Formalização de Resultados Teóricos em Assistente de Provas

Maria Julia Dias Lima* e Cláudia Nalon

Departamento de Ciência da Computação, Universidade de Brasília, Campus Universitário Darcy Ribeiro, Asa Norte, 70910-900, Brasília, DF, Brasil
majuhdl@gmail.com e nalon@unb.br

Resumo Formalização da sintaxe e da semântica da lógica monomodal utilizando assistente de provas Coq, com objetivo de automatização do processo, possibilitando a reutilização dos resultados obtidos.

Palavras-Chave: Lógica modal · Coq · Formalização de resultados.

1 Introdução

Lógica Modal é uma lógica que utiliza operadores modais na construção de sua linguagem [3]. Essa linguagem é utilizada no desenvolvimento de argumentos matemáticos, com base em teoremas, axiomas, criação de modelos, sistemas, provas matemáticas e suas análises.

Tal lógica consiste na utilização de operadores modais, de forma que se possa considerar como situações têm sua verdade ou falsidade alterada se consideramos diferentes situações para essas argumentações. Podemos dividir essa lógica em monomodal e multimodal, relacionando com a quantidade de operadores modais utilizados na construção da lógica (respectivamente, apenas um operador ou mais de um).

Com o objetivo de formalizar a lógica monomodal, foram criadas definições [1] dos principais pontos desse tipo de sistema. Inicialmente, foi definida a sintaxe, constituída das definições relacionadas a como são formadas as fórmulas. Nesse trabalho, a sintaxe é constituída das definições de fórmula bem formada, forma normal negada para as fórmulas, tamanho de fórmulas bem formadas, igualdade sintática e simplificação de fórmulas. Além disso, foi mostrado que a função de transformação de fórmulas em sua forma normal negada é correta e que nenhuma fórmula possui tamanho zero. Com relação à semântica, foi definida a satisfatibilidade das fórmulas bem formadas em suas versão local.

Todos esses resultados foram mostrados em função da definição de Kripke para modelo [3], utilizando as definições teóricas de tipos de mundo, relações, e as funções que os relacionam, gerando tais modelos.

O objetivo deste trabalho é a verificação da correção dessas definições e funções, mostrando que estão corretas, obtendo os resultados desejados. Isso tudo

* A primeira autora recebeu apoio financeiro parcial da Universidade de Brasília por intermédio de bolsa de Iniciação Científica (PIBIC 2020-2021).

deve ser feito de forma automatizada, utilizando a ferramenta de assistente de provas Coq [2].

O Coq [2] utiliza um cálculo construtivo indutivo. A partir dele, são construídas provas utilizando-se de táticas e teoremas já definidos e provados no processo de criação do assistente. Essas definições e as provas se encontram em bibliotecas que são importadas da base do sistema, sendo utilizadas como auxiliares no processo de provas, com o objetivo de facilitar e reutilizar os itens que já foram mostrados previamente no assistente. Tal processo de reutilização permite que seja possível também reutilizar o que está sendo criado nesse projeto em outros projetos futuros, similarmente ao que fazemos com as bibliotecas do assistente.

Esse artigo é formulado da seguinte maneira: na próxima seção, temos as definições formais das definições utilizadas nesse projeto; na seção seguinte, são apresentados os resultados que foram obtidos pela formalização dos conceitos escolhidos no assistente de provas, Coq; e, por fim, temos a seção de conclusão.

2 A lógica modal

Os operadores modais são símbolos que dão às sentenças uma qualificação diferente da original, similar à função de advérbios em uma frase, expandindo o significado do que tínhamos inicialmente. Nesse sentido, podemos caracterizá-la como a expansão de lógicas que não consideram essas qualificações, como a clássica.

Essa lógica possui uma sintaxe e uma semântica. Consideramos aqui apenas a lógica monomodal, com apenas um operador, o de necessidade e seu dual, de possibilidade. Provaremos alguns resultado sobre essas definições na próxima seção.

