x\sigma\gamma\alpha\gamma\alpha$ ou $x\sigma\gamma\alpha\sigma\gamma\alpha =_{AC} x\sigma\gamma\sigma\gamma\alpha$ e como $\sigma\gamma$ e $\gamma\alpha$ são idempotentes, temos $x\sigma\gamma\alpha\sigma\gamma\alpha =_{AC} x\sigma\gamma\alpha$.

E portanto temos $\sigma\gamma\alpha$ satisfazendo Υ, Δ e $\sigma\gamma\alpha|_{\mathcal{V}ar(\Gamma)} = \delta\alpha|_{\mathcal{V}ar(\Gamma)}$ um unificador assimétrico de Γ .

Suponha que $\sigma\gamma$ viole (v_1, v_2) , logo $v_1\sigma\gamma \downarrow_{=AC} S \oplus T_1$ e $v_2\sigma\gamma \downarrow_{=AC} S \oplus T_2$, onde $T_1 \oplus T_2$ é irredutível e S é não nulo. Defina a substituição $\phi = \{v'_1 \mapsto T_1, v'_2 \mapsto T_2, v_{12} \mapsto S\}$. Como $\theta = \{v_1 \mapsto v'_1 \oplus v_{12}, v_2 \mapsto v'_2 \oplus v_{12}\}$ então obtemos,

$$\theta\phi = \{v_1 \mapsto S \oplus T_1, v_2 \mapsto S \oplus T_2, v'_1 \mapsto T_1, v'_2 \mapsto T_2, v_{12} \mapsto S\}$$

Afirmção: Para todo $x \in \mathcal{V} \setminus \{v'_1, v'_2, v_{12}\}$. $x\sigma\theta\phi\gamma \downarrow_{=AC} x\sigma\gamma \downarrow$

Como que σ é idempotente, $v_1, v_2 \in \text{Im}(\sigma)$ e v'_1, v'_2, v_{12} serem variáveis novas então $v\sigma = v$ para $v = v_1, v_2, v'_1, v'_2$ e v_{12} . Temos:

- $v_1\sigma\theta\phi\gamma \downarrow_{=E} v_1\theta\phi\gamma \downarrow_{=E} (S \oplus T_1)\gamma \downarrow_{=E} v_1\sigma\gamma\gamma =_E v_1\sigma\gamma$.
- $v_2\sigma\theta\phi\gamma \downarrow_{=AC} v_2\theta\phi\gamma \downarrow_{=AC} (S \oplus T_2)\gamma \downarrow_{=AC} v_2\sigma\gamma\gamma =_{AC} v_2\sigma\gamma$.
- $v'_1\sigma\theta\phi\gamma \downarrow_{=AC} v'_1\theta\phi\gamma \downarrow_{=AC} T_1\gamma =_{AC} T_1$.
- $v'_2\sigma\theta\phi\gamma \downarrow_{=AC} v'_2\theta\phi\gamma \downarrow_{=AC} T_2\gamma =_{AC} T_2$.
- $v_{12}\sigma\theta\phi\gamma \downarrow_{=AC} v_{12}\theta\phi\gamma \downarrow_{=AC} S\gamma =_{AC} S$.

Para $w \neq v_1, v_2, v'_1, v'_2$ e v_{12} temos $w\theta\phi\gamma \downarrow_{=AC} w\gamma \downarrow$ e portanto $w\sigma\theta\phi\gamma \downarrow_{=AC} w\sigma\gamma \downarrow$.

Para simplificar denotaremos $\sigma_1 := \sigma\theta$ e $\gamma_1 := \phi\gamma$, então $\sigma_1\gamma_1 = \sigma\theta\phi\gamma$. Como $\theta\sigma\theta = \sigma\theta$ e $\theta\sigma_1 = \sigma_1$, então pela afirmação acima temos,

$$\forall x \in \mathcal{V} \setminus \{v'_1, v'_2, v_{12}\}. x\theta\sigma_1\gamma_1 \downarrow_{=AC} x\sigma_1\gamma_1 \downarrow.$$

Afirmção: $\sigma_1\gamma_1$ satisfaz $\Upsilon'\theta$

Sendo $\Upsilon'\theta$ definido como na regra de inferência *ramificação variável* então podemos separar em vários casos sobre os elementos de Υ . Sejam $v_i \in \{v_1, v_2\}$ e $v'_i \in \{v'_1, v'_2\}$, w uma variável.

