Ciências Exatas e da Terra - Ciência da Computação - Teoria da Computação

Formalização do Teorema de Normalização Forte Modular

Trabalho de Iniciação Científica

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

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

Introdução

Modularidade é uma propriedade desejável de sistemas de reescrita porque permite que um sistema combinado herde as propriedades dos seus componentes. Terminação não é modular, mesmo assim sobre certas restrições modularidade pode ser recuperada. Nesse trabalho, é apresentado uma formalização do Teorema de Normalização Forte Modular no assistente de provas Coq. A prova segue as ideias da tese de PhD do Lengrand [2], mas acredita-se que essa é a primeira formalização deste teorema.

As contribuições deste trabalho podem ser resumidas em:

- Foi construída uma prova construtiva do Teorema de Normalização Forte Modular, e
- foi provado a equivalência entre a definição do Lengrand de normalização forte e a definição indutiva padrão de normalização forte.

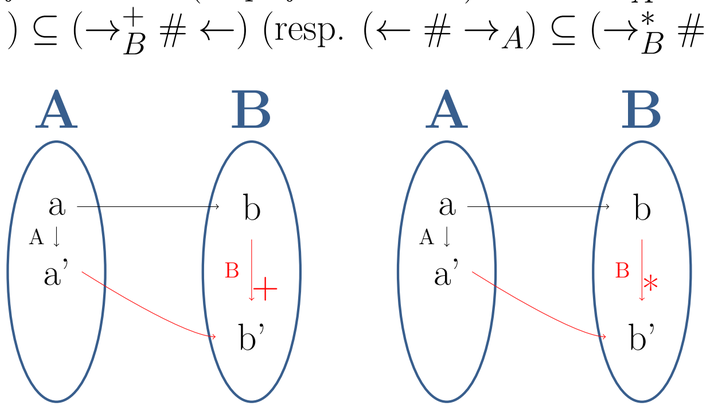
O Teorema de Normalização Forte Modular

Uma relação de um conjunto A para si mesmo é uma relação de redução sobre um conjunto, i.e. uma relação de redução sobre A é um subconjunto de $A \times A$. Uma relação de um conjunto para si mesmo é um *relação de redução sobre um conjunto*, i.e. uma relação de redução sobre A é um subconjunto $A \times A$. Se $\rightarrow_A$ é uma relação de redução sobre A, então uma *sequência de redução* é uma sequência da forma $a_0 \rightarrow_A a_1 \rightarrow_A a_2 \rightarrow_A \ldots$. Uma sequência de redução $a_0 \rightarrow_A a_1 \rightarrow_A a_2 \rightarrow_A \ldots \rightarrow_A a_n\, (n \geq 0)$ é umm n-passos redução de a_0. Uma sequência de redução é finita se ela é uma redução em n-passos para algum $n \in \mathbb{N}$, e infinita caso contrário. Nós escrevemos $\rightarrow_A^+$ (resp. $\rightarrow_A^*$) para o fecho transitivo (resp. reflexivo e transitivo) de $\rightarrow_A$. Um elemento $a \in A$ é fortemente normalizado w.r.t. $\rightarrow_A$ se toda sequência de redução começando de a é finita, e neste caso nós escrevemos $a \in SN^{\rightarrow_A}$. Normalmente, essa ideia é expressada indutivamente como se segue:

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

Para apresentar o teorema, nós precisamos definir as noções de simulação forte e fraca. Nas seguintes definições A e B são conjuntos arbitrários.

Seja $\rightarrow$ uma relação de A para B, $\rightarrow_A$ uma relação de redução sobre A e $\rightarrow_B$ uma relação de redução sobre B. A relação de redução $\rightarrow_B$ *fortemente* (resp. *fracamente*) simula $\rightarrow_A$ através de $\rightarrow$ se $(\leftarrow \# \rightarrow_A) \subseteq (\rightarrow_B^+ \# \leftarrow)$ (resp. $(\leftarrow \# \rightarrow_A) \subseteq (\rightarrow_B^* \# \leftarrow)$).



Seja $\rightarrow$ uma relação de A para B, $\rightarrow_1$ e $\rightarrow_2$ duas relações de redução em A, e $\rightarrow_B$ uma relação de redução em B. Suponha que:

1. $\rightarrow_B$ simula fortemente $\rightarrow_1$ através de $\rightarrow$;
2. $\rightarrow_B$ simula fracamente $\rightarrow_2$ através de $\rightarrow$;
3. $A \subseteq SN^{\rightarrow_2}$.

Então $\leftarrow (SN^{\rightarrow_B}) \subseteq SN^{\rightarrow_1 \cup \rightarrow_2}$. Em outras palavras,

$$\forall a : A, a \in \leftarrow (SN^{\rightarrow_B}) \text{ implica } a \in SN^{\rightarrow_1 \cup \rightarrow_2}.$$

Metodologia

Para verificar formalmente o teorema em questão, optou-se por utilizar o assistente de provas Coq [3], que provê uma linguagem formal com o intuito de facilitar a escrita de definições matemáticas, teoremas e especificações em geral, checando sua validade via *software*. Em relação à prova do teorema de normalização forte modular e da equivalência, a prova foi quebrada em diversos resultados intermediários. O projeto com os códigos está disponível no link: `https://github.com/flaviodemoura/MSNorm`.

Resultados

Lengrand usa a seguinte definição para normalização forte:
$Definition SN \{A : Type\}\{red : Red A\}(a : A) : Prop :=$
$\forall P,\, patriarchal\, red\, P \rightarrow P\, a.$

Neste trabalho foi usada a definição indutiva e foi provado a equivalência entre as duas definições:
Definition SN' {A : Type} {red : Red A} (a : A) : Prop :=
$sn\_acc : (\forall b,\, red\, a\, b \rightarrow SN'\, red b) \rightarrow SN'\, red\, a.$

O teorema seguinte *SNbySimul* é conhecido como normalização forte por simulação. O teorema afirma que se uma relação de redução sobre A, digamos $redA$, é fortemente simulada por uma relação de redução sobre B, digamos $redB$, através de R então a pré-imagem de qualquer elemento que satisfaz o predicado $(SN'redB)$ também satisfaz $(SN'redA)$.

Theorem SNbySimul {A B} {redA : Red A} {redB: Red B} {R: Rel A B} :
$StrongSimul\, redA\, redB\, R \rightarrow \forall a,\, Imagem(inverseR)(SN'redB)\, a$
$\rightarrow SN'redA\, a.$

O lema *SNunion*, que é um resultado também utilizado na prova do teorema principal, dá uma caracterização do predicado $SN'(redA!\_!red'A)$. Uma propriedade importante usada é a chamada estabilidade. Nós dizemos que um predicado P é estável w.r.t. a relação de redução R quando, para todo a e b tal que $R\, a\, b$, $P\, a$ implica $P\, b$.

O Teorema de Normalização Forte Modular é specificado na sintaxe de Coq como abaixo:
Theorem ModStrNorm {A B: Type} {redA red'A: Red A} {redB: Red B}
{R: Rel A B} :
$(StrongSimul\, red'A\, redB\, R) \rightarrow (WeakSimul\, redA\, redB\, R) \rightarrow$
$(\forall b : A,\, SN'\, redA\, b) \rightarrow \forall a : A,\, Imagem(inverseR)(SN'redB)\, a \rightarrow$
$SN'(redA!\_!red'A)\, a.$

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.

Referências

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

[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, (2008). The Coq Proof Assistant Reference Manual V8.2. INRIA. Disponível em: `http://coq.inria.fr/coq/distrib/current/refman/`

Instituição de Fomento: CNPq