

## **PROPOSTA DE PADRÕES DE PROPRIEDADES E TÁTICAS DE PROVA PARA SISTEMAS ESPECIFICADOS EM GRAMÁTICA DE GRAFOS NA PLATAFORMA RODIN.**

SIMONE DRAWANZ RUTZ<sup>1</sup>; PLINIO FINKENAUER JUNIOR<sup>2</sup>; LUCIANA FOSS<sup>3</sup>;  
 SIMONE COSTA.

<sup>1</sup>UNIVERSIDADE FEDERAL DE PELOTAS – sdrutz@inf.ufpel.edu.br

<sup>2</sup>UNIVERSIDADE FEDERAL DE PELOTAS – pfinkenauer@inf.ufpel.edu.br

<sup>3</sup>UNIVERSIDADE FEDERAL DE PELOTAS – lfoss@inf.ufpel.edu.br

UNIVERSIDADE FEDERAL DE PELOTAS – simone.costa@gmail.com

### 1. INTRODUÇÃO

Gramática de grafos (GG) (EHRING, 1997) é uma linguagem de especificação formal, utilizada na descrição de sistemas. Por ser uma linguagem visual torna a descrição de situações complexas mais intuitivas ao entendimento. Neste formalismo o sistema é descrito através de grafos e de regras de transformação de grafos, onde seu comportamento é determinado pela aplicação destas regras ao estado atual do sistema (descrito também por um grafo).

Uma GG é composta por um grafo inicial e um conjunto de regras (RIBEIRO, 1997). O grafo inicial define o estado inicial do sistema, isto é, descreve a configuração inicial do sistema e como ele se apresenta antes da aplicação de qualquer regra.

As regras (morfismos entre grafos) definem as possíveis mudanças que podem acontecer no sistema. As regras possuem os seguintes componentes: um grafo esquerdo (L), um grafo direito (R) e um morfismo entre grafos, o qual mapeia L em R. O lado esquerdo determina os componentes que devem estar no estado atual do sistema para que a regra seja aplicada e o lado direito especifica as modificações que devem ocorrer no grafo estado após a aplicação da regra. As regras são aplicadas a um grafo estado quando existe um match (morfismo total entre grafos), que identifica que todos os elementos do lado esquerdo da regra estão presente no grafo estado.

A especificação em GG permite a verificação formal do sistema descrito, o que possibilita investigar a validade de propriedades específicas do mesmo. Uma das técnicas de verificação utilizada é a Prova de Teoremas. Uma abordagem, previamente proposta (DA COSTA, 2010), que adota esta técnica para GG especifica tanto o grafo inicial, quanto as regras utilizando teoria dos conjuntos e lógica de primeira ordem, além de propor uma tradução de GG para a linguagem Event-B (DEPLOY). Esta tradução permitiu o uso da ferramenta Rodin (DEPLOY) para a verificação de propriedades. As propriedades são descritas como invariantes do sistema (isto é propriedades que devem ser válidas para todos os estados possíveis do sistema). A técnica de prova utilizada é a indução matemática: obrigações de prova para o estado inicial e para cada uma das regras do sistema são geradas. O processo de prova é semi-automático, ou seja, ele é capaz de verificar algumas obrigações de prova automaticamente mas para outras ele exige interação com o usuário para completar a prova.

O objetivo deste trabalho é de propor táticas de prova (LEMONS JUNIOR, 2013<sup>2</sup>) que facilitem esta interação, sugerindo para o usuário um passo- a- passo para a realização da prova, de acordo com a propriedade especificada.

## 2. METODOLOGIA

O desenvolvimento desta pesquisa exige conhecimentos em gramática de grafos e em como realizar especificações neste tipo modelo, para isso foi necessário estudar os conceitos que envolvem GG. É parte do processo de desenvolvimento do projeto a identificação de propriedades adequadas de serem verificadas em sistemas especificados em gramática de grafos, considerando como técnica de verificação a prova de teoremas.

É necessária a especificação de um sistema para ser utilizado como estudo de caso, pois é nele que serão analisados os padrões propostos e verificadas propriedades. Para especificar um sistema em GG (LEMONS JUNIOR, 2013<sup>1</sup>), define-se um grafo que represente seu estado inicial e um conjunto de regras entre grafos, que descrevam as diversas possibilidades de comportamento do sistema.

Na adoção da técnica de prova de teoremas para GG, tanto o sistema quanto seu comportamento devem ser descritos utilizando teoria dos conjuntos e lógica. Existe uma abordagem que permite a prova de teoremas de GG que permite o uso da ferramenta Rodin para realizar a verificação. O sistema em questão deve ser descrito na linguagem Event-B, que é a linguagem suportada pela plataforma Rodin. O Rodin é um provador semi-automático, que durante a verificação gera um conjunto de obrigações de prova. Parte destas obrigações são provadas automaticamente, mas outras necessitam interação do usuário para conclusão da prova. Neste último caso, o usuário deve dar o caminho para a conclusão da prova, utilizando táticas disponíveis na ferramenta, selecionando hipóteses ou até mesmo rodando provadores disponíveis.