Definimos sua sintaxe, ou seja, o formato como suas fórmulas devem ser escritas e quais operadores e símbolos utilizaremos. A sintaxe da lógica modal é formada pelo que chamamos de fórmulas bem formadas, FBFs. Primeiramente, definimos o conjunto de proposições P, o conjunto de constantes e os utilizamos para definir as FBFs.

Definição 1 *Denotamos por* $C = \{\mathbf{true}, \mathbf{false}\}$ *o conjunto de* constantes.

Definição 2 *Denotamos por* P *o conjunto enumerável de* símbolos proposicionais*, em que* $P = \{p, q, r, ...\}$*, com elementos indexados ou não.*

Definição 3 *O conjunto das fórmulas bem formadas,* FBF*s, é dado indutivamente a partir do conjunto* P *de símbolos proposicionais, conforme segue:*

- φ *está em* FBF*, se* $\varphi \in C$*,*
- φ *está em* FBF*, se* $\varphi \in P$*,*
- $\neg\varphi$*,* $\Box\varphi$ *e* $\Diamond\varphi$ *estão em* FBF*, se* $\varphi \in$ FBF*,*
- $\varphi \vee \psi$*,* $\varphi \wedge \psi$ *e* $\varphi \rightarrow \psi$ *estão em* FBF*, se* φ *e* $\psi \in$ FBF*s.*

Uma das noções que utilizamos é a de tamanho de uma fórmula, que é dado pela soma da quantidade de todos os símbolos proposicionais e operadores lógicos da fórmula, que, nesse caso, é dada por uma função definida recursivamente.

Definição 4 *O tamanho de uma fórmula é definido por* $f : \mathsf{FBF} \longrightarrow \mathbb{N}$*:*

- $f(\varphi) = 1$*, se* $\varphi \in P$ *ou* $\varphi \in C$
- $f(\neg\varphi) = f(\Box\varphi) = f(\Diamond\varphi) = 1 + f(\varphi)$
- $f(\varphi \wedge \psi) = f(\varphi \vee \psi) = f(\varphi \rightarrow \psi) = 1 + f(\varphi) + f(\psi)$

Utilizamos a Forma Normal Negada (FNN) como uma forma de padronização do formato das fórmulas, com o objetivo de facilitar a leitura de sua sintaxe, além de reduzir os seus operadores somente aos de $\neg, \wedge, \vee, \Box, \Diamond$.

Definição 5 *A Forma Normal Negada tem o formato de uma fórmula com seus operadores reduzidos a* $\neg$*, aplicado somente a símbolos proposicionais, e aos operadores:* $\wedge, \vee, \Box, \Diamond$*.*

Definição 6 *A Forma Normal Negada de uma fórmula é gerada pela função* $g : \mathsf{FBF} \longrightarrow \mathsf{FBF}$*, na qual* $\varphi, \psi \in \mathsf{FBF}$ *e* $p \in P$*:*

- $g(p) = p$
- $g(\mathbf{true}) = \mathbf{true}$
- $g(\mathbf{false}) = \mathbf{false}$
- $g(\neg p) = \neg p$
- $g(\neg\mathbf{true}) = \mathbf{false}$
- $g(\neg\mathbf{false}) = \mathbf{true}$
- $g(\neg\neg\varphi) = g(\varphi)$
- $g(\neg(\varphi \vee \psi)) = g(\neg\varphi) \wedge g(\neg\psi)$
- $g(\neg(\varphi \wedge \psi)) = g(\neg\varphi) \vee g(\neg\psi)$
- $g(\neg(\varphi \rightarrow \psi)) = g(\varphi) \wedge g(\neg\psi)$
- $g(\neg\Box\varphi) = \Diamond g(\neg\varphi)$
- $g(\neg\Diamond\varphi) = \Box g(\neg\varphi)$
- $g(\varphi \vee \psi) = g(\varphi) \vee g(\psi)$
- $g(\varphi \wedge \psi) = g(\varphi) \wedge g(\psi)$
- $g(\varphi \rightarrow \psi) = g(\neg\varphi) \vee g(\psi)$
- $g(\Box\varphi) = \Box g(\varphi)$
- $g(\Diamond\varphi) = \Diamond g(\varphi)$

Para a semântica, é utilizada a noção de modelos de Kripke [3] para a avaliação das fórmulas. Esses modelos são utilizados na definição da semântica dos operadores modais porque utilizamos a noção de mundo e das relações entre eles para definir a satisfatibilidade das fórmulas, especialmente as que utilizam os operadores modais.