i) Tome $(w, t) \in \Upsilon$ onde $w \neq v_1, v_2$ e $t \neq v_1, v_2$. Logo $(w, t) \in \Upsilon'$ e $(w, t\theta) \in \Upsilon'\theta$, como $t\theta\sigma_1\gamma_1 =_{AC} t\sigma_1\gamma_1 =_{AC} t\sigma\gamma$ e $\sigma\gamma$ por hipótese satisfaz Υ então $w\sigma\gamma \downarrow \oplus t\sigma\gamma \downarrow$ é irredutível, portanto $w\sigma_1\gamma_1 \downarrow \oplus t\theta\sigma_1\gamma_1 \downarrow$ é irredutível. Assim $\sigma_1\gamma_1$ satisfaz $(w, t\theta) \in \Upsilon'\theta$.

ii) suponha $(v_i, t) \in \Upsilon$ onde $t \neq v_1, v_2$, implica que $(v'_i, t), (v_{12}, t) \in \Upsilon'$ e $(v'_i, t\theta), (v_{12}, t\theta) \in \Upsilon'\theta$.

$$v'_i\sigma_1\gamma_1 \downarrow \oplus t\theta\sigma_1\gamma_1 \downarrow =_{AC} T_i \oplus t\sigma\gamma \downarrow \text{ e } v_{12}\sigma_1\gamma_1 \downarrow \oplus t\theta\sigma_1\gamma_1 \downarrow =_{AC} S \oplus t\sigma\gamma \downarrow$$

Porém $\sigma\gamma$ por hipótese satisfaz Υ e portanto $v_i\sigma\gamma \downarrow \oplus t\sigma\gamma \downarrow$ é irredutível, como $v_i\sigma_1\gamma_1 \downarrow =_{AC} v_i\sigma\gamma =_{AC} T_i \oplus S$, concluímos que $T_i \oplus t\sigma\gamma \downarrow$ e $S \oplus t\sigma\gamma \downarrow$ são irredutíveis. Então $\sigma_1\gamma_1$ satisfaz $(v'_1, t), (v'_2, t), (v_{12}, t) \in \Upsilon'\theta$.

iii) Suponha $(w, v_i) \in \Upsilon$ onde $w \neq v_1, v_2$.

Logo $(w, v_i) \in \Upsilon'$ e $(w, v_{12}), (w, v'_i) \in \Upsilon'\theta$, analogamente ao caso anterior: $v'_i\sigma_1\gamma_1 \downarrow \oplus w\theta\sigma_1\gamma_1 \downarrow =_{AC} T_i \oplus w\sigma\gamma \downarrow$ e $v_{12}\sigma_1\gamma_1 \downarrow \oplus w\theta\sigma_1\gamma_1 \downarrow =_{AC} S \oplus w\sigma\gamma \downarrow$.

Por hipótese $\sigma\gamma$ satisfaz Υ , portanto $v_i\sigma\gamma \downarrow \oplus w\sigma\gamma \downarrow$ é irredutível, como $v_i\sigma_1\gamma_1 \downarrow =_{AC} v_i\sigma\gamma =_{AC} T_i \oplus S$, concluímos que $T_i \oplus w\sigma\gamma \downarrow$ e $S \oplus w\sigma\gamma \downarrow$ são irredutíveis.

Então $\sigma_1\gamma_1$ satisfaz $(w, v'_i), (w, v'_2), (w, v_{12}) \in \Upsilon'\theta$.

iv) Seja $(v'_i, v_{12}) \in \Upsilon'\theta$, então $v'_i\sigma_1\gamma_1 \downarrow \oplus v_{12}\sigma_1\gamma_1 \downarrow =_{AC} T_i \oplus S$ que, por hipótese, é irredutível, portanto $\sigma_1\gamma_1$ satisfaz $\{(v'_1, v_{12}), (v'_2, v_{12}), (v_{12}, v'_1), (v_{12}, v'_2)\}$. Por outro lado sendo $(v'_1, v'_2) \in \Upsilon'\theta$ temos que $v'_1\sigma_1\gamma_1 \downarrow = T_1$ e $v'_2\sigma_1\gamma_1 \downarrow = T_2$, e como $T_1 \oplus T_2$ é irredutível por hipótese então $v'_1\sigma_1\gamma_1 \downarrow \oplus v'_2\sigma_1\gamma_1 \downarrow$ é irredutível, implicando que $\sigma_1\gamma_1$ satisfaz $\{(v'_1, v'_2), (v'_2, v'_1)\}$.

