Raport științific final

(2020–2022)

Competiția	**Proiect experimental demonstrativ – PED 2019**
Nr. contract:	404PED/2020
Cod proiect:	PN-III-P2-2.1-PED-2019-0955
Domeniul de cercetare:	Information and Communication Technologies
Titlul:	Verificare Formală Bazată pe Componente
Acronim:	COMP
Dată începere proiect:	23/10/2020
Dată finalizare proiect:	22/10/2022
Durata (luni):	24
Buget total:	597 535 RON
Sursa 1 – bugetul de stat:	597 535 RON
Sursa 2 – alte surse atrase:	0 RON
Pagina web proiect:	`http://imar.ro/~diacon/COMPproject/PN-III-P2-2.1-PED-2019-0955.html`
Instituția coordonatoare:	Institutul de Matematică „Simion Stoilow" al Academiei Române
Director de proiect:	Dr. Habil. Răzvan Diaconescu

1 Realizarea obiectivelor proiectului

Proiectul *Verificare Formală Bazată pe Componente* a avut două obiective majore:

1. să ofere suport pentru dezvoltarea corectă și eficientă a sistemelor bazate pe componente la un nivel avansat, adecvat industriei; și
2. să încurajeze eforturi educaționale în domeniul metodelor formale atât în industrie cât și universități și centre de cercetare.

Ambele obiective au fost realizate în întregime. Mai precis, în ceea ce privește primul obiectiv, în etapa 1 de implementare a proiectului am dezvoltat modelul matematic și definiția unui nou limbaj, numit COMP, care concretizează paradigma de specificare bazată pe compuneri ierarhice de obiecte comportamentale. Fundamentele matematice solide ale limbajului COMP (bazate pe conceptul de echivalență comportamentală în contextul algebrelor multi-sortate cu sorturi ascunse) sunt principalul factor care asigură *dezvoltarea corectă* a sistemelor bazate pe componente. Cel de-al doilea factor major în acest proces este dat de metodologiile de specificare și verificare ale limbajului COMP, dezvoltate în primele două activități ale etapei 2 de implementare a proiectului. Metodologiile de specificare definesc un stil de specificare/programare care garantează existența unei proceduri automate – conform metodologiilor de verificare – de analiză formală a sistemelor bazate pe componente.

Dezvoltarea eficientă a acestor sisteme se realizează cu ajutorul unor instrumente software dedicate, implementate în activitățile 3 (parser), 4 (analiză statică), și 5 (generare de cod) din cadrul etapei 2 de realizare a proiectului, precum și în prima activitate (suport pentru metodologii de verificare) din cadrul etapei 3 de realizare a proiectului. Aceste instrumente pun în practică metodologiile de specificare și verificare, reducând considerabil efortul utilizatorilor/programatorilor și riscul unor erori. Studiile desfășurate în etapa 3 au demonstrat utilizarea limbajului COMP pentru a produce programe concise și corecte. Mai mult, COMP favorizează ierarhiile complexe de obiecte, similare celor larg răspândite în industrie: efortul de programare scade tot mai mult pe măsură ce crește complexitatea ierarhiei de obiecte; de exemplu, studiul de caz a arătat că pentru o ierarhie de adâncime 3, o specificație scrisă în COMP este de două ori mai scurtă decât o specificație echivalentă scrisă într-un limbaj convențional de specificare comportamentală.

Studiul de caz, împreună cu metodologiile de specificare și verificare, contribuie de asemenea la realizarea celui de-al doilea obiectiv al proiectului. Rezultatele obținute în proiect sunt documentate corespunzător: de la documentul care conține o descriere a fundamentelor matematice și definiția limbajului, la ghidul de utilizare a interpretorului, la tutorial, studiul de caz, și alte exemple; toate sunt disponibile pe pagina web a sistemului COMP. Documentele pot fi parcurse în general independent unele de altele și sunt accesibile mai multor categorii de cititori: studenți și cercetători, de exemplu, pentru definiția limbajului și pentru metodologiile de specificare și verificare; sau ingineri de sistem pentru ghidul de utilizare și pentru tutorial. Mai mult, biblioteca de exemple ilustrează separat aspecte diferite ale utilizării limbajului COMP și ale tehnologiei de verificare formală: compuneri paralele, cu sincronizare, indexate, sau analiza de proprietăți cu sau fără constrângeri suplimentare.