Definição 7 *Um* frame *é uma tupla* $\langle W, R\rangle$*, no qual* W *é um conjunto não vazio (de mundos possíveis) e* R *é uma relação em* W*.*

Definição 8 *Um* modelo *é uma tupla* $\langle F, \pi\rangle$*.* W*, no qual* F *é um* frame *e* $\pi : W \longrightarrow (\mathsf{FBF} \rightarrow \{true, false\})$ *é a função de avaliação com relação a esse* frame*.*

Para simplificar notação, no restante do texto nós escrevemos $\langle W, R, \pi\rangle$ ao invés de $\langle\langle W, R\rangle, \pi\rangle$. A semântica é a definição da satisfatibilidade de uma fórmula bem formada, em um determinado modelo, podendo ser ela definida de forma local ou global.

Definição 9 *A satisfatibilidade de uma fórmula na lógica monomodal em um modelo $M = \langle W, R, \pi\rangle$ e um mundo $w \in W$, é dada pela seguinte relação:*

- $\langle M, w\rangle \models$ **true**
- $\langle M, w\rangle \not\models$ **false**
- $\langle M, w\rangle \models p$ *se, e somente se,* $\pi(w, p) = true, p \in P$;
- $\langle M, w\rangle \models \neg\varphi$ *se e somente se* $\langle M, w\rangle \not\models \varphi$
- $\langle M, w\rangle \models \varphi \wedge \psi$ *se, e somente se,* $\langle M, w\rangle \models \varphi$ *e* $\langle M, w\rangle \models \psi$;
- $\langle M, w\rangle \models \varphi \vee \psi$ *se, e somente se,* $\langle M, w\rangle \models \varphi$ *ou* $\langle M, w\rangle \models \psi$;
- $\langle M, w\rangle \models \varphi \rightarrow \psi$ *se, e somente se,* $\langle M, w\rangle \not\models \varphi$ *ou* $\langle M, w\rangle \models \psi$;
- $\langle M, w\rangle \models \Box\varphi$ *se, e somente se,* $\forall w, w' \in W, wRw' \rightarrow \langle M, w\rangle \models \varphi$;
- $\langle M, w\rangle \models \Diamond\varphi$ *se, e somente se* $\exists w, w' \in W, wRw'$ *e* $\langle M, w\rangle \models \varphi$;

Podemos definir a satisfatibilidade localmente, ou seja, em função da existência de pelo menos um mundo em que a fórmula seja satisfeita.

Definição 10 *Uma fórmula φ é* satisfatível localmente *se, e somente se, existe um modelo $M = \langle W, R, \pi\rangle$ e existe um mundo $w \in W$ tal que $\langle M, w\rangle \models \varphi$.*

A semântica é utilizada para que possamos identificar os significados de cada símbolo da fórmula, tornando possível definições como equivalência entre fórmulas, além de provas de correção e completude, e de consistência para a lógica e o cálculo que escolhermos utilizar.

3 Resultados

Como resultados, obtivemos as formalizações no Coq das definições acima, além de provas sobre a correção da transformação fornecida pelas funções de transformação de FBF em FNN e de equivalência semântica entre elas. A formalização e demais documentos referentes a este projeto podem ser encontrados em http://cic.unb.br/~nalon/#software.