Então em todos os casos obtemos que $\sigma_1\gamma_1$ satisfaz $\Upsilon'\theta$.

Afirmção: $\sigma_1\gamma_1$ satisfaz $\Delta\theta$

Suponha $(r, t) \in \Delta$, então $(r\theta, t\theta) \in \Delta\theta$. Como v'_i, v_{12} são variáveis novas, $v'_i, v_{12} \notin \mathcal{V}ar(r) \cup \mathcal{V}ar(t)$, obtemos que: $r\theta\sigma_1\gamma_1 \downarrow =_{AC} r\sigma\gamma \downarrow$ e $t\theta\sigma_1\gamma_1 \downarrow =_{AC} t\sigma\gamma \downarrow$.

Assim $(r\theta\sigma_1\gamma_1 \downarrow \oplus t\theta\sigma_1\gamma_1 \downarrow) \downarrow =_{AC} (r\sigma\gamma \downarrow \oplus t\sigma\gamma \downarrow) \downarrow \neq 0$, implicando que, $\sigma_1\gamma_1$ satisfaz $(r\theta, t\theta) \in \Delta\theta$ e então $\sigma_1\gamma_1$ satisfaz $\Delta\theta$.

Portanto, $\sigma\theta\gamma_1|_{\mathcal{V}ar(\Gamma)} = \sigma_1\gamma_1|_{\mathcal{V}ar(\Gamma)} =_{AC} \sigma\gamma|_{\mathcal{V}ar(\Gamma)} = \delta$ é um unificador assimétrico de Γ , que satisfaz $\Upsilon'\theta$ e $\Delta\theta$. Pelo Teorema 4.2 existe um renomeamento de variáveis α tal que, $\delta\alpha|_{\mathcal{V}ar(\Gamma)} \in$

$\mathcal{Inst}(\Gamma, \sigma\theta, \Upsilon'\theta, \Delta\theta)$. Se $\sigma\gamma$ satisfaz (v_1, v_2) então que $\delta \in \mathcal{Inst}(\Gamma, \sigma, \Upsilon'', \Delta)$, então em ambos os casos temos $\delta\alpha|_{\mathcal{Var}(\Gamma)} \in \mathcal{Inst}(\Gamma, \sigma\theta, \Upsilon'\theta, \Delta\theta) \cup \mathcal{Inst}(\Gamma, \sigma, \Upsilon'', \Delta)$. \square

Lema 5.15. Se $\sigma\|\Upsilon\|\Delta \implies_{ARam} \sigma\theta\|\Upsilon'\theta\|\Delta\theta \vee \sigma\|\Upsilon''\|\Delta$, então

$$\mathcal{Inst}(\Gamma, \sigma, \Upsilon, \Delta) \subseteq_{\alpha} \mathcal{Inst}(\Gamma, \sigma\theta, \Upsilon'\theta, \Delta\theta) \cup \mathcal{Inst}(\Gamma, \sigma, \Upsilon'', \Delta)$$

Demonstração. Análogo ao caso da ramificação não variável. \square

Lema 5.16. Se $\sigma\|\Upsilon\|\Delta \implies_{Dec} \bigvee_{i=1}^n \sigma_i\|\Upsilon_i\|\Delta_i \vee \sigma\|\Upsilon\|\Delta'$ então

$$\mathcal{Inst}(\Gamma, \sigma, \Upsilon, \Delta) \subseteq \bigcup_{i=1}^n \mathcal{Inst}(\Gamma, \sigma_i, \Upsilon_i, \Delta_i) \cup \mathcal{Inst}(\Gamma, \sigma, \Upsilon, \Delta')$$

Demonstração. Pela definição da regra de decomposição existe um conjunto completo de unificadores da equação $s = ? t$, $U := \{\theta_1, \dots, \theta_n\}$, tal que para cada $i \in \{1, \dots, n\}$, $\mathcal{Var}(\mathcal{Im}(\theta_i)) \cap \mathcal{Dom}(\sigma) = \emptyset$.

E além disso temos:

$$\sigma_i = \sigma\theta_i, \Upsilon_i = \Upsilon\theta_i, \Delta_i = \Delta\theta_i \text{ e } \Delta' = \Delta \cup (s, t)$$

Tome $\delta \in \mathcal{Inst}(\Gamma, \sigma, \Upsilon, \Delta)$, e portanto $\delta = \sigma\gamma|_{\mathcal{Var}(\Gamma)}$, onde $\sigma\gamma$ é idempotente satisfazendo Υ, Δ .