2 Nivelul de maturitate tehnologică (TRL)

COMP reunește două sub-tehnologii majore: pe de o parte, o tehnologie de specificare și verificare comportamentală; și pe de altă parte, un puternic motor de rescriere de termeni (Maude). Acestea sunt integrate printr-o suită de biblioteci software, numită SpeX, care facilitează dezvoltarea experimentală de limbaje noi de specificare.

- Încă de la începutul proiectului, am estimat nivelul de maturitate tehnologică al tehnologiei de specificare și verificare comportamentală la 2: conceptele sale fundamentale erau deja formulate și validate de comunitatea științifică printr-o publicație într-un jurnal bine cunoscut. Între timp, în cadrul proiectului, am obținut dovezi experimentale ale conceptului (definiția limbajului în etapa 1, metodologii și interpretor în etapa 2, și tehnici de verificare formală în etapa 3), și am validat tehnologia în condiții de laborator printr-o serie de exemple și printr-un studiu de caz de dimensiuni medii. Prin urmare, estimăm nivelul final al acestei sub-tehnologii la 4.
- SpeX a fost dezvoltat în ultimii 2 ani, în paralel cu implementarea limbajului COMP. În linii mari, SpeX este un mediu software de dezvoltare eterogen pentru specificații și verificări formale. Constă din biblioteci scrise în limbajul Maude care simplifică integrarea de noi limbaje de specificare precum COMP. Tehnologia a fost validată în laborator încă din primul an de implementare a proiectului (prin integrarea unor limbaje convenționale de specificare), și revalidată în cel de-al doilea an de implementare a proiectului în mediul său relevant de utilizare (dezvoltarea de limbaje experimentale) prin integrarea limbajului COMP. Estimăm nivelul final al acestei sub-tehnologii la 5.
- Maude este o tehnologie preexistentă de specificare și analiză formală folosind rescrieri de termeni, cu suport avansat pentru metaprogramare – fără de care actuala implementare a interpretorului COMP nu ar fi fost posibilă. Este un sistem complex și matur din punct de vedere tehnologic, validat prin multiple studii de caz și tool-uri dezvoltate de mai multe echipe de cercetare în ultimele decenii. Estimăm nivelul său de maturitate tehnologică la 5.

Agregând cele trei niveluri de maturitate tehnologică descrise mai sus, obținem un TRL final 4 al întregului sistem COMP (limbaj, metodologii de utilizare, și interpretor), ceea ce corespunde scopului anunțat în propunerea de proiect.

3 Gradul de atingere a rezultatelor estimate

Proiectul și-a propus obținerea a patru rezultate majore:

1. definirea unui limbaj de specificare formală, cu fundamente matematice solide, dedicat compunerii ierarhice de obiecte comportamentale;

2. implementarea unui suport software adecvat pentru limbajul de specificare (compilator/interpretor, API, interfață a utilizatorului);

3. dezvoltarea de metodologii de utilizare a limbajului și a instrumentelor software atât pentru specificarea cât și pentru verificarea obiectelor comportamentale;

4. realizarea unei biblioteci de exemple care ilustrează diferite aspecte ale limbajului și desfășurarea unui studiu de caz de dimensiuni medii.

