MAC5715 - Tópicos de POO
Padrão: Teorias Formais

Ana Paula Mota(NUSP: 3671589) e Daniel Ribeiro (NUSP: 3667708)

1 Objetivo

Pesquisar, compreender e estender o conhecimento de áreas como matemática, estatística e computação (mas se aplica a qualquer área cujo conhecimento seja formalizado).

2 Motivação

Ao buscar soluções ou conhecimentos nas áreas formais, é freqüente sermos remetidos a problemas que originaram as soluções, a definições relacionadas e a outras áreas que surgem como uma abstração dos problemas. Tudo isso gera uma grande rede de dados, fatos, idéias, definições e formalismos, na qual é muito fácil perder de vista de onde saímos e onde queremos chegar.

Esse padrão busca organizar todos os elementos envolvidos, de modo que se possa navegar nessa rede sem perder o objetivo.

3 Aplicabilidade

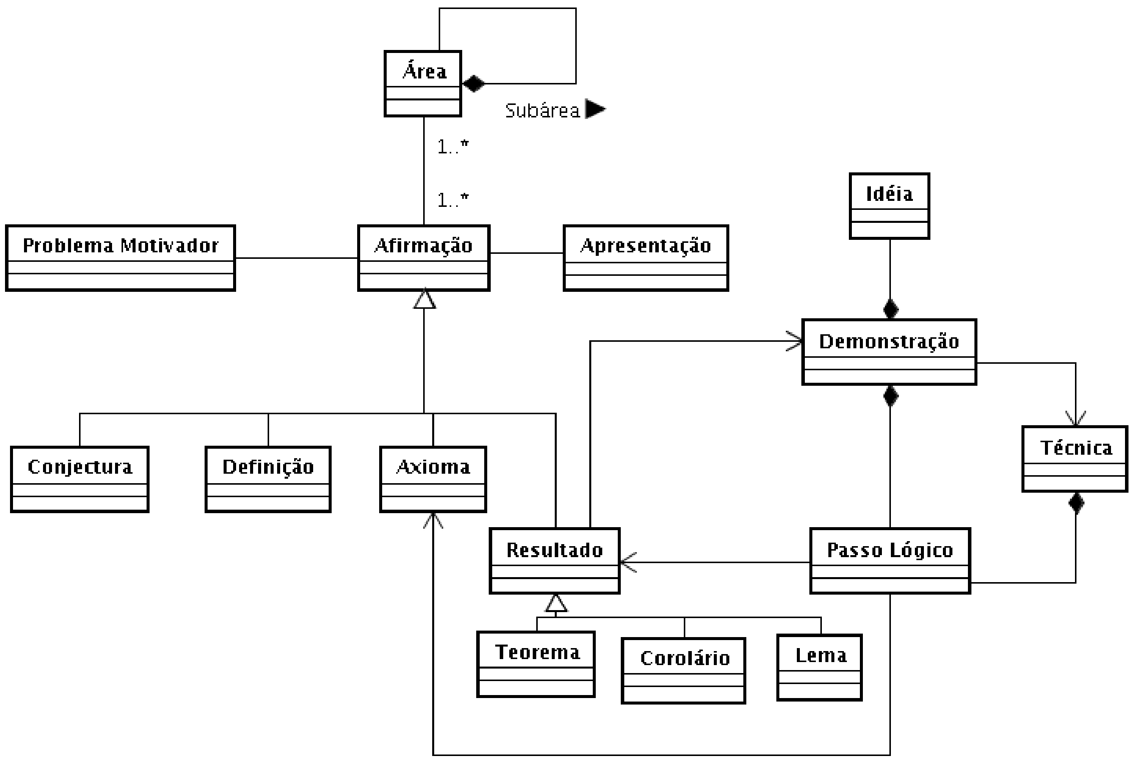
O padrão deve ser utilizado quando:

- For necessário determinar o que é importante considerar, e o que não é, para provar algum fato de uma determinada área do conhecimento.
- Explicitar os fatos são mais importantes.
- Provar algum fato a ser incluso na área.
- Propor novos problemas correlatos a outros problemas já resolvidos ou enunciados (ex: P = NP ?).

