PRIMEIROS PASSOS PARA A ESPECIFICAÇÃO E VERIFICAÇÃO FORMAL DE UM SISTEMA DE TROCA DENOMINADO ESCAMBO

JOÃO VITOR CHAGAS POSSOBOM VAZ[1]; SIMONE ANDRÉ DA COSTA CAVALHEIRO[2]

[1]UFPel – jvcpvaz@inf.ufpel.edu.br
[2]UFPel - simone.costa@inf.ufpel.edu.br

1. INTRODUÇÃO

Com o crescimento do tamanho e da complexidade dos sistemas computacionais, surgiu a necessidade de construir especificações mais precisas para descrever o comportamento desses sistemas. A utilização de métodos formais para a descrição de um modelo se apresenta como uma alternativa interessante, no sentido de tornar o modelo construído mais confiável e robusto. Usando técnicas baseadas na matemática, esses métodos são usados para descrever um sistema, para analisar seu comportamento e para auxiliar em seu projeto, verificando as principais propriedades de interesse por meio de ferramentas de análise precisas e eficazes. A especificação formal, por meio da definição precisa de um sistema (utilizando uma linguagem com semântica definida), é uma excelente maneira de descobrir erros de projeto, permitindo também analisar se um programa tem certas propriedades desejáveis.

Como um método de especificação formal tem-se as gramáticas de grafos (GG) (LEILA, 2000) que fornecem um mecanismo no qual as transformações locais em grafos podem ser modeladas de uma maneira visual e matematicamente precisa. É um método formal que se diferencia dos demais por possuir uma representação visual gráfica e um meio natural para explicar situações complexas de modo intuitivo, o que facilita a sua compreensão e não exige um conhecimento avançado com respeito ao formalismo. Basicamente, os estados dos sistemas são modelados por grafos e as possíveis mudanças de comportamento por regras de transformações de grafos.

Por sua vez, o Event-B (ABRIAL, 2010) é um formalismo usado para especificar e raciocinar sobre sistemas discretos complexos e é sustentado pelo rigor matemático. A plataforma Rodin é uma ferramenta para especificação, refinamento e prova que usa como linguagem de entrada o Event-B, onde refinamento é usado para acrescentar incrementalmente detalhes à especificação. A plataforma Rodin é um conjunto de ferramentas dedicado a apoiar o desenvolvimento de tais sistemas. O mesmo já contém vários plug-ins: verificador estático, gerador de obrigação de prova, provadores, verificadores de modelo, animadores, transformadores UML, manipulador de documento de requisitos etc. Contém também vários elementos de modelagem como: variáveis, invariantes e transições. Os usuários podem desenvolver modelos e ir refinando conforme for necessário, ao fazer isso eles são capazes de raciocinar, modificar, e decompor seus modelos antes de iniciar a implementação efetiva do sistema correspondente. Usando o Event-B, o sistema e suas propriedades são especificadas usando lógica de conjuntos e lógica de predicados, usa prova e refinamento para mostrar que as invariantes são mantidas enquanto o desenvolvimento prossegue.

Este trabalho consiste na especificação e verificação formal de um sistema de troca denominado Escambo. O sistema, em elaboração pelo discente do curso em Ciência da Computação da UFPel Rafael Nascimento, já foi especificado em UML e implementado. As etapas deste trabalho consistem na especificação do sistema em GG na ferramenta AGG (Berlin, 2017) na sua respectiva tradução para o Event-B (CAVALHEIRO; FOSS; RIBEIRO, 2017), na descrição lógica de propriedades desejadas e por fim na verificação destas propriedades por meio da técnica de prova de teoremas (LEILA, 2000). Até o presente momento se estudou o referencial teórico necessário ao desenvolvimento deste trabalho.

2. METODOLOGIA

Para a resolução deste trabalho são necessárias algumas etapas: algumas já concluídas e outras a serem seguidas. Começando com a compreensão do Event-B e Rodin, foi necessário estudo e entendimento sobre a modelagem, a abstração e refinamento, algumas técnicas matemáticas usadas para a especificação formal, bem como o uso de algumas ferramentas de prova, como a demonstração de obrigações de prova por meio de provadores de teoremas interativos. Além disso foi analisado referencial teórico (CRAIGEN, 1993), para a compreensão da Gramática de Grafos. Este modelo será utilizado para a especificação do sistema Escambo definido em um trabalho de conclusão de curso, onde o objetivo fim é a troca de produtos. No Escambo, o usuário pode cadastrar produto, editar produto, qualificar um produto, etc. e um administrador com direitos de ver produtos denunciados, banir produtos e banir usuários. Este sistema será especificado usando um ambiente de desenvolvimento para sistemas e transformações de grafos denominado AGG (The Attributed Graph Grammar System) e traduzido para o Event-B utilizando um tradutor automático, em seguida será feita a verificação e comprovação de algumas propriedades deste sistema.