Porém o desenvolvimento dessas obrigações de provas não é muito intuitivo, então para facilitar a interação na realização das provas propõem-se táticas para a realização das mesmas. Estas táticas serão definidas para os padrões de propriedades definidos na primeira etapa do trabalho, estabelecendo um passo-a-passo para a conclusão das obrigações de prova geradas para estas propriedades.

## 3. RESULTADOS E DISCUSSÃO

Após um estudo aprofundado sobre GG pode-se observar onde a utilização de GG como método formal de especificação é aplicável de forma satisfatória. As áreas de Engenharia de Software e de Sistemas Distribuídos podem fazer bom uso deste formalismo.

O processo de desenvolvimento de software compreende algumas fases, sendo elas estudo de viabilidade, análise de requisitos, especificação do software, implementação, teste, implantação e manutenção. O uso de GG se enquadraria perfeitamente na fase de especificação. As propriedades a serem especificadas são identificadas e recolhidas na fase de análise de requisitos onde são definidas todas as funcionalidades do software. GG, pelo seu caráter visual, tornaria mais simples a interação entre as fases de análise de requisitos e a fase de implementação, pois muitas vezes o desenvolvimento de software é realizado por pessoas distintas entre as fases. Não podendo esquecer também que a especificação em GG permite a realização de provas sobre propriedades e isso pode causar bons reflexos na fase de teste, pois a verificação das propriedades especificadas ajuda a prevenir falhas.

Em relação aos Sistemas Distribuídos, que atualmente têm se tornado cada vez mais utilizados, a aplicação de uma técnica de especificação formal contribuiria na diminuição da sua complexidade. Como já foi dito anteriormente, a GG é um método formal visual e por consequência mais intuitivo.

Levando em consideração os resultados da pesquisa até então se vê a necessidade de se estudar com mais afinco a ferramenta Rodin, para então poder de forma efetiva iniciar a proposta das táticas de prova para especificações em GG.

#### 4. CONCLUSÕES

A especificação e verificação formal têm por objetivo descrever sistemas e seu comportamento, para que então possam ser verificadas e garantidas suas propriedades. Este tipo de técnica é de grande ajuda quando empregada a sistemas amplos e de alta complexidade, pois estes tipos de sistema tendem a gerar uma vasta gama de casos de teste, o que torna muito custoso o desenvolvimento para então a correção de possíveis falhas no mesmo.

A utilização de técnicas de especificação formal tende a dar um maior nível de segurança ao sistema que será implementado, garantido que certas funções do mesmo não irão gerar nenhum tipo de conflito durante a execução, diminuindo o tempo de desenvolvimento e implantação. Este mesmo efeito pode ser notado no tempo que será empregado na fase de testes e correção.

Tornar a especificação e a verificação formais menos custosas e mais intuitivas, faria com que o processo de desenvolvimento de sistemas em geral fosse muito mais simples e rápido, trazendo mais segurança e confiabilidade. Por estas razões a proposta de táticas de prova irá ajudar a diminuir o custo da verificação formal o que certamente a tornaria um ótimo recurso para o processo de criação de sistemas.

#### 5. REFERÊNCIAS BIBLIOGRÁFICAS

da Costa, S. A. **Relational Approach of Graph Grammars**. 2010. Tese (PhD em Computação). UFRGS.

Lemos Junior, L. C. (2013). **Towards the use of Proof Tactics for Theorem Proving Graph Grammars through Rodin**. In : WEIT 2013. Rio Grande, RS<sup>1</sup>.

Ribeiro, L.; Korff, M. **Métodos Formais para Especificação: Gramática de Grafos**, Pelotas – RS. Novembro de 1997.

DEPLOY. **Event-B and the Rodin platform**, Maio 2013. Acessado em: 26 set. 2013. Online. Disponível em: <http://www.event-b.org/> .

Lemos Junior, L. C. (). **Theorem Proving Graph Grammars: Strategies for Discharging Proof Obligations**. Em: SBMF 2013<sup>2</sup>.

Ehrig, H., Heckel, R., Korff, M., Löwe, M., Ribeiro, L., Wagner, A., Corradini, A.: **Handbook of graph grammars and computing by graph transformation**. World Scientific Publishing Co., of graph grammars and computing by graph transformation. World Scientific Publishing Co., Inc., River Edge, NJ, USA (1997).