

CLAV - ESPECIFICAÇÃO E VERIFICAÇÃO DO MODELO FORMAL

Armando Santos and Gonalo Duarte

University of Minho, Braga, Portugal

Resumo CLAV   uma plataforma que est  a ser desenvolvida pelo Departamento de Inform tica da Universidade do Minho em parceria com a Dire o Geral do Livro, Arquivos e Bibliotecas (DGLAB), e tem como objetivo a classifica o e avalia o de todos os documentos que circulam pelas institui es p blicas portuguesas. Neste momento existe um modelo do problema especificado em OWL (*Ontology Web Language*), mas tem sofrido v rias altera es no decorrer do  ltimo ano e n o existiu tempo para estudar o impacto dessas mesmas altera es nas pr -condi es e invariantes do modelo. Neste projeto, inserido na Unidade Curricular de Labor torios em Engenharia Inform tica (LEI) do MIEI/UM, pretende-se formalizar o modelo de ra z assim como os seus invariantes e garantir a consist ncia dos mesmos, sendo capaz de detetar erros que, at  agora, n o tenham sido identificados.

Keywords: Administra o P blica · M todos Formais · Engenharia Inform tica · Alloy Analyzer · OWL.

1 Introdu o

At  agora, em Portugal, n o existia nenhum sistema de informa o que gerisse a classifica o e a avalia o dos documentos gerados no  mbito dos processos que circulam dentro das institui es p blicas portuguesas. O CLAV veio mudar isso com a elabora o de um cat logo, que se pretende que venha a ser a refer ncia nacional de todos os processos da Administra o P blica (AP), tendo sido modelado numa ontologia. Esta ontologia est  especificada num modelo formal que representa o conjunto de conceitos referentes aos processos de neg cio e aos relacionamentos entre eles. Infelizmente, todos os dados e documenta o de apoio est o espalhados, desorganizados e em diferentes formatos, o que os torna extremamente dif ceis de manter num dom nio t o complexo como o da AP. No entanto, embora j  tenham sido feitos esfor os para criar um formato neutro, como a Macro-estrutura Funcional (MEF), e v rios sistemas de explora o e exporta o, devido aos problemas associados com a inser o manual dos dados oriundos das diversas institui es e   complexidade e instabilidade dos invariantes e restri es associadas ao modelo n o   poss vel garantir a coer ncia das rela es entre os processos de neg cio. Esta incoer ncia   extremamente cr tica uma vez que a classifica o e avalia o dos processos possui legisla es associadas e lida com a remo o ou conserva o (digital e f sica) de documentos governamentais.

Deste modo, no contexto da unidade curricular de Laboratórios em Engenharia Informática do Mestrado Integrado em Engenharia Informática da Universidade do Minho e associado ao perfil de Métodos Formais em Engenharia Informática, apresentamos, neste artigo, a especificação e verificação, de raiz, da ontologia e o estudo da coerência dos invariantes e pré-condições que fazem parte dela. Devido à natureza puramente relacional inerente no domínio do problema em questão, iremos tirar partido de métodos algébricos e relacionais para nos ajudar a raciocinar sobre o problema em mãos e utilizar o *Alloy model checker* para nos auxiliar a encontrar falhas no desenho do modelo.