3.1 Sintaxe

Inicialmente, foram definidos os conceitos de conjunto de símbolos proposicionais, *Props*, como um conjunto equivalente ao de $\mathbb{N}$ (já que P é enumerável). Além disso, o conjunto de constantes, *Const*, foi definido como contendo os símbolos *tt* e *ff*, que correspondem, na linguagem do provador às constantes **true** e **false**, respectivamente.

```
Definition Props := nat.
Inductive Const: Set := tt | ff.
```

A definição de fórmula bem-formada foi feita de forma indutiva, em função do tipo da fórmula, de forma similar à desenvolvida na teoria, como mostrado abaixo. Por exemplo, a linha "$PropsF : Props \longrightarrow formula$" diz que todo símbolo proposicional é uma fórmula. Já a linha "$Not : formula \longrightarrow formula$" diz que a negação de uma fórmula é uma fórmula. Ou seja, temos que a última parte mostra que temos uma fórmula e as partes anteriores definem do que é formada essa fórmula.

```
Inductive formula : Type :=
  | PropsF : Props → formula
  | ConstF : Const → formula
  | Not : formula → formula
  | And : formula → formula → formula
  | Or : formula → formula → formula
  | Imp : formula → formula → formula
  | Box : formula → formula
  | Diamond : formula → formula.
```

Definimos também a função de tamanho de fórmula, de forma similar a como definimos na teoria, recursivamente, mostrada abaixo. Ela recebe uma fórmula e retorna o seu tamanho. Abaixo, a notação `match` indica que a avaliação do argumento da função é feita por casamento de padrões; o padrão `_` corresponde a todos os não anteriormente especificados.

```
Fixpoint size (f: formula) : nat :=
  match f with
  | PropsF p ⇒ 1
  | ConstF _ ⇒ 1
  | Not f ⇒ 1 + size f
  | And f g ⇒ 1 + (size f) + (size g)
  | Or f g ⇒ 1 + (size f) + (size g)
  | Imp f g ⇒ 1 + (size f) + (size g)
  | Box f ⇒ 1 + (size f)
  | Diamond f ⇒ 1 + (size f)
  end.
```

3.2 Semântica

Nas definições abaixo, extraídas da entrada para o Coq, utilizamos um novo conceito, o conceito de tipos. Um tipo é, basicamente, uma coleção de objetos. No Coq, todos os tipos são habitados, podendo ser interpretados, portanto, como conjuntos não-vazios. O tipo é utilizado para a nossa definição de mundos porque, como visto, o conjunto dos mundos não pode ser vazio na nossa teoria.

```
Definition W := Type.
Definition R := relation W.
```

Definimos, então, um *frame*, também como um tipo. Nessa definição, utilizamos o conceito de conjunto de mundos W, definido acima. Além disso, temos R, um conjunto de relações binárias. Os símbolos % `type` indicam que essa construção deve ser considerada pelo assistente de provas também como um tipo. Essa definição diz que temos um *Frame*, que é um tipo, no qual temos um conjunto de mundos e um conjunto de relações binárias, tais que as relações são definidas entre dois desses mundos.

```
Definition Frame := (W × R) % type.
```

A definição da função de avaliação é feita como na Seção 3.1: dado um mundo W e um símbolo proposicional (nesse caso, um dos símbolos pertencentes ao conjunto *Props*), retorna verdadeiro ou falso (como definidos pelo tipo *bool* em Coq).

```
Definition pi := W → Props → bool.
```

Por fim, a definição de modelo é dada pelas triplas ordenadas de mundos, W, relações, R, e função de avaliação, pi:

```
Definition Model := (Frame × pi) %type.
```

A definição de satisfatibilidade é feita recursivamente para cada formato de fórmula. Para um símbolo proposicional p, a função retorna True (respectivamente, False) se a função pi o avalia para verdadeiro (respectivamente, para falso). No caso de fórmulas complexas, aplica-se recursão. Por exemplo, para a fórmula $\varphi \vee \psi$, recursão é aplicada às suas subfórmulas φ e ψ. Note na definição abaixo que, na notação do provador, *Or* é o operador na linguagem-objeto; o operador $\vee$ simboliza a operação na metalinguagem.

```
Fixpoint sat (M:Model) (w:W) (f:formula): Prop :=
 let R := snd(fst(M)) in
 let pi:= snd M in
  match f with
  | ConstF tt ⇒ True
  | ConstF ff ⇒ False
  | PropsF p ⇒ if (pi w p) then True else False
  | Not f ⇒ ~(sat M w f)
  | And f g ⇒ (sat M w f) ∧ (sat M w g)
  | Or f g ⇒ (sat M w f) ∨ (sat M w g)
  | Imp f g ⇒ ~(sat M w f) ∨ (sat M w g)
  | Box f ⇒ ∀ w':W, (R w w') → (sat M w' f)
  | Diamond a f ⇒ ∃ w':W, (R w w') ∧ (sat M w' f)
  end.
```

