

Raport Tehnic și Științific 2017

privind implementarea proiectului PN-III-P2-2.1-PED-2016-0494

December 7, 2017

Implementarea primei faze a proiectului *Formal Verification of Reconfigurable Systems* a fost efectuată între 17 August 2017 și 31 Decembrie 2017. Rezultatele tehnice pentru 2017 sunt conforme cu contractul și sunt:

1. definiția limbajului *H-spec*, care se găsește în documentul [CD17] (disponibil și pe pagina web a proiectului);
2. o librărie de exemple pentru ilustrarea și testarea caracteristicilor principale ale *H-spec*, care se găsește la <https://ontohub.org/forver>.

Acestea sunt discutate în secțiuni separate după cum urmează.

1 Definiția limbajului de specificații *H-spec*

În această secțiune oferim o prezentare generală a caracteristicilor principale ale definiției limbajului *H-spec*. Documentul tehnic complet este disponibil la adresa Web indicată mai sus.

1.1 Caracteristicile limbajului *H-spec*

Un document în *H-spec* constă sau din specificarea a noi logici hibride sau din specificarea unui sistem reconfigurabil într-o logică hibridă.

Logici hibride. Am introdus o sintaxă declarativă pentru specificarea parametrilor metodei generice de hibridizare de logici, introdusă în [DM16], articol care introduce fundamentele teoretice pentru acest proiect. Aceștia sunt:

- numele noii logici hibridizate,
- numele logicii de bază a hibridizării,
- tipurile de simboluri care sunt permise într-o cuantificare,
- constrângerile asupra modelelor logicii hibridizate.

Presupunem ca o librărie de posibile constrângeri pentru fiecare logica de bază este disponibilă, din care utilizatorul poate alege cand specifică o noua logică hibridizată. Două tipuri de constrângeri sunt posibile:

- asupra relațiilor de accesibilitate:
 - reflexivă: $(\forall w)R(w, w)$
 - simetrică: $(\forall w_1, w_2)R(w_1, w_2) \implies R(w_2, w_1)$
 - transitivă: $(\forall w_1, w_2, w_3)R(w_1, w_2) \wedge R(w_2, w_3) \implies R(w_1, w_3)$
 - serială: $(\forall w_1)(\exists w_2)R(w_1, w_2)$
 - euclideană: $(\forall w_1, w_2, w_3)R(w_1, w_2) \wedge R(w_1, w_3) \implies R(w_2, w_3)$
 - funcțională: $(\forall w_1)(\exists! w_2)R(w_1, w_2)$
 - lineară: $(\forall w_1, w_2, w_3)(R(w_1, w_2) \wedge R(w_1, w_3)) \implies (R(w_2, w_3) \vee R(w_3, w_2) \vee @_{w_2} w_3)$
 - totală: $(\forall w_1, w_2)R(w_1, w_2) \vee R(w_2, w_1)$

unde w, w_1, w_2, w_3 sunt lumi posibile și R este relația de accesibilitate între lumi;

- asupra modelelor locale:
 - mulțimea de lumi a fiecărui model local este aceeași,
 - nominalii (numele de lumi) sunt interpretați în același fel în fiecare model local,
 - simbolurile de un anumit tip sunt interpretate în același fel în fiecare model local,
 - funcțiile parțiale au același domeniu de definiție în fiecare model local.

Alternativ, o nouă logică hibridizată poate fi specificată prin adăugarea de noi constrângeri semantice sau noi simboluri permise în cuantificări într-o logică hibridizată existentă.

Specificații în *H-spec*. Specificațiile nestructurate în *H-spec* într-o logică hibridizată au trei părți:

- numele logicii hibridizate,
- numele unei specificații în logica de bază a logicii hibridizate, conținând partea de date a specificației,
- o parte de configurații, constând în declarații de nume de stări și evenimente și în propoziții în logica hibridizată.