4 Estrutura

Ver a figura 1.

Figura 1: Estrutura em UML



5 Participantes

5.1 Área

Descreve uma área de conhecimento formal, tais como estatística, combinatória, topologia[Sim63], teoria dos grafos[BM76], lógica, teoria de Galois[Jac85], teoria de Ramsey[GRS90], programação linear[Dan91], teoria de conjuntos[End77], complexidade computacional[Coo00], entre outras. As áreas podem ter subáreas (exemplo: Complexidade Computacional é subárea de Ciência da Computação).

5.2 Problema Motivador

Algum problema, concreto ou abstrato, que motiva a construção de conhecimento numa área. Exemplos:

- Essa estrutura de rede agüenta o dobro de requisições?
- É possível encontrar uma fórmula para resolução de equações de grau arbitrário e com coeficientes num corpo qualquer?

5.3 Afirmação

Alguma coisa que se diz sobre algum assunto da área em questão. Podem ser motivadas por um ou mais problemas motivadores. Os tipos de afirmação são:

5.3.1 Axioma

Alguma coisa que se toma como verdade. São utilizadas como base do conhecimento das áreas, e podem ser definidas de modo arbitrário (formando os sistemas axiomáticos equivalentes), desde que consistente.

Exemplo: As operações de adição (+) e multiplicação (.) são comutativas: $x + y = y + x$ e $x.y = y.x$

5.3.2 Definição

Nomeia conceitos, conjuntos, ou elementos. Serve para encapsular conceitos, tornar outras definições ou afirmações mais concisas, e cria um vocabulário comum entre referências do assunto.

Exemplo: Definição dos números racionais

$$\mathbb{Q} = \{\frac{m}{n} : m \in \mathbb{Z}, n \in \mathbb{Z}, n \neq 0\}$$

5.3.3 Resultado

Um resultado é algo que é provado (com ao menos uma demonstração) a partir das afirmações de outros resultados ou de axiomas. Dependendo da sua importância e trivialidade (conceito altamente subjetivo) frente a outros resultados, pode ser de 3 tipos:

- Teorema: Resultado em geral muito importante, com várias aplicações. Os teoremas julgados centrais (pelo menos no instante que são nomeados) costumam receber o adjetivo de *Fundamental*.

Exemplo: Todo domínio de integridade finito é um corpo[Gon].

- Proposição: Resultado não central.

  Exemplo: $m > 1$, fixo e $m \in \mathbb{Z}, \bar{a} \in \mathbb{Z}_m \Leftrightarrow mdc(a, m) \neq 1, \bar{a} \neq 0$

- Lema: Resultado considerado trivial, ou de menor importância. Nem sempre é demonstrado. Costuma vir de resultado de refinamento de longas demonstrações de outros tipos de resultados.

- Corolário: Conseqüência imediata (um outro conceito altamente subjetivo) de um outro resultado (em geral que não seja um corolário).

5.3.4 Conjectura

Algo que se supõe ser verdade, mas não há nenhuma prova correta para o fato ou sua negação. Quando demonstrado, torna-se um resultado, e quando refutado, sua negação vira um resultado. Algumas conjecturas também podem se provar indecidíveis dentro de uma teoria (ou seja, a teoria não é capaz de provar ou refutar a conjectura).

5.4 Apresentação

Uma apresentação de uma teoria determina tanto o que é axioma e o que é resultado, além de classificar resultados em teoremas, lemas e corolários. A apresentação de uma teoria pode servir torná-la mais acessível (por exemplo tornando os resultados mais difíceis de serem provados em teoremas), ou apenas mostrar que há mais de um jeito de apresentar as mesmas coisas (contudo, o fato que de dois conjunto de axiomas diferentes é possível demonstrar as mesmas coisas é algo que também precisa ser demonstrado).