A definição de satisfatibilidade local também segue a apresentação da Seção 3.2. Uma fórmula é localmente satisfatível, se existe um modelo e um mundo nesse modelo que satisfaçam a fórmula recebida como entrada.

```
Definition local_sat (f:formula): Prop := ∃ M:Model, ∃ w:W, sat M w f.
```

Duas fórmulas são semanticamente equivalentes se sua avaliação é a mesma em todos os modelos e mundos:

```
Definition eq_semantica (f g : formula) : Prop :=
  ∀ (M:Model) (w:W), sat M w f = sat M w g.
```

3.3 Forma Normal Negada

A função abaixo define fórmulas na Forma Normal Negada (FNN). Tal função recebe uma fórmula em FBF e retorna verdadeiro ou falso, ou seja, se a fórmula está na FNN ou não. Lembrando, o padrão _ corresponde a todos os não anteriormente especificados. Portanto, quando o operador de negação *Not* é aplicado a símbolos proposicionais, a função retorna verdadeiro; aplicado a qualquer outra fórmula, resulta em falso.

```
Fixpoint is_NNF (f:formula): Prop :=
  match f with
  | PropsF p ⇒ True
  | ConstF ff ⇒ True
  | ConstF tt ⇒ True
  | Not (PropsF p) ⇒ True
  | Not _ ⇒ False
  | And f g ⇒ (is_NNF f ) → (is_NNF g)
  | Or f g ⇒ (is_NNF f ) → (is_NNF g)
  | Imp _ _ ⇒ False
  | Box f ⇒ (is_NNF f)
  | Diamond f ⇒ (is_NNF f)
  end.
```

Definimos a função indutiva de transformação de uma fórmula em sua FNN no formato abaixo, preservando as características teóricas. A função recebe uma fórmula em FBF como entrada e retorna outra fórmula em FBF. É importante observar que o Coq só aceita a formalização de funções totais e terminantes. Observa-se da definição abaixo que a função é de fato total. Entretanto, o assistente de prova não consegue encontrar automaticamente as condições de terminação. O motivo é que o resultado da função é aplicado a fórmulas que não são subfórmula da entrada. Por exemplo, da Definição 6, o resultado da aplicação a

$\neg(\varphi \vee \psi)$ é o resultado da recursão sobre $\neg\varphi$ e $\neg\psi$. Estas últimas não são subfórmulas de $\neg(\varphi \vee \psi)$ e, portanto, o assistente não consegue extrair o princípio de indução adequado e provar automaticamente sua terminação. Entretanto, é claramente observável que a recursão ocorre em argumentos de tamanhos menores do que o original. Por isso, esta função foi definida de forma mais geral (utilizando `Function` ao invés de `Fixpoint`) e adicionando-se que o cálculo da terminação é feita em relação ao tamanho da fórmula. Isto é expresso pela anotação {`measure` *size f*} na seguinte definição.

```
Function NNF (f:formula) {measure size f}: formula :=
  match f with
  | PropsF p ⇒ PropsF p
  | ConstF ff ⇒ ConstF ff
  | ConstF tt ⇒ ConstF tt
  | Not (PropsF p) ⇒ Not (PropsF p)
  | Not (ConstF ff) ⇒ ConstF tt
  | Not (ConstF tt) ⇒ ConstF ff
  | Not (Not f) ⇒ NNF (f)
  | Not (And f g) ⇒ Or (NNF (Not f)) (NNF (Not g))
  | Not (Or f g) ⇒ And (NNF (Not f)) (NNF (Not g))
  | Not (Imp f g) ⇒ And (NNF f) (NNF (Not g))
  | Not (Box f) ⇒ Diamond (NNF (Not f))
  | Not (Diamondf) ⇒ Box (NNF (Not f))
  | And f g ⇒ And (NNF f) (NNF g)
  | Or f g ⇒ Or (NNF f) (NNF g)
  | Imp f g ⇒ Or (NNF (Not f)) (NNF g)
  | Box f ⇒ Box (NNF f)
  | Diamond f ⇒ Diamond (NNF f)
end.
```