Se $\sigma\gamma$ não viola (s, t) então $\delta \in \mathcal{Inst}(\Gamma, \sigma, \Upsilon, \Delta')$, vamos supor agora que δ viole (s, t) , isto é, $s\sigma\gamma \downarrow =_{AC} t\sigma \downarrow$, equivalentemente, $s\sigma\gamma =_{\oplus} t\sigma\gamma$. E por U ser um conjunto completo de unificadores de $s = ? t$ então existe um $i \in \{1, \dots, n\}$ tal que $\theta_i|_{\mathcal{Var}(s,t)} \lesssim_{\oplus} \sigma\gamma|_{\mathcal{Var}(s,t)}$ e portanto existe uma substituição ϕ tal que $\theta_i\phi =_{\oplus} \sigma\gamma|_{\mathcal{Var}(s,t)}$. Note que σ é idempotente, então: $\sigma\theta_i\phi =_{\oplus} \sigma\sigma\gamma|_{\mathcal{Var}(s,t)} = \sigma\gamma|_{\mathcal{Var}(s,t)}$.

Tome α uma substituição tal que $\mathcal{Dom}(\alpha) = \mathcal{Dom}(\sigma\gamma) \setminus \mathcal{Var}(s, t)$ e $x\alpha = x\sigma\gamma$ para todo $x \in \mathcal{Dom}(\alpha)$ e portanto $x\sigma\gamma\alpha = x\sigma\gamma$ pois $\sigma\gamma$ é idempotente. Então obtemos $x\sigma\theta_i\phi\alpha =_{\oplus} x(\sigma\gamma|_{\mathcal{Var}(s,t)})\alpha = x\sigma\gamma$. Assim podemos concluir que $\sigma_i\phi\alpha =_{\oplus} \sigma\gamma$ implicando que $\sigma_i\phi$ é idempotente e por $\theta_i\sigma\theta_i = \sigma\theta_i = \sigma_i$ temos que $\sigma_i\phi\alpha$ satisfaz $\Upsilon\theta_i$ e $\Delta\theta_i$ pois $\sigma\gamma$ satisfaz Υ e Δ .

Portanto $\delta = \sigma\gamma|_{\mathcal{Var}(\Gamma)} = \sigma_i\phi\alpha|_{\mathcal{Var}(\Gamma)}$, $\sigma_i\phi\alpha$ é idempotente satisfazendo $\Upsilon\theta_i$ e $\Delta\theta_i$, implicando que $\delta \in \mathcal{Inst}(\Gamma, \sigma_i, \Upsilon_i, \Delta_i)$. \square

Lema 5.17. Se $\sigma\|\Upsilon\|\Delta \implies_{Elim} \sigma\theta\|\Upsilon\theta\|\Delta\theta$ então, $\mathcal{Inst}(\Gamma, \sigma, \Upsilon, \Delta) \subseteq_{\alpha} \mathcal{Inst}(\Gamma, \sigma\theta, \Upsilon\theta, \Delta\theta)$.

Demonstração. Tome $\delta \in \mathcal{Inst}(\Gamma, \sigma, \Upsilon, \Delta)$ então $\delta = \sigma\gamma|_{\mathcal{Var}(\Gamma)}$ onde $\sigma\gamma$ é idempotente satisfazendo Υ e Δ .

Afirmção 1. $v\gamma = 0$:

Note que existe $t \stackrel{?}{=} t' \in \Gamma$ tal que $x \oplus y$ é subtermo de t' e $[x \mapsto v \oplus S], [y \mapsto v \oplus S'] \in \sigma$, como δ é um unificador assimétrico de Γ então $(x \oplus y)\delta \downarrow =_{AC} x\delta \downarrow \oplus y\delta \downarrow =_{AC} x\delta \oplus y\delta$.

Note que $x, y \in \mathcal{Var}(\Gamma)$ então $x\delta = x\sigma\gamma$ e $y\delta = y\sigma\gamma$, assim obtemos:

$$x\sigma\gamma =_{AC} (v \oplus S)\gamma \downarrow =_{AC} (v\gamma \oplus S\gamma) \downarrow \quad \text{e} \quad y\sigma\gamma =_{AC} (v \oplus S')\gamma \downarrow =_{AC} (v\gamma \oplus S'\gamma) \downarrow$$

Pela definição da regra *Eliminação*, temos que só podemos aplicá-la quando não é possível aplicar nenhuma regra de *Ramificação* e separação, e portanto para todo termo simples e não variável $s \in_{\oplus} S$ e $s' \in_{\oplus} S'$ temos que $(v, s) \in \Upsilon$ ou $v \in \mathcal{Var}(s)$ e $(v, s') \in \Upsilon$ ou $v \in \mathcal{Var}(s')$. Logo sendo $s \in_{\oplus} S$ um termo simples e não variável, isto é, um termo simples e não variável na soma S temos que $v \in \mathcal{Var}(s)$ ou $(v, s) \in \Upsilon$.

