Gabriela Moreira Mafra

Tradução automática de especificação formal modelada em TLA+ para linguagem de programação

Joinville

2019

UNIVERSIDADE DO ESTADO DE SANTA CATARINA
BACHARELADO EM CIÊNCIA DA COMPUTAÇÃO

Gabriela Moreira Mafra

TRADUÇÃO AUTOMÁTICA DE ESPECIFICAÇÃO FORMAL MODELADA EM TLA+ PARA LINGUAGEM DE PROGRAMAÇÃO

Trabalho de conclusão de curso submetido à Universidade do Estado de Santa Catarina como parte dos requisitos para a obtenção do grau de Bacharel em Ciência da Computação

Cristiano Damiani Vasconcellos
Orientador

Karina Girardi Rôggia
Co-Orientador

Joinville, Março de 2019

TRADUÇÃO AUTOMÁTICA DE ESPECIFICAÇÃO FORMAL MODELADA EM TLA+ PARA LINGUAGEM DE PROGRAMAÇÃO

Gabriela Moreira Mafra

Este Trabalho de Conclusão de Curso foi julgado adequado para a obtenção do título de Bacharel em Ciência da Computação e aprovado em sua forma final pelo Curso de Ciência da Computação Integral do CCT/UDESC.

Banca Examinadora

Cristiano Damiani Vasconcellos - Doutor
(orientador)

Adelaine Gelain - Mestre

Paulo Torrens - Mestre

Agradecimentos

Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Resumo

Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Palavras-chaves: Especificação de software, Lógica temporal, Geração de código, Métodos formais, Model checking

Abstract

Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Keywords: Software specification, Temporal Logic, Code Generation, Formal Methods, Model Checking

Contents

List of Figures

List of Tables

Lista de Abreviaturas

1 Introdução

1.1 Objetivos

Esse trabalho é feito com a intenção de elaborar um método de tradução, através do mapeamento de estruturas e construtores, de especificações formais descritas em TLA+ para código em linguagem de programação com possibilidade de ser executado e modificado; assim como implementar um tradutor que aplique esse método.

1.1.1 Objetivos Específicos

- Encontrar mapeamentos entre as estruturas de especificação em TLA+ e estruturas de linguagens de programação
- Implementar um gerador de código Elixir, com capacidade de fazer *parsing* de especificações em TLA+ e aplicar os mapeamentos necessários.

2 TLA$^+$

TLA+ é uma linguagem de especificação de software, criada por Leslie Lamport [CITAR] voltada à modelagem de sistemas concorrentes. Ela se propõe a oferecer uma maneira mais simples de escrever um algoritmo, ao utilizar um nível de abstração acima do que há ao escrever código em uma linguagem de programação. Assim, ao programar, não é necessário atentar-se a detalhes de implementação, permitindo o foco no comportamento do algoritmo - e não das suas dependências.

As especificações são descritas em fórmulas matemáticas, com pequenas adaptações de sintaxe. Para facilitar a curva de aprendizado para engenheiros, foi criada a linguagem PlusCal, com uma sintaxe semelhante a linguagens de programação imperativas, e que traduz seus programas para TLA+. A linguagem PlusCal não permite especificar sistemas tão complexos quanto os que podem ser escritos diretamente em TLA+, mas, devido à tradução para a linguagem original, aproveita completamente as capacidades dela de verificação de propriedades.

O método de especificação é baseado em máquinas de estados e, sendo assim, a descrição de um modelo é composta por uma condição inicial, que determina os possíveis estados inciais, e por uma relação de transições, que determina os possíveis estados que podem suceder cada estado em uma execução. Dessa forma, o conjunto de comportamentos especificado é composto por todos os comportamentos cujo estado inicial satisfaz a condição inicial e todas as transições estão na relação.

Lamport destaca [HYPERBOOK] que as especificações deveriam ser sobre modelos de uma abstração do sistema, e não algo retirado do próprio sistema. Semelhante à planta de um edifício, a especificação pode ser consultada para obter informações sobre o edifício (ou programa) de forma mais conveniente, além de ser capaz de facilitar uma série de verificações e perceber problemas enquanto a mudança ainda não é inviavelmente custosa.

article latexsym ifthen

verbatim

$$\text{EXTENDS Integers}$$

$$\text{VARIABLES small, big}$$

$$\begin{aligned}\text{TypeOK} \triangleq\ & \land \text{small} \in 0 \mathinner{..} 3 \\ & \land \text{big} \quad \in 0 \mathinner{..} 5\end{aligned}$$

$$\begin{aligned}\text{Init} \triangleq\ & \land \text{big} \quad = 0 \\ & \land \text{small} = 0\end{aligned}$$

$$\begin{aligned}\text{FillSmall} \triangleq\ & \land \text{small}' = 3 \\ & \land \text{big}' \quad = \text{big}\end{aligned}$$

$$\begin{aligned}\text{FillBig} \triangleq\ & \land \text{big}' \quad = 5 \\ & \land \text{small}' = \text{small}\end{aligned}$$

$$\begin{aligned}\text{EmptySmall} \triangleq\ & \land \text{small}' = 0 \\ & \land \text{big}' \quad = \text{big}\end{aligned}$$

$$\begin{aligned}\text{EmptyBig} \triangleq\ & \land \text{big}' \quad = 0 \\ & \land \text{small}' = \text{small}\end{aligned}$$

$$\begin{aligned}\text{SmallToBig} \triangleq\ & \text{IF } \text{big} + \text{small} \leq 5 \\ & \text{THEN } \land \text{big}' \quad = \text{big} + \text{small} \\ & \qquad\quad \land \text{small}' = 0\end{aligned}$$

$$\text{ELSE} \quad \land \text{big}' = 5$$
$$\land \text{small}' = \text{small} - (5 - \text{big})$$

$$\text{BigToSmall} \triangleq \text{IF } \text{big} + \text{small} \leq 3$$
$$\text{THEN} \quad \land \text{big}' = 0$$
$$\land \text{small}' = \text{big} + \text{small}$$
$$\text{ELSE} \quad \land \text{big}' = \text{small} - (3 - \text{big})$$
$$\land \text{small}' = 3$$

$$\text{Next} \triangleq \lor \text{FillSmall}$$
$$\lor \text{FillBig}$$
$$\lor \text{EmptySmall}$$
$$\lor \text{EmptyBig}$$
$$\lor \text{SmallToBig}$$
$$\lor \text{BigToSmall}$$

* Modification History

* Last modified Sun May 19 09:36:17 BRT 2019 by gabriela

* Created Sun May 19 09:35:45 BRT 2019 by gabriela