Toate cele patru rezultate au fost atinse în totalitate, potrivit planului de realizare a proiectului. Primul rezultat a fost obținut în urma activităților 1 (modelul matematic) și 2 (definiția limbajului de specificare formală) din cadrul etapei 1; dezvoltarea documentației corespunzătoare (disponibilă pe pagina web a sistemului COMP) s-a realizat în activitatea 6 a etapei 2 de implementare a proiectului. Cel de-al doilea rezultat a fost obținut în activitățile 3 (parser), 4 (analiză statică pentru evaluarea compunerii de obiecte), 5 (compilator / generare de cod) din cadrul etapei 2, și a fost finalizat în activitățile 1 (verificator) și 3 (interpretor și raportare de erori) din cadrul etapei 3 de implementare a proiectului. Al treilea rezultat a fost obținut în activitățile 1 (metodologii de specificare) și 2 (metodologii de verificare) din cadrul etapei 2, și în activitățile 2 (metodologii de debugging) și 4 (ghid de utilizare a limbajului și interpretorului) din cadrul etapei 3 de implementare a proiectului. Ultimul rezultat a fost obținut în etapa 3 de implementare a proiectului, în activitățile 5 (validare a rezultatelor anterioare printr-un studiu de caz) și 6 (dezvoltarea unei biblioteci de exemple, disponibilă de asemenea pe pagina web a sistemului COMP).

Fiecare rezultat obținut în cadrul proiectului este însoțit de o serie de livrabile (cod sursă, documentație, exemple, etc.) enumerate în secțiunea 6 de mai jos. Prezentări detaliate ale activităților de cercetare / dezvoltare experimentală și ale rezultatelor parțiale sau finale obținute în urma lor sunt incluse în rapoartele științifice și tehnice redactate pentru fiecare dintre cele trei etape de implementare a proiectului.

4 Impactul rezultatelor obținute

Dezvoltarea limbajului COMP și a instrumentelor software aferente de specificare și verificare formală marchează un reper important în evoluția paradigmei de specificare comportamentală. Spre deosebire de abordările convenționale, care folosesc reprezentări structurale fidele ale sistemelor studiate, abordarea comportamentală pune în evidență funcțiile sistemelor și atributele observabile din exterior, fără a investiga funcționarea lor internă. Utilizarea acestei paradigme de specificare produce deseori specificații concise, cu un grad ridicat de generalitate, însă dificil de verificat formal deoarece, în abordarea comportamentală, nu suntem interesați să probăm dacă două stări sunt identice din punct de vedere structural, ci dacă au același comportament.

Proiectul de față rezolvă problema verificării comportamentale în două faze:

1. prin identificarea unei clase bogate de specificații comportamentale – obținute prin compuneri de obiecte – care admit o procedură automată de verificare; și

2. prin dezvoltarea unui limbaj, unor metodologii, și unor tehnici de verificare (cu suport software adecvat) pentru ierarhii de obiecte comportamentale.

Prima dintre cele două faze este de natură teoretică, bazată pe rezultate *state-of-the-art* din domeniul specificațiilor comportamentale care au fost deja validate de comunitatea științifică. Cea de-a doua este de natură experimental-demonstrativă, realizată în a acest proiect: COMP este primul limbaj de specificare și mediu de verificare dedicat compunerii ierarhice de obiecte comportamentale.

În consecință, COMP contribuie la dezvoltarea cercetării de avangardă în domeniul specificării comportamentale. Prin documentația realizată în cadrul acestui proiect și prin instrumentele software implementate (disponibile online sub licență *open source*, și însoțite de ghid de utilizare, tutorial, etc.), COMP are un potențialul educațional ridicat, putând fi utilizat deja în universități și în centre de cercetare. Mai mult, pentru că paradigma de specificare comportamentală – și, în particular, compunerile ierarhice de obiecte comportamentale – s-a dovedit deja, prin studii de caz, a fi adecvată pentru modelări de tehnologii software de tip *object-oriented*, COMP are de asemenea un potențial aplicativ ridicat în industrie.

5 Exploatarea și diseminarea rezultatelor proiectului

Principalul vector de diseminare a rezultatelor proiectului este pagina web `http://imar.ro/~diacon/COMPproject/PN-III-P2-2.1-PED-2019-0955.html`. Aceasta conține, printre alte informații, un link către pagina sistemului COMP: `http://imar.ro/~diacon/COMPproject/COMP.html`, unde sunt publicate documente precum definiția limbajului, ghidul de utilizare, studiu de caz, etc.