- $v \in \mathcal{Var}(s)$: Então $v\gamma \neq_E s\gamma \oplus T$ pois a árvore de posições de ambas são distintas.
- $(v, s) \in \Upsilon$: Como $\sigma\gamma$ satisfaz Υ então $v\sigma\gamma \downarrow \oplus s\sigma\gamma \downarrow$ está em sua forma normal, note que σ é idempotente e portanto $v\sigma = v$ e $s\sigma = s$, implicando que $v\gamma \downarrow \oplus s\gamma \downarrow$ é irreduzível, isto é, $v\gamma \downarrow \oplus s\gamma \downarrow$ é irreduzível.

De forma análoga para $s' \in_{\oplus} S'$.

Como $v\gamma \downarrow \oplus S\gamma \downarrow$ ou $v\gamma \downarrow \oplus S'\gamma \downarrow$ é redutível, pois δ é um unificador assimétrico de Γ , temos que $v\gamma = 0$ pois não existe $s \in_{\oplus} S$ e $s' \in_{\oplus} S'$ tais que $s\gamma$ ou $s'\gamma$ anulam $v\gamma$. Portanto, $\sigma\gamma = \sigma\theta\gamma$, e notando que $v\theta\sigma\theta = 0\sigma\theta = 0 = v\theta = v\sigma\theta$ então obtemos que $\theta\sigma\theta\gamma = \sigma\theta\gamma = \sigma\gamma$.

Como $\sigma\gamma$ satisfaz Υ e Δ temos que $\theta\sigma\theta\gamma$ satisfaz Υ e Δ portanto $\sigma\theta\gamma$ satisfaz $\Upsilon\theta$ e $\Delta\theta$, isto é, $\delta \in \mathcal{Inst}(\Gamma, \sigma\theta, \Upsilon\theta, \Delta\theta)$ □

Lema 5.18. Se $\sigma \parallel \Upsilon \parallel \Delta \implies \mathcal{J}_{AXO} \bigvee_{i=1}^n \sigma_i \parallel \Upsilon_i \parallel \Delta_i$ então $\mathcal{Inst}(\Gamma, \sigma, \Upsilon, \Delta) \subseteq_{\alpha} \bigcup_{i=1}^n \mathcal{Inst}(\Gamma, \sigma_i, \Upsilon_i, \Delta_i)$.

Demonstração. Fica demonstrado pelos Lemas 5.12a 5.17. □

No próximo teorema, utilizaremos a mesma notação da definição 3.18, encontrada na página 107.

Teorema 5.3. *Sejam $\sigma \parallel \Upsilon \parallel \Delta$ um estado válido de \mathcal{J}_{AXO} , $n \in \mathbb{N}$ e a família $F_n = \{\sigma_i \parallel \Upsilon_i \parallel \Delta_i\}_{i \in I}$ de estados de \mathcal{J}_{AXO} tais que $\sigma \parallel \Upsilon \parallel \Delta \xRightarrow{\mathcal{J}_{AXO}} \bigvee_{i \in I}^{\leq n} \sigma_i \parallel \Upsilon_i \parallel \Delta_i$. Então, $\mathcal{I}nst(\Gamma, \sigma, \Upsilon, \Delta) \subseteq_{\alpha} \bigcup_{i \in I} \mathcal{I}nst(\Gamma, \sigma_i, \Upsilon_i, \Delta_i)$.*

Demonstração. Vamos provar por indução sobre $n \in \mathbb{N}$, sejam $\sigma \parallel \Upsilon \parallel \Delta$, $n \in \mathbb{N}$ e F_n como na hipótese.

Hipótese de indução: Suponha que para algum $n \geq 0$ vale o teorema.

Caso base: $n = 0$ e então $F_n = \{\sigma \parallel \Upsilon \parallel \Delta\}$ que é trivialmente verdadeiro.