Pentru specificații structurate, vom folosi Distributed Ontology, modeling and specification Language DOL [Mos+15]. DOL este un meta-limbaj pentru structurarea ontologiilor, specificațiilor și a modelelor MDE, independent de formalismul utilizat la nivelul specificațiilor nestructurate. O specificație structurată în DOL poate conține părți scrise în logici diferite. Pentru *H-spec* vom folosi doar structurarea omogenă, unde toate specificațiile care apar într-o specificație structurată sunt în aceeași logică.

1.2 Conținutul definiției curente a *H-spec*

1. Sintaxa limbajului *H-spec* este dată în notație BNF. Este structurată în două părți, una pentru sintaxa abstractă și una pentru sintaxa concretă, fiecare din ele împărțite în următoarele sub-părți:
 - a) sintaxa documentelor;
 - b) sintaxa specificațiilor structurate; și
 - c) sintaxa specificațiilor nestructurate.
2. Semantica limbajului *H-spec*, cu următoarele părți:
 - a) o prezentare generală a fundamentelor matematice;
 - b) semantica documentelor;
 - c) semantica specificațiilor structurate;
 - d) semantica specificațiilor nestructurate.

2 Librăria inițială de exemple de specificații în *H-spec*

Această librărie va ilustra și testa principalele caracteristici ale *H-spec*. Se află într-un stadiu inițial, urmând a fi completată în a doua fază a proiectului, când celelalte obiective ale proiectului se vor desfășura. Librăria conține:

- Un exemplu simplu, de tip “hello-world”, care introduce un sistem cu doar trei stări, toate numite explicit. În două dintre ele, o propoziție este adevărată.

Logica specificației este hibridizarea neconstrânsă a logicii propoziționale.

- O rafinare a exemplului precedent în care relația de accesibilitate este complet specificată, în sensul că doar tranzițiile specificate între lumi sunt posibile într-un model.
- Specificarea unui calculator reconfigurabil pentru numere naturale, cu o operație binară care într-o stare a sistemului este suma și în cealaltă este înmulțirea.

Exemplul folosește o hibridizare a logicii de ordinul întâi în care constrângerile semantice sunt date folosind sorturi și operații rigide definite de utilizator.

- Specificarea unui sistem de generare cu două moduri de operare, fiecare cu două sub-moduri: se generează numere pare sau impare, respectiv litere mari sau mici.

Acest exemplu ilustrează o dublă hibridizare a logicii propoziționale unde constrângerile semantice constau în aceleași lumi în modele locale și aceeași interpretare a nominalilor în modelele locale.

- O specificare a unui buffer plastic, cu două moduri de operare: într-unul se comportă ca o coadă iar în celălalt ca o stivă. Acesta este un exemplu de referință care a fost propus în [DM16].
Specificarea ilustrează un proces sofisticat de hibridizare care folosește o constrângere semantică non-tipică, anume că simbolurile de funcții parțiale rigide vor fi interpretate în modelele locale ca funcții parțiale cu același domeniu de definiție.
- Specificația unui sistem ATM cu moduri pentru validarea PIN-ului și operații asupra contului. Specificația este intenționat eronată în funcționalitate și va fi folosită pentru a ilustra demonstrarea consecințelor neintenționate ale sistemului: după validarea PIN-ului, putem opera asupra oricărui cont în loc să putem opera doar asupra contului curent.
Specificarea ilustrează o dublă hibridizare a logicii algebrelor parțiale cu simboluri rigide.
- Specificarea logicilor care apar în exemplele din [DM16] folosind limbajul *H-spec*. Acest exemplu ilustrează construcțiile din *H-spec* pentru declararea de noi logici hibridizate.

References

- [CD17] Mihai Codescu and Răzvan Diaconescu. *H-spec language definition*. 2017.
- [DM16] Răzvan Diaconescu and Alexandre Madeira. “Encoding Hybridized Institutions into First Order Logic”. In: *Mathematical Structures in Computer Science* 26 (2016), pp. 745–788.
- [Mos+15] Till Mossakowski et al. “The Distributed Ontology, Modeling and Specification Language – DOL”. In: *The Road to Universal Logic*. Ed. by Buchsbaum A. Koslow A. Birkhauser, Cham, 2015.

Director de proiect,
Răzvan Diaconescu