Pe lângă pagina web, rezultatele proiectului au fost comunicate și prin participări la seminarii științifice și conferințe. La sfârșitul anului 2021, unul dintre membrii proiectului a ținut o prezentare în cadrul *Logic Seminar*, un seminar științific organizat de Centrul de Cercetare pentru Logică, Optimizare și Securitate (LOS) din cadrul Universității din București împreună cu Institutul de Matematică „Simion Stoilow” al Academiei Române. La discuții au participat studenți și cercetători de la Universitatea din București, de la Institutul de Matematică „Simion Stoilow” al Academiei Române, și de la Universitatea „Alexandru Ioan Cuza” din Iași.

De asemenea, în perioada 28–30 iunie 2022, câteva dintre cele mai importante rezultate ale proiectului au fost prezentate la WADT 2022 (*26th International Workshop on Algebraic Development Techniques*). Workshopul a avut loc în Aveiro, Portugalia, și a fost organizat de membri ai departamentului de matematică din cadrul Universității din Aveiro sub egida IFIP WG 1.3 (*Foundations of System Specification*). Rezumatul și slide-urile prezentate sunt disponibile pe pagina web a sistemului COMP și pe

pagina workshopului, la adresa: `http://wadt2022.web.ua.pt/ListofTalks.html`. În urma expunerii, am primit o invitație de extindere a lucrării astfel încât să poată fi inclusă în volumul post-proceedings *Recent Trends in Algebraic Development Techniques*, ce urmează a fi publicat de Springer în seria LNCS.

Participarea la WADT 2022 și la o serie de discuții și prezentări în cadrul unui seminar intern la care au participat cercetători din Japonia, România, și Spania au contribuit la identificarea unor direcții viitoare de dezvoltare ale limbajului COMP și ale bibliotecilor SpeX ce au permis implementarea sa. În particular, în cazul limbajului COMP, o extensie importantă de interes este de a introduce structuri și funcții generice prin intermediul modulelor parametrizate, ceea ce ar reduce și mai mult efortul de specificare a obiectelor comportamentale. În cadrul bibliotecilor SpeX, am identificat un potențial semnificativ de utilizare a lor pentru a implementa și integra alte limbaje de specificare și verificare. Un prim efort în această direcție a fost demarat deja împreună cu cercetători din Japonia și Spania.

6 Livrabile/indicatori obținuți la finalul proiectului

Nr. crt.	**Livrabile/indicatori planificați**	**Nr.**	**Livrabile/indicatori realizați**	**Nr.**
1	Design și metodologii	2	• definiția limbajului (fundamente matematice, sintaxă, semantică) • metodologii de utilizare	2
2	Suport software	3	Toolset-ul COMP, care include: • parser, analiză statică, și generare de cod • biblioteci suport • interpretor și debugger	3
3	Documentație și exemple	4	• manual de referință • ghid de utilizare • bibliotecă de exemple • studiu de caz	4
4	Diseminare	3	• pagina tehnică a sistemului • tutorial online • prezentare la WADT 2022 (rezumat și slide-uri)	3
5	Managementul proiectului	2	• pagina web a proiectului • rapoarte științifice și tehnice	2

* Rezultate obținute în cadrul proiectului

Proiectul *Verificare Formală Bazată pe Componente* contribuie la înțelegerea sistemelor software pe care le folosim zi de zi – și care ne influențează activitatea – și propune instrumente solid fundamentate din punct de vedere matematic ce pot îmbunătăți calitatea serviciilor oferite de astfel de sisteme. Principalul său rezultat este un mediu integrat de specificare și verificare, numit COMP, dedicat studiului acelor sisteme software pe care le putem descrie prin compunerii ierarhice de obiecte comportamentale: sistemele constau deseori în ansamble de subsisteme sau componente care, la rândul lor, au subcomponente, subsubcomponente, și așa mai departe. Fiecare dintre aceste subsisteme/componente este modelat printr-un obiect comportamental, o entitate pe care o analizăm prin prisma interacțiunilor sale cu alte obiecte, fără a lua în considerare structura sau funcționarea sa internă.