Passo indutivo: Podemos separar de forma disjunta F_n da seguinte forma $F_n = \mathcal{I}_n \dot{\cup} \mathcal{R}_n$ onde \mathcal{I}_n são os estados irreduzíveis de F_n e \mathcal{R}_n os redutíveis e portanto $\mathcal{I}_n \subseteq F_{n+1}$ e para cada $\sigma_i \parallel \Upsilon_i \parallel \Delta_i \in \mathcal{R}_n$, podemos aplicar uma regra de inferência obtendo $\sigma_i \parallel \Upsilon_i \parallel \Delta_i \xRightarrow{\mathcal{J}_{AXO}} \bigvee_{j=1}^{n_i} \sigma_j^i \parallel \Upsilon_j^i \parallel \Delta_j^i$ então $\{\sigma_j^i \parallel \Upsilon_j^i \parallel \Delta_j^i\}_{j \in \{1, \dots, n_i\}} \subseteq F_{n+1}$.

Pelo Lema 5.18 $\mathcal{I}nst(\Gamma, \sigma_i, \Upsilon_i, \Delta_i) \subseteq_{\alpha} \bigcup_{j=1}^{n_i} \mathcal{I}nst(\Gamma, \sigma_j^i, \Upsilon_j^i, \Delta_j^i)$, com $F_{n+1} = \{\sigma_j \parallel \Upsilon_j \parallel \Delta_j\}_{j \in J}$ e aplicando a HI sobre F_n temos $\mathcal{I}nst(\Gamma, \sigma, \Upsilon, \Delta) \subseteq_{\alpha} \bigcup_{i \in I} \mathcal{I}nst(\Gamma, \sigma_i, \Upsilon_i, \Delta_i) \subseteq_{\alpha} \bigcup_{j \in J} \mathcal{I}nst(\Gamma, \sigma_j, \Upsilon_j, \Delta_j)$, e o resultado segue para todo $n \in \mathbb{N}$. \square

Observação 5.1. *Portanto podemos tomar $F = F_n$ no qual n é o menor inteiro tal que F_n contém apenas estados finais obtidos a partir do estado válido $\sigma \parallel \Upsilon \parallel \Delta$, pois o algoritmo \mathcal{J}_{AXO} é terminante.*

Teorema 5.4. *Seja $\sigma \parallel \emptyset \parallel \emptyset$ um estado inicial de \mathcal{J}_{AXO} . se $L = \{\sigma_i \parallel \Upsilon_i \parallel \Delta_i\}_{i \in I}$ o resultado de aplicar o algoritmo \mathcal{J}_{AXO} em $\sigma \parallel \emptyset \parallel \emptyset$. Então $\mathcal{I}nst(\Gamma, \sigma, \emptyset, \emptyset) =_{\alpha} \bigcup_{i \in I} \mathcal{I}nst(\Gamma, \sigma_i, \Upsilon_i, \Delta_i)$.*

Demonstração. Como o algoritmo \mathcal{J}_{AXO} aplicado em $\sigma \parallel \emptyset \parallel \emptyset$ retornou a lista L da hipótese então existe um $n \in \mathbb{N}$ tal que $F_n = \{\sigma_j' \parallel \Upsilon_j' \parallel \Delta_j'\}_{j \in J}$ tem apenas estados finais, e portanto pela definição do algoritmo \mathcal{J}_{AXO} , $L \subseteq F_n$ e para todo $\sigma_j' \parallel \Upsilon_j' \parallel \Delta_j' \in F_n \setminus L$ temos que σ_j' não é um unificador assimétrico de Γ . Logo pelo Lema 5.11 temos $\mathcal{I}nst(\Gamma, \sigma_j', \Upsilon_j', \Delta_j') = \emptyset$. E portanto pelo Lema 5.3 obtemos

$$\mathcal{I}nst(\Gamma, \sigma, \emptyset, \emptyset) \subseteq_{\alpha} \bigcup_{j \in J} \mathcal{I}nst(\Gamma, \sigma_j', \Upsilon_j', \Delta_j') \subseteq \bigcup_{i \in I} \mathcal{I}nst(\Gamma, \sigma_i, \Upsilon_i, \Delta_i)$$

Por outro lado dado $\sigma_i \parallel \Upsilon_i \parallel \Delta_i \in L$ então σ_i é um unificador assimétrico de Γ que é uma instância de σ e portanto $\sigma_i \in \mathcal{I}nst(\Gamma, \sigma, \emptyset, \emptyset)$, então $\bigcup_{i \in I} \mathcal{I}nst(\Gamma, \sigma_i, \Upsilon_i, \Delta_i) \subseteq \mathcal{I}nst(\Gamma, \sigma, \emptyset, \emptyset)$. \square

Corolário 5.1 (Correção de \mathcal{J}_{AXO}). *Sejam Γ um problema de unificação, \mathcal{U}_{XOR} um conjunto completo de unificadores de Γ e $\sigma \in \mathcal{U}_{XOR}$.*

Se $L := \mathcal{J}_{AXO}(\Gamma, \sigma \parallel \emptyset \parallel \emptyset)$ então para cada $\sigma_i \parallel \Upsilon_i \parallel \Delta_i \in L$ temos que σ_i é um unificador assimétrico de Γ e uma instância de σ .