3. RESULTADOS E DISCUSSÃO

Até o momento foram feitos alguns estudos sobre Event-B, gramáticas de grafos e sobre a ferramenta AGG. No Event-B foi construído um exemplo completo de desenvolvimento de um pequeno sistema sobre o controle de carros em uma ponte que ligava um continente a uma ilha. Esse sistema estava equipado com dois semáforos: verde e vermelho, onde um dos semáforos estava situado no continente e o outro na ilha, e também equipado com quatro sensores de carro, cada um com dois estados: ligado ou desligado. Os sensores foram usados para detectar a presença de carros entrando ou saindo da ponte. Tudo isso partindo de uma especificação inicial e sendo refinado em uma série de modelos cada vez mais detalhados. Na especificação inicial foi descrito o limite do número de carros. No primeiro refinamento foi especificada a ponte de sentido

único, no segundo refinamento foi introduzido os semáforos e no terceiro refinamento foi modelado os sensores. O refinamento permite o desenvolvimento e análise gradual do sistema, já que um modelo inicial detalhado com todas informações seria complicado demais para ser compreendido e analisado. Cada um dos modelos construídos foi analisado e comprovado. Nesse sistema haviam algumas restrições, tais como os motoristas deviam obedecer aos semáforos e não passar quando um semáforo estivesse vermelho, o número de carros na ponte e ilha era limitado e a ponte era de sentido único, não podendo passar em ambos os sentidos ao mesmo tempo.

Para uma especificação no evento B, temos dois tipos de componentes: contexto e máquina. Um contexto descreve a parte estática de um modelo contendo basicamente constantes e axiomas, onde os axiomas são afirmações que são assumidas como verdadeiras no resto do modelo e eles podem ser marcados como teoremas, cada um consistindo de um rótulo e um predicado. Já uma máquina descreve o comportamento dinâmico de um modelo por meio de variáveis cujos valores são alterados por eventos. Visto que a condição sob a qual um evento pode ser executado é dada por uma guarda, esses eventos definem uma possível mudança de estado para uma máquina e possuem os seguintes elementos: nome, parâmetros, guardas, testemunhas e ações. Os nomes dos parâmetros devem ser únicos, ou seja, não deve haver constante ou variável com o mesmo nome. Cada guarda consiste em um rótulo e um predicado. Testemunhas também são compostas de um rótulo e um predicado que estabelece uma ligação entre os valores das variáveis e parâmetros dos eventos concretos e abstratos onde na maioria das vezes o predicado acaba sendo uma igualdade simples. Uma máquina é então composta basicamente por variáveis, invariantes e eventos, onde uma invariante é uma declaração que deve ser válida em cada estado da máquina e consiste de um rótulo e um predicado.

Sobre gramática de grafos foi possível observar que é uma linguagem visual e excelente para explicar situações complexas de modo formal e intuitivo, trocando então a representação de strings por grafos, modelando os estados como grafos e possíveis mudanças de estado como regras de transformações. Como exemplo temos o grafo da Figura 1 que mostra algumas ocorrências no jogo PacMan de uma maneira simples e de fácil entendimento.

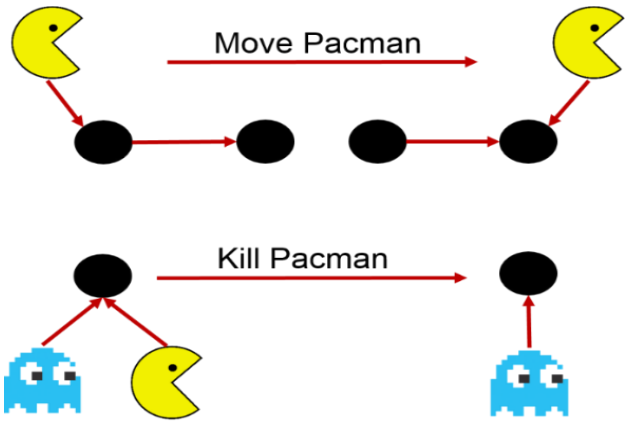

Figura 1: Ações do jogo PacMan em grafos

Ao invés de ter sido feita usando grafos, essa especificação poderia ser feita usando strings, porém a dificuldade de entendimento seria maior se comparada a essa.

De uma maneira bem intuitiva também é possível especificar a gramática de grafos usando a ferramenta AGG que é uma linguagem visual baseada em regras que suporta uma abordagem algébrica para transformação de grafos e que se destina à especificação e implementação de aplicações com dados estruturados em grafos complexos.

4. CONCLUSÕES

Neste trabalho foi realizado o estudo da linguagem Event-B, a especificação de um sistema de controle de carros em uma ponte na ferramenta Rodin e o estudo sobre a linguagem gramática de grafos. As próximas etapas consistem na compreensão detalhada do sistema de trocas de produtos Escambo, na sua especificação em gramática de grafos usando a ferramenta AGG, na sua tradução (por meio de uma ferramenta automática) para o Event-B e por fim na especificação e prova de propriedades.

5. REFERÊNCIAS BIBLIOGRÁFICAS

ABRIAL, J.R. **Modeling in Event-B: System and Software.** Cambridge University Press, New York, 2010.

Berlin,T. **A brief Description of AGG**, Berlin 2 mar. 2017. Acessado em 23 ago. 2018. Online. Disponível em: http://www.user.tu-berlin.de/o.runge/agg/index.html

CAVALHEIRO, S.; FOSS, L.; RIBEIRO, L. **Theorem proving graph grammars with attributes and negative application conditions**. Theoretical Computer Science, Elsevier, 2017.

LEILA, R. **Métodos Formais de Especificação: Gramáticas de Grafos**. Instituto de Informática, Porto Alegre, 2000. Acessado em 23 ago. 2018. Online. Disponivel em: ftp://ftp.inf.ufrgs.br/pub/leila/eri.ps.gz