2 O Problema

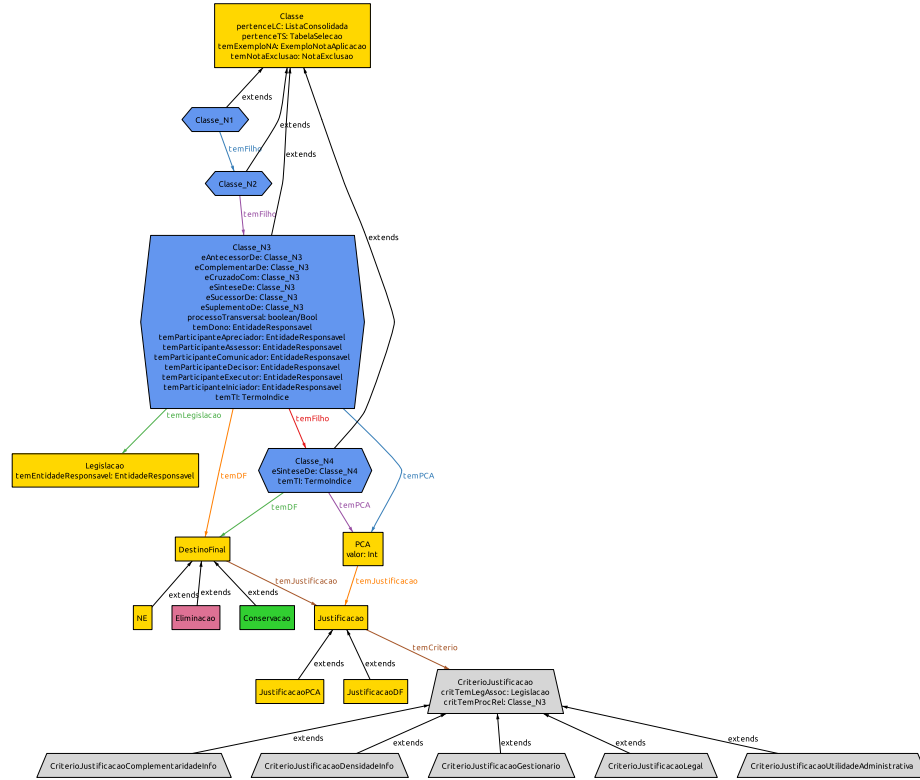


Figura 1: Meta-modelo simplificado

Cada instituição pública portuguesa desempenha uma função específica dentro da AP (p. ex. a prestação de cuidados de saúde), associado a cada função existe um conjunto de várias sub-funções (p. ex. a gestão de utentes e serviços clínicos)

e cada sub-função possui uma lista de processos de negócio que, concretamente, se materializam em documentos (p. ex. um processo de negócio pertencente à sub-função de gestão de utentes seria o registo clínico de utentes). A Lista Consolidada possui esta estrutura hierárquica de 4 níveis onde os processos de negócio são passíveis de ser desdobrados para efeitos de avaliação como falaremos mais à frente. Cada classe da LC possui um conjunto de atributos que a descreve e a partir do 3º nível (PNs) começam a surgir relações mais complicadas entre processos no campo chamado contexto de avaliação. Este contexto de avaliação, como também iremos ver mais à frente, tem associado um conjunto de invariantes que influenciarão o campo das decisões de avaliação. Este último campo é responsável por conter a informação sobre o Prazo de Conservação Administrativa (PCA) e Destino Final (DF) de um processo que correspondem, respetivamente, ao prazo que o documento deve ser guardado e qual o seu destino uma vez que este prazo expire.

Embora as entidades principais no domínio do problema sejam as classes da LC, existem várias outras que se relacionam direta ou indiretamente com cada uma das classes e que fornecem uma maior profundidade e complexidade ao modelo como podemos observar na figura 1.

Observando o meta-modelo simplificado, onde a azul se encontram os 4 níveis de classe, verificamos que este possui uma complexidade natural mesmo sem lhe impor alguma restrição. Sendo assim, e dado o contexto sério em que o problema está inserido, torna-se claro que deve ser feita alguma coisa no que diz respeito a dar algumas garantias acerca da coerência e consistência da LC.

2.1 Primeiro *Checkpoint*

Sendo o CLAV um projeto que já existe há 1 ano e já se encontra com alguns componentes operacionais, decidiu-se pegar em toda a documentação existente sobre o modelo e os seus requisitos e, com a ajuda do Professor José Carlos Ramalho, fazer um apanhado de todas as entidades e relações existentes. Durante esta primeira fase, bastantes das reuniões semanais serviram para apurar pequenos detalhes e dúvidas que iam surgindo.

Uma das razões que motivaram este investimento inicial, apesar de já existir uma ontologia definida pela qual nos podíamos guiar, foi a de existir muita documentação solta e incompleta que nem sempre estava de acordo com a versão mais recente da ontologia. Foi então, elaborado um documento atualizado que documenta os mais recentes requisitos e invariantes e que já se tornou bastante útil no refinamento da ontologia original, nomeadamente na eliminação de entidades e relações obsoletas e no apuramento do domínio e contradomínio de várias relações.

Na Secção 3 iremos falar mais detalhadamente sobre cada entidade e relação do modelo e na Secção 4 será abordada a respetiva implementação em Alloy.

2.2 Segundo *Checkpoint*

Uma das principais motivações deste projeto é estudar a forma como os mais variados invariantes interagem entre si e se de alguma forma se contradizem. É neste sentido que o Alloy, sendo uma linguagem de modelação de software leve que nos permite especificar o tanto o modelo como as restrições a ele associadas, ajuda a detetar erros ingénuos e subtis.

Após o investimento inicial em colecionar todo o material relevante e necessário sobre o problema, deu-se início ao ciclo de vida de verificação do problema [1]. Apesar dos invariantes serem abordados com mais detalhes na secção 3.3 é possível adiantar já que foram identificados 38 restrições no total, sendo que 23 dessas foram acrescentadas no tal processo de verificação.

Podemos concluir que o Alloy teve um impacto positivo na análise das restrições do modelo e na especificação do modelo formal. É importante realçar que a utilização de um *model checker* não descarta a necessidade de prova mas é muito útil para encontrar falhas de *design* como podemos constatar. A ausência de contra-exemplos dá uma grande confiança de que uma prova de correção está ao alcance.

2.3 Avaliação Final

3 Modelo Formal

3.1 Domínio

3.2 Relações envolvidas

3.3 Invariantes

4 Modelação em ALLOY

4.1 Especificação

4.2 Verificação

5 Dificuldades

6 Conclusão e Trabalho Futuro

Referências

1. José N. Oliveira and Miguel A. Ferreira, Member, IEEE: Alloy Meets the Algebra of Programming: A Case Study. IEEE TRANSACTIONS ON SOFTWARE ENGINEERING, VOL. 39, NO. 3, MARCH 2013