5.5 Demonstração

Um conjunto de passos seqüenciais (dentro de um sistema lógico que se julgue apropriado) corretos que mostram que um resultado de fato é verdadeiro. As demonstrações podem ter várias idéias que motivam e norteiam a demonstração.

5.6 Idéia

É uma descrição de alto nível dos passos lógicos e técnicas a serem utilizadas. Podem ser versões mais simples de técnicas muito complexas, ou de outras idéias mais gerais (e portanto mais difíceis de entender).

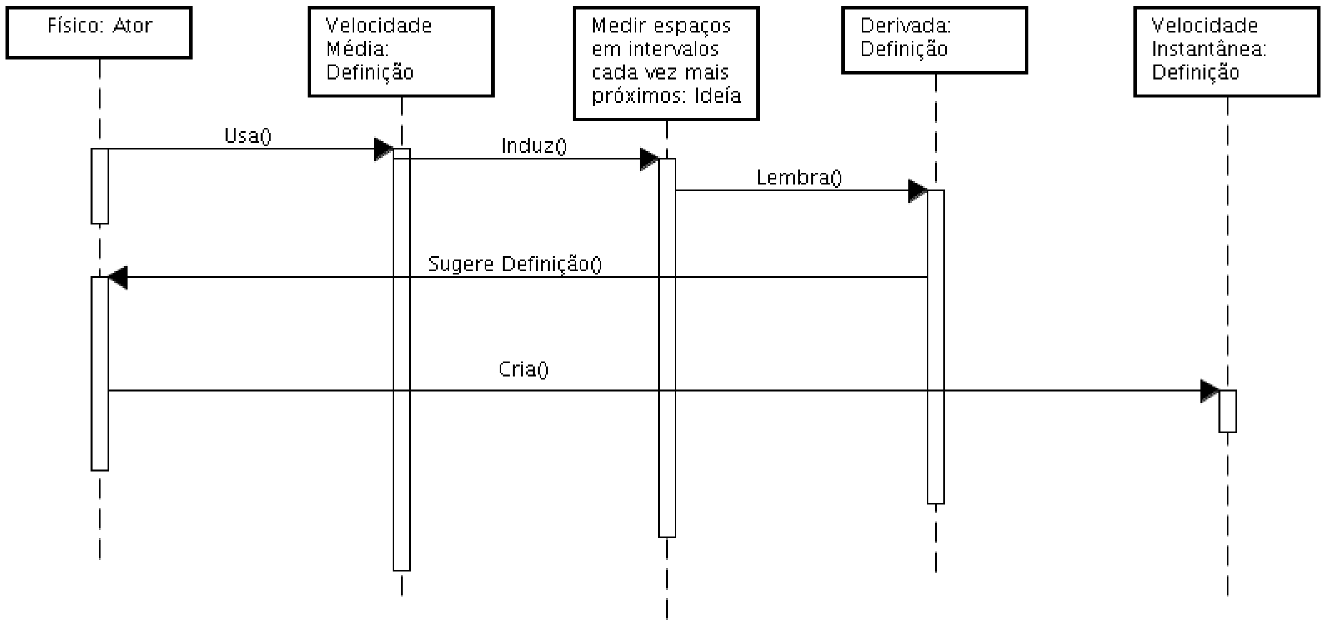


Figura 2: Uma nova definição

Exemplo: Sabemos calcular velocidade média de um corpo. Sabemos que quanto mais curto o tempo entre duas medições de espaço, mais próximos da velocidade instantânea estaremos. Então temos uma idéia similar à de derivada. Surge então a definição da velocidade instantânea em função da derivada da função de espaço sobre o tempo.

5.7 Passo Lógico

Operações lógicas corretas que partem daquilo que já se conhece (resultado ou axioma de alguma área).

