Formalização do Teorema de Modularização da Normalização Forte

Trabalho de Iniciação Científica

Orientador: Prof. Dr. Flávio L. C. de Moura
Departamento de Ciência da Computação
Universidade de Brasília - UnB
e-mail: `flaviomoura@unb.br`

Aluno: Raphael Soares Ramos
Departamento de Ciência da Computação
Universidade de Brasília - UnB
e-mail: `raphael.soares.1996@gmail.com`

Introdução

Sistemas de reescrita são estruturas algébricas constituídas de um conjunto munido de uma operação binária. Modularidade é uma propriedade desejável para sistemas de reescrita porque permite que um sistema combinado herde as propriedades de suas componentes. Terminação não é modular em geral, mas pode ser recuperada sob certas restrições. Nesse trabalho, apresentamos uma formalização do Teorema de Normalização Forte Modular no assistente de provas Coq. Assistentes de provas são programas de computador utilizados para especificar teorias e programas, e provar teoremas sobre estas teorias.

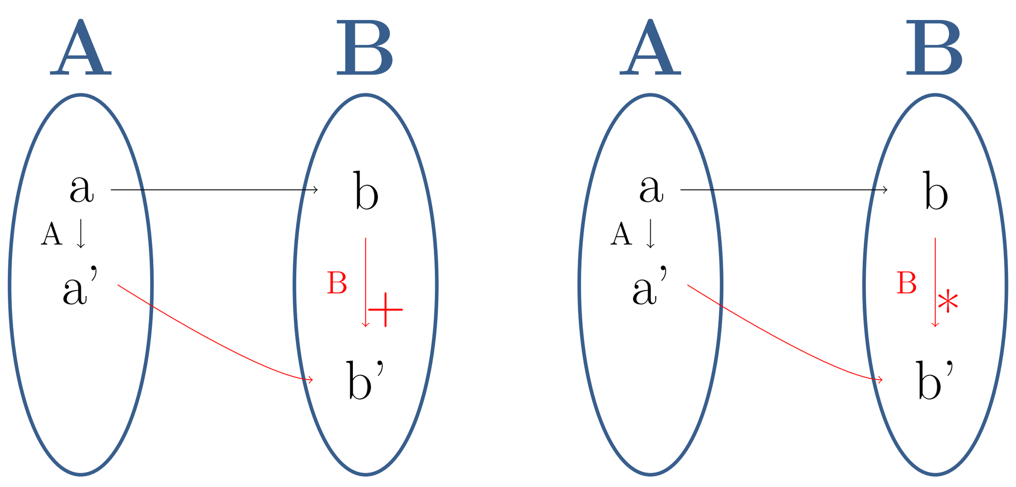
O Teorema de Modularização da Normalização Forte

Uma relação binária sobre um conjunto A é um subconjunto de $A \times A$, que também chamaremos de *relação de redução sobre* A e denotaremos por $\to_A$. Assim, $a \to_A b$ significa que $(a, b) \in A \times A, \forall a, b \in A$. Uma *sequência de redução* é uma sequência da forma $a \to_A a_1 \to_A a_2 \to_A \ldots$, onde a_i é obtido a partir de a após i passos. Neste contexto, $\to_A^+$ (resp. $\to_A^*$) denota o fecho transitivo (resp. reflexivo-transitivo) de $\to_A$. A relação inversa de $\to$ é denotada por $\leftarrow$.

Um elemento $a \in A$ é fortemente normalizável w.r.t. $\to_A$ se toda sequência de redução a partir de a é finita, e neste caso, escrevemos $a \in SN^{\to_A}$:

$$a \in SN^{\to_A} \text{ sse } \forall b, (a \to_A b \text{ implica b } \in SN^{\to_A})$$

Sejam A e B conjuntos munidos de relações de redução $\to_A$ e $\to_B$, respectivamente, e $\to$ uma relação de A para B. Dizemos que $\to_B$ simula fortemente (resp. fracamente) $\to_A$ via $\to$ quando:



Teorema 1 *Sejam A e B conjuntos, $\to$ uma relação de A para B, $\to_1$ e $\to_2$ duas relações de redução em A, e $\to_B$ uma relação de redução em B. Suponha que:*

1. $\to_B$ simula fortemente $\to_1$ através de $\to$;
2. $\to_B$ simula fracamente $\to_2$ através de $\to$;
3. $A \subseteq SN^{\to_2}$.