Demonstração. Direto da definição do algoritmo \mathcal{J}_{AXO} , pois escolhemos apenas os estados que σ_i é um unificador assimétrico, e σ_i é uma instância de σ pela definição das regras de inferência de \mathcal{J}_{AXO} . \square

Corolário 5.2 (Completude de \mathcal{J}_{AXO}). *Sejam Γ um problema de unificação, \mathcal{U}_{XOR} um conjunto completo de unificadores de Γ e $\sigma \in \mathcal{U}_{XOR}$.*

Se $L := \{\sigma_i \parallel \Upsilon_i \parallel \Delta_i\} = \mathcal{J}_{AXO}(\Gamma, \sigma \parallel \emptyset \parallel \emptyset)$ e δ um unificador assimétrico de Γ que é uma instância de σ então existe um estado $\sigma_i \parallel \Upsilon_i \parallel \Delta_i \in L$ tal que $\sigma_i|_{\text{var}(\Gamma)} \lesssim_{\oplus} \delta|_{\text{var}(\Gamma)}$

Demonstração. Como δ é um unificador assimétrico de Γ que é uma instância de σ , temos

$$\delta \in \mathcal{Inst}(\Gamma, \sigma, \emptyset, \emptyset) \subseteq_{\alpha} \bigcup_{i \in I} \mathcal{Inst}(\Gamma, \sigma_i, \Upsilon_i, \Delta_i),$$

e portanto existe um renomeamento de variáveis α tal que $\delta\alpha|_{\text{var}(\Gamma)} \in \mathcal{Inst}(\Gamma, \sigma_i, \Upsilon_i, \Delta_i) \neq \emptyset$, então σ_i é um unificador assimétrico de Γ e $\sigma_i|_{\text{var}(\Gamma)} \lesssim_{\oplus} \delta\alpha|_{\text{var}(\Gamma)}$, equivalentemente, $\sigma_i|_{\text{var}(\Gamma)} \lesssim_{\oplus} \delta|_{\text{var}(\Gamma)}$

\square

Conclusão e Trabalhos Futuros

Neste trabalho apresentamos um estudo do problema de unificação módulo as teorias equacionais $ACUN$ e $ACUNh$, seguindo as técnicas propostas em [11, 16, 18]. Mostramos que no caso de $ACUN(h)$ -unificação elementar com constantes, o problema é decidível em tempo polinomial, uma vez que o problema reduz para solubilidade de sistemas sobre $\mathbb{Z}_2/\mathbb{Z}_2[h]$. No caso $ACUN(h)$ -unificação geral, apresentamos o resultado proposto por Schulz em [16], que garante a complexidade de decidir o problema se torna NP -difícil.

Apresentamos um estudo detalhado sobre o algoritmo \mathcal{J}_{XORh} , proposto por Liu [18], para solubilidade de $ACUN(h)$ -unificação para problemas gerais. Provamos que esse algoritmo é terminante, completo e correto, gerando sempre um conjunto completo de $ACUN(h)$ -unificadores finito, para tal, explicitamos a importância da regra *purificação* que é terminante e correta. Liu [18] afirma que seu algoritmo produz um conjunto completo de $ACUN(h)$ -unificadores que possui poucas redundâncias ou nenhuma, isto é, quase sempre gera um conjunto minimal, possuindo uma implementação muito simples, se contrapondo com outras abordagens propostas por [6], [15].

Desenvolvemos também um estudo detalhado do algoritmo \mathcal{J}_{AXO} , proposto por Liu [18], para $ACUN$ -unificação *assimétrica*. Mostramos que \mathcal{J}_{AXO} é correto e completo utilizando uma técnica alternativa àquela proposta em [18]. Fizemos referência para sua prova de terminalidade.