5.8 Técnica

As técnicas são padrões (ou fôrmas) de passos lógicos a serem seguidos visando provar algum fato. São o equivalente matemático a um *Template Method*[GHJV95]. Os tipos mais comuns de técnicas são: indução, prova direta, absurdo, construção, e equivalências lógicas (tais como as leis de DeMorgan, ou implicações contrapositivas[Wik06]).

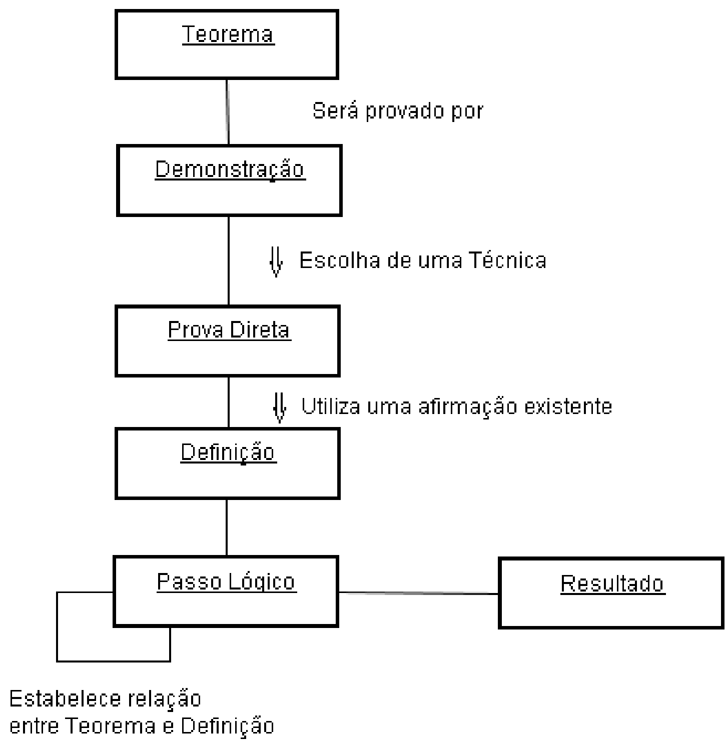
6 Dinâmica

A correta interação entre os participantes apresentados anteriormente é o que garantirá os objetivos propostos. Nesta seção, descreveremos algumas interações.

6.1 Prova de um teorema existente

Na figura(Prova de teorema) apresentamos a interação entre alguns participantes na prova de um teorema. Utilizamos uma definição existente para desenvolver a seqüência de passos lógico e alcançar o resultado almejado.

Figura 3: Prova de teorema



6.1.1 Exemplo

Teorema: $\forall m$ e $n \in \mathbb{Z}$, se $m + n$ é par $\Rightarrow m - n$ é par

Demonstração: Suponha $m, n \in \mathbb{Z}$ (específicos, mas escolhidos arbitrariamente tal que m + n é par.

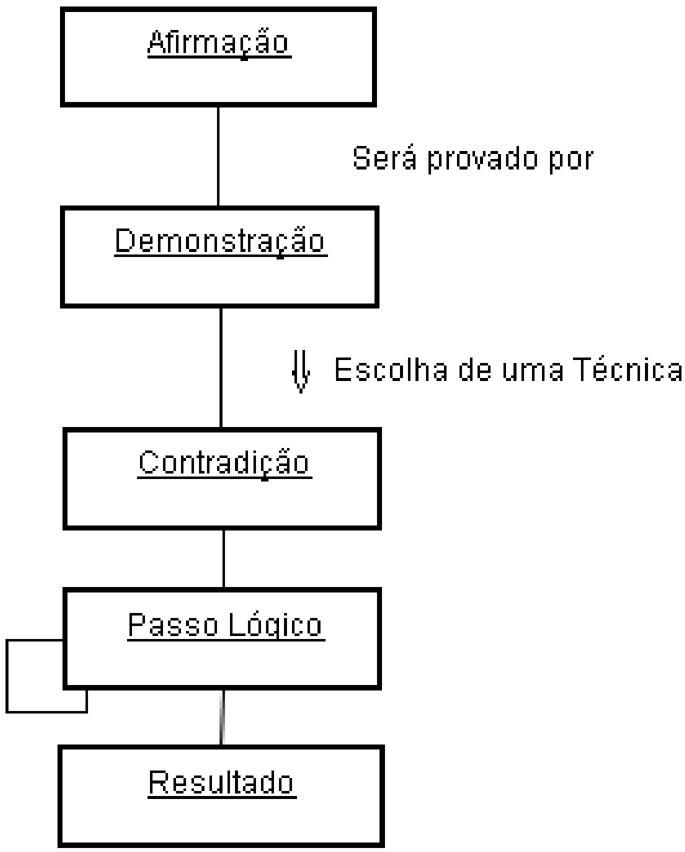
Definição: Pela definição de par, $m + n = 2k$ para algum $k \in \mathbb{Z}$. A diferença entre m e n pode ser expressa como:

$$m - n = (2k - n) - n = 2k - 2n = 2(k - n)$$

Resultado: A expressão $k - n$ é um número inteiro que multiplicado por 2 é um inteiro par.

6.2 Prova de uma afirmação

Figura 4: Prova de afirmação



6.2.1 Exemplo

O exemplo descreve a prova da falsidade da afirmação apresentada. A técnica escolhida foi a contradição.

Afirmação: $\forall a, b \in \mathbb{R}, (a^2 = b^2) \rightarrow a = b$

Demonstração: Suponha $a = 1, b = -1$. Vamos aplicar a igualdade proposta: $a^2 = 1eb^2 = 1$, porém $a \neq b$.

Resultado: $\exists a, b \in \mathbb{R}, (a^2 = b^2) \rightarrow a = b$

7 Conseqüências

- Re-utilização: Com esse padrão, é fácil re-utilzar idéias e técnicas de outras demonstrações para desenhar novas técnicas e idéias. Além disso, torna mais simples as demonstrações, ao indicar quais passos são comuns à outras demonstrações
- Visão do Todo: Fica simples determinar os fatos que possuem mais implicação, os que envolvem mais áreas, sem se preocupar com as demonstrações.
- Visão de Dependências: Caso se busque estudar um resultado em particular, é possível determinar quais afirmações precisam ser estudadas, sem se preocupar com resultados adjacentes, menos relevantes, ou com generalizações.
- Novas demonstrações: É mais simples de descrever demonstrações para novos resultados ou novas demonstrações para um resultado, pois é possível tentar intuir quais técnicas e idéias vão ser utilizadas, além de se poder estudar as propriedades do objeto.

Referências

[BM76] J. A. Bondy and U. S. R. Murty. *Graph Theory with Applications.* American Elsevier, 1976.

[Coo00] Stepnen A. Cook. The P versus NP problem. 2000.

[Dan91] George B. Dantzig. *Linear Programming and Extensions.* Springer, 1991. DAN g2 91:1 P-Ex.

[End77] H. B. Enderton. *Elements of Set Theory.* Academic Press, 1977.

[GHJV95] Erich Gamma, Richard Helm, Ralph Johnson, and John Vlissides. *Design patterns: elements of reusable object-oriented software.* Addison-Wesley Professional, 1995.

[Gon] A. Gonçalves. *Introdução à álgebra.*

[GRS90] R. L. Graham, B. Rothschild, and J. H. Spencer. *Ramsey Theory*. Wiley-Interscience Series in Discrete Mathematics and Optimization. John Wiley & Sons, New York, second edition, 1990.

[Jac85] N. Jacobson. *Basic Algebra I*. Freeman and Company, New York, 2 edition, 1985.

[Sim63] George F. Simmons. *Introduction to Topology and Modern Analysis*. McGraw-Hill, 1963.

[Wik06] Wikipedia. Contrapositive, 2006. [Online; accessed 22-Oct-2006].