Mediul integrat de dezvoltare formală COMP include, în primul rând, un limbaj avansat de specificare comportamentală adecvat compunerii ierarhice de obiecte, care minimizează efortul necesar descrierii unora dintre cele mai complexe ierarhii. În plus, COMP include o serie de metodologii de specificare și verificare formală care garantează, atunci când sunt folosite împreună, o procedură automată de verificare a proprietăților comportamentale. Acestea sunt însoțite de un interpretor dedicat care implementează metodologiile și de o colecție de exemple ce ilustrează aspecte diferite ale limbajului și câteva dintre principalele funcții ale interpretorului.

Atenția deosebită acordată sistemelor bazate pe ierarhii de obiecte comportamentale face ca setul de instrumente software propus să fie potrivit abordării tehnologiilor orientate pe obiecte, care au o largă utilizare în industrie. Din perspectiva verificării formale, rezultatul culminant al proiectului este că toate verificările pot fi efectuate automat: tehnologia oferită de COMP are o curbă lină de învățare, cu intervenții minime din partea utilizatorilor în timpul verificării.

Director de proiect
Dr. Habil. Răzvan Diaconescu
Data: 22/10/2022

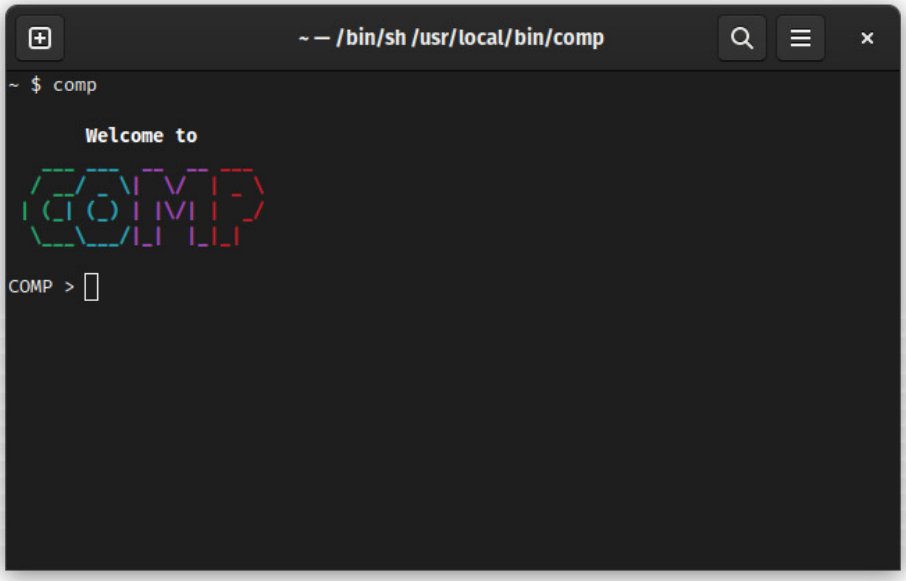

Figura 1: Linia de comandă a interpretorului COMP

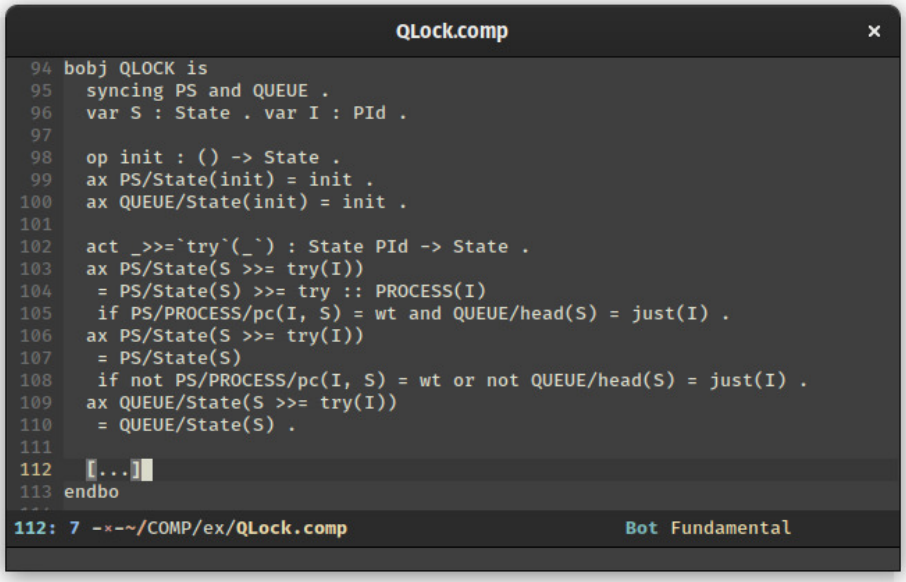

Figura 2: Specificarea unui protocol de excludere mutuală

```
~ — /bin/sh /usr/local/bin/comp
Opening WATCH
* Theorem 2: Pressing the hour-incrementation pusher does not interfere with
    the internal ticking of the watch.
* We rely on the following lemma:
Adding declaration ax not M:Nat = N:Nat if M:Nat < N:Nat = true [label:
    Lemma-2.1]
* Let H, M, and S be the hour, minute, and second indicators, respectively, and
    <59 an arbitrary value less than 59.
Adding declaration op <59 : () -> Nat
Adding declaration ax <59 < N:Nat = true if N:Nat = 59
* For both M and S we distinguish two cases, depending on whether they are less
    than 59, or 59.
Checking tick inc-hour(H:Nat : M:Nat : S:Nat) ~ inc-hour tick(H:Nat : M:Nat :
    S:Nat)
forall (M:Nat = <59 or M:Nat = 59) and (S:Nat = <59 or S:Nat = 59)
| Proved! The property holds.
|____________________________
* QED
Closing WATCH
COMP >
```

Figura 3: Verificarea unei proprietăți comportamentale

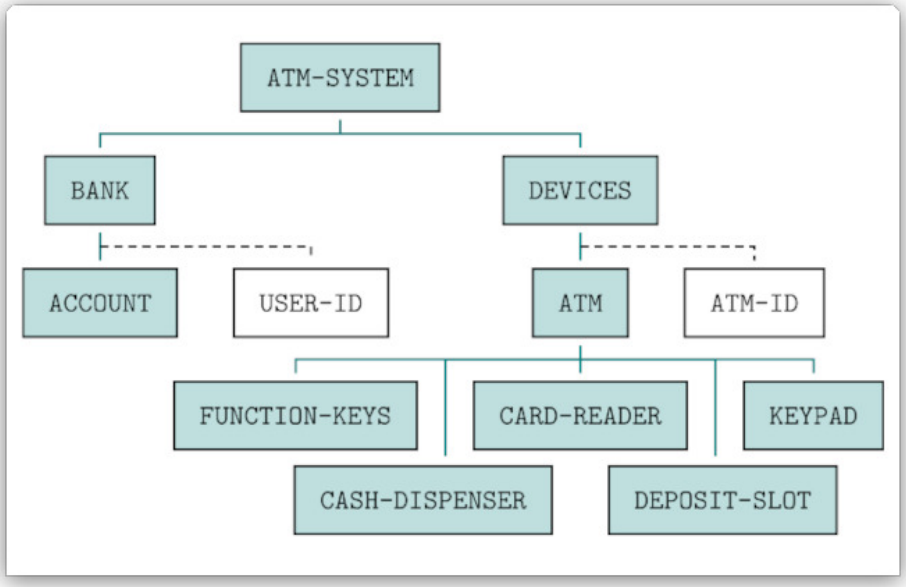

Figura 4: Structura ierarhică a unui sistem de automate bancare