Icelandic Research Fund
Application: 228646-051

1.1 Title and abstract

Title in English

Runtime and Equational Verification of Concurrent Programs

Title in Icelandic

Keyrslutíma- og jöfnusannprófun samhliða forrita.

Acronym

ReVoCoP

Abstract In English

Most modern software is designed or forced to run concurrently with other programs because of the significant increase in efficiency that concurrency offers. However, the complexity of such systems also increases - something that leads to costly and dangerous errors - and verification procedures become more expensive. Additionally, such procedures, when conducted manually, are also prone to human error. Formal verification uses mathematics to analyze systems and therefore removes the latter weakness. We study the underpinnings of two techniques for formally verifying concurrent systems. Concurrency here is modeled through process algebras, and so our initial approach is through equational logic, which is a classic method for analyzing such systems. Here, we search for equational axiomatizations for Milner's Calculus of Communicating Systems (CCS) modulo weak bisimilarity, which is a crucial notion of equivalence between processes underlying their formal verification in the presence of internal computational steps. Second, we study which temporal logics can express specifications for concurrent systems and focus on finding which properties of these logics can be checked at runtime. We finally aim to automate the synthesis of the detection-at-runtime mechanism in order to completely eradicate human error. This project's results will impact both research communities and lead to an increase in the capabilities of formal verification techniques in the field of concurrent programs.

Abstract In Icelandic

Nútíma hugbúnaður er yfirleitt hannaður eða neyddur til að keyra samhliða öðrum forritum til að spara tíma. Hins vegar eykur krafan um samhliða keyrslu flækjustig slíks hugbúnaðar - sem veldur dýrum og skaðlegum villum - og um leið kostnað við að sannreyna hugbúnaðinn. Auk þess býður handvirk sannprófun upp á hættu á mannlegum mistökum. Þann veikleika er hægt að forðast með formlegum stærðfræðilegum greiningaraðferðum. Hér skoðum við undirstöður tveggja aðferða til að sannreyna fjölþráða kerfi formlega. Við notum ferlaalgebru sem líkan fyrir fjölþráða vinnslu, og fyrsta nálgun okkar notar jöfnurökfræði, sem er klassísk aðferð til að greina slík kerfi. Í þessum hluta leitum við að jöfnufrumsemdukerfi fyrir Milner's CCS (samskiptakerfagrunnreikning) miðað við veik tvílíkindi (weak bisimilarity), sem er mikilvægt hugtak um jafngildi ferla sem liggur til grundvallar formlegri sannprófun þegar einingar geta framkvæmt reikninga á milli samskiptaskrefa. Seinni nálgun okkar skoðar hvers konar tímarökfræði má nota til að tjá kröfur til samhliða kerfa og beinir sjónum að því hvaða eiginleika slíkra rökfræðikerfa unnt er að sannprófa