Como trabalhos futuro, pretendemos generalizar a abordagem de Liu [18] para teorias equacionais de grupos abelianos com expoente p , onde p é um primo qualquer. Como um segundo passo pretendemos estender a unificação nominal [2, 17] para teoria equacional $ACUN(h)$, mostrando inicialmente que α -equivalência pode ser estendida módulo $ACUN(h)$, seguindo a abordagem em [1].

Referências Bibliográficas

- [1] M. Ayala-Rincón, W. de Carvalho-Segundo, M. Fernández and D. Nantes-Sobrinho. *A Formalisation of Nominal Equivalence with Associative and Commutative Function Symbols*. In *Proc. of 11th Workshop on Logical and Semantic Frameworks, with Applications (LSFA)*, 2016. (To appear.)
- [2] M. Ayala-Rincón, M. Fernández and D. Nantes-Sobrinho. *Nominal Narrowing*. In *Proc. of Formal Structures for Computation and Deduction (FSCD) 2016*, volume 52 of LIPIcs, pages 11:1–11:17, Schloss Dagstuhl , 2016.
- [3] F. Baader *Unification in Commutative Theories*. In *J. Symb. Comput.*, vol. 8(5), pages 479–497, 1989
- [4] F. Baader and T. Nipkow. *Term Rewriting and All that.*, Cambridge University Press, 1998.
- [5] L. Bachmair and N. Dershowitz. *Completion for rewriting modulo a congruence*. In *Theoretical Comput. Sci.*, 67(2&3):173–201, Oct. 1989.
- [6] A. Boudet, J. P. Jouannaud, and M. Schmidt-Schauß. *Unification in Boolean Rings and Abelian Groups*. In *J. of Symb. Comput.*, 8(5), vol. 67, pages 449–477, 1989.
- [7] V. Cortier, S. Delaune and P. Lafourcade. *A survey of algebraic properties used in cryptographic protocols*. In *J. of Computer Security*, vol. 14(1), pages 1–43, 2006.
- [8] D. Dolev and A. C. Yao. *On the security of public key protocols* In *IEEE Trans. on Information Theory*, volume 29(2), pages 198–208, 1983.

- [9] S. Erbatur, S. Escobar, D. Kapur, Z. Liu, C. A. Lynch, C. A. Meadows, J. Meseguer, S. Santiago and R. Sasse. *Asymmetric Unification: A New Unification Paradigm for Cryptographic Protocol Analysis*. In *Proc. of CADE*, vol. 7898 of LNCS, pages 231–248, Springer, 2013.
- [10] S. Escobar, C. A. Meadows e J. Meseguer - Maude-NPA: Cryptographic Protocol Analysis Modulo Equational Properties In *Foundations of Security Analysis and Design (FOSAD) 2007/2008/2009 Tutorial Lectures* vol. 5705, pages 1–50,2009.
- [11] Q. Guo, P. Narendran and D. A. Wolfram. *Unification and Matching Modulo Nilpotence*. In *Proc. of Conference on Automated Deduction (CADE)*, vol. 1104 of LNCS, pages 261–274, Springer, 1996.
- [12] E. Kaltofen, M.S. Krishnamoorthy and B.D. Saunders. *Fast parallel computation of Hermite and Smith forms of polynomial matrices..* In *SIAM Journal of Algebraic and Discrete Methods*, vol. 8(4), pages 683–690, 1987.
- [13] W. Nutt. *Unification in Monoidal Theories*. In *10th International Conference on Automated Deduction (CADE)*, vol.449, pages 618-632, Springer, 1990.
- [14] C. Papadimitriou and S. Kenneth. *Combinatorial Optimization Algorithms and Complexity*. Prentice Hall, 1982.
- [15] M. Schmidt-Schauß. *Unification in a Combination of Arbitrary Disjoint Equational Theories*. In *Proc. of Conference on Automated Deduction (CADE)*, vol. 310 of LNCS, pages 378–396, Springer, 1988
- [16] Schulz K.U. (1997) A criterion for intractability of E-unification with free function symbols and its relevance for combination of unification algorithms. In Comon H. (eds) *Rewriting Techniques and Applications*. RTA 1997. Lecture Notes in Computer Science, vol 1232. Springer, Berlin, Heidelberg
- [17] C. Urban, A. Pitts and M. Gabbay. *Nominal unification*. In *Theor. Comput. Sci.*, volume 323(1-3), pages 473–497, 2004.

- [18] Z. Liu. *Dealing Efficiently with Exclusive-Or, Abelian Groups and Homomorphism in Cryptographic Protocol Analysis*. *PhD Thesis*, Clarkson University, 2012.