Então $\leftarrow (SN^{\to_B}) \subseteq SN^{\to_1 \cup \to_2}$. Em outras palavras,

$$\forall a : A, a \in \leftarrow (SN^{\to_B}) \text{ implica } a \in SN^{\to_1 \cup \to_2}.$$

Resultados

A prova do Teorema da Modularização da Normalização Forte foi subdividida em diversas etapas. A seguir, listamos os resultados mais importantes que nos levaram a prova completa deste teorema:

```
Definition patriarchal {A} (red:Red A) (P:A → Prop): Prop :=
  ∀ x, (∀ y, red x y → P y) → P x.

Definition SN {A:Type} (red:Red A) (a:A): Prop :=
  ∀ P, patriarchal red P → P a.

Inductive SN' {A:Type} (red: Red A) (a:A): Prop :=
  sn_acc: (∀ b, red a b → SN' red b) → SN' red a.

Theorem SN'EquivSN {A:Type} {R : Red A} : ∀ t, SN' R t ↔ SN R t.

Lemma WeakStrongSimul {A B} (redA1 redA2:Red A)(redB:Red B)
(R:Rel A B):    WeakSimul redA1 redB R →
        StrongSimul redA2 redB R →
        StrongSimul (redA1 # redA2) redB R.

Lemma SNbySimul {A B} {redA: Red A} {redB: Red B} {R: Rel A B}:
  StrongSimul redA redB R →
  ∀ a, Image (inverse R) (SN' redB) a → SN' redA a.

Lemma inclUnion {A} {redA red'A: Red A}:
  ∀ a, (SN' redA a) → (∀ b, (((refltrans redA) # red'A) a b) →
       SN' (redA !_! red'A) b) → (SN' (redA !_! red'A) a).

Lemma SNinclUnion {A} {redA red'A: Red A}: (∀ b, SN' redA b →
                                  ∀ c, red'A b c → SN' redA c) →
                           (∀ a, (SN' ((refltrans redA) # red'A) a) →
                         (SN' redA a) → (SN' (redA !_! red'A) a)).

Lemma SNunion {A} {redA red'A: Red A}:
  (∀ b, SN' redA b → ∀ c, red'A b c → SN' redA c) →
  ∀ a, (SN' (redA !_! red'A) a) ↔
       (SN' ((refltrans redA) # red'A) a) ∧ ((SN' redA) a).

Theorem ModStrNorm {A B: Type} {redA red'A: Red A}
        {redB: Red B} {R: Rel A B}:
  (StrongSimul red'A redB R) →
  (WeakSimul redA redB R) →
  (∀ b: A, SN' redA b) → ∀ a:A, Image (inverse R) (SN' redB) a →
                                SN' (redA !_! red'A) a.
```

Conclusão

A prova formalizada é construtiva, no sentido que não depende da lógica clássica, o que é interessante do ponto de vista computacional devido ao conteúdo algorítmico correspondente das provas. Provas construtivas são normalmente mais difíceis e elaboradas do que as clássicas, mas são mais preferíveis no contexto da ciência da computação.

O teorema da normalização forte modular é um resultado abstrato que diz as condições para a união de duas relações de redução que preservam a normalização forte. Esse teorema é, por exemplo, aplicado em [1] para estabelecer a propriedade PSN de um cálculo com substituições explícitas.

O projeto com os códigos encontra-se disponível em

`https://github.com/flaviodemoura/MSNorm`.

Referências

[1] KESNER, D. A Theory of Explicit Substituitions with Safe and Full Composition. Logical Methods in Computer Science 5.3:1, 1-29, 2009.

[2] LENGRAND, S. Normalisation & Equivalence in Proof Theory & Type Theory. PhD Thesis. Université Paris 7 & University of St Andrews, 2006.

[3] The Coq Development Team, (2018). The Coq Proof Assistant Reference Manual V8.8. INRIA. Disponível em: `http://coq.inria.fr/coq/distrib/current/refman/`

Instituição de Fomento: FUB