



Especificação Formal de Software

Gabriela Moreira Mafra

Universidade do Estado de Santa Catarina

gabrielamoreiramafra@gmail.com

16 de Março de 2020



Especificação Formal

Arquitetos desenham plantas detalhadas antes de colocar tijolos e pregos. Mas poucos programadores escrevem sequer um rascunho do que seus programas serão antes de começar a programá-los. Podemos aprender com arquitetos [Lamport 2015].



Plantas e especificações



- Permite verificações
- Serve como base para consulta
- Mais fácil de modificar do que o produto final
- Vem antes da produção



Verificação formal

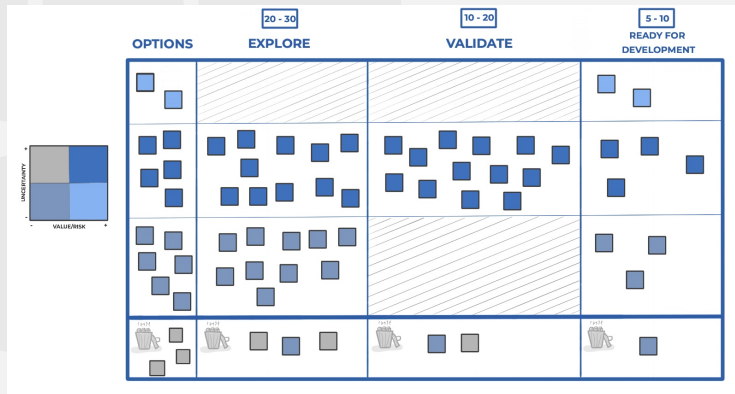
A partir de uma especificação, é possível verificar propriedades de maneira automatizada.

Isso permite buscar por otimizações, e encontrar *bugs*.

Esses benefícios foram reportados pela *Amazon Web Services* [Newcombe et al. 2015], que afirma ter usado TLA⁺ em 10 sistemas complexos.

Desenho de solução

Na engenharia de software, existem etapas de planejamento. Pode ser feito em um documento de texto, uma prova de conceito ou uma especificação formal.





Geração de código

A implementação - ou a tradução da especificação em linguagem de programação - pode ser feita por um programador ou um tradutor automático.

Problemas da tradução manual:

- Suscetível a erro - causando a perda de propriedades verificadas.
- Custosa



Geração de testes

A partir das propriedades verificadas, é possível gerar testes automatizados.

Benefícios dos testes

- Minimizar o impacto de alterações no código.
- Servir como cenário básico para simulação.



Considerações

Os benefícios da especificação formal de software são relevantes se bem aplicados.

- Geração de protótipos.
- Otimização e busca de problema.

Pode ser incorporada como etapa de desenvolvimento de empresas de software que seguem outros processos de especificação.



Referências



LAMPORT, L. Who builds a house without drawing blueprints? *Commun. ACM*, Association for Computing Machinery, New York, NY, USA, v. 58, n. 4, p. 38–41, mar. 2015. ISSN 0001-0782. Disponível em: <https://doi.org/10.1145/2736348>.



NEWCOMBE, C. et al. How amazon web services uses formal methods. *Commun. ACM*, ACM, New York, NY, USA, v. 58, n. 4, p. 66–73, mar. 2015. ISSN 0001-0782. Disponível em: <http://doi.acm.org/10.1145/2699417>.



Obrigada!

Especificação Formal de Software

Gabriela Moreira Mafra

Universidade do Estado de Santa Catarina

gabrielamoreiramafra@gmail.com

16 de Março de 2020

Fim :D