A prova de terminação é feita por indução no tamanho da fórmula, sendo que a maior parte dos casos é obtida automaticamente através de simplificação pelo assistente de prova, utilizando aritmética linear inteira. Para o caso da implicação, foi necessário utilizar fatos sobre desigualde entre inteiros, mas o restante da prova é obtida automaticamente também com o auxílio da implementação dos procedimentos de prova, no Coq, para a aritmética linear inteira.

Além de totalidade e terminação, é essencial que provemos que a função *NNF* é correta, isto é, mostrar que o resultado da sua aplicação está, de fato, no formato de FNN. O próximo lema mostra a correção da função:

```
Theorem NNF_is_NNF (f:formula) :
  is_NNF (NNF f).
```

A prova do teorema acima é feita por indução sobre o resultado da aplicação de (*NNF f*), que se baseia na medida de complexidade (no tamanho da fórmula) dada acima. A prova é obtida automaticamente pelo provador.

O teorema seguinte mostra que a função de transformação de uma fórmula na sua forma normal negada preserva seu valor semântico.

`Theorem` *eq_f_NNF_f* $(f : formula)$:
$\forall\ (M{:}Model)\ (w{:}W),\ sat\ M\ w\ f \leftrightarrow sat\ M\ w\ (NNF\ f)$.

A prova foi feita por indução em $(FNN\ f)$, assim como na prova de terminação da aplicação da função *FNN* apresentada na seção anterior. Para os casos-base, isto é constantes, símbolos proposicionais ou negações de símbolos proposicionais, as provas são simples e seguem diretamente da definição de satisfatibilidade para estas fórmulas (porque a fórmula e sua forma normal negada coincidem). A hipótese de indução é de que a propriedade vale para fórmulas de tamanho menor que a fórmula que está sendo analisada. Para fórmulas complexas, isto é, com operadores, são aplicadas as hipóteses e a conclusão segue em cada caso com poucas linhas de prova. Por exemplo, precisamos mostrar que, dados um modelo M e um mundo w, o resultado da aplicação de $sat\ M\ w$ para a fórmula $Not\ (Not\ Props\ p)$ é exatamente o mesmo que $sat\ M\ w\ (Props\ p)$, na qual esta última fórmula é o resultado da aplicação $NNF\ Not\ (Not\ Props\ p)$.

4 Conclusão

Neste trabalho, apresentamos uma formalização da lógica monomodal no assistente de provas Coq, baseada em teoremas e definições teóricas. Assim, mostramos ser possível a formalização de conceitos matemáticos teóricos de sintaxe e semântica, relacionados à lógica monomodal na linguagem computacional do assistente de provas. Em um próximo projeto de pesquisa, essa lógica será expandida para a multimodal, completando, assim, essa etapa de formalizações.

Referências

1. Cláudia Nalon, Clare Dixon, and Ullrich Hustadt. 2019. Modal Resolution: Proofs, Layers, and Refinements. ACM Trans. Comput. Logic 20, 4, Article 23 (August 2019), 38 pages. https://doi.org/10.1145/3331448
2. The Coq Proof Assistant, version 8.12.2 (December 2020) https://doi.org/10.5281/zenodo.4501022
3. Melvin Fitting, Richard L. Mendelsohn: First-Order Modal Logic. Springer Science+Business Media, Dordrecht (1998) https://doi.org/10.1007/978-94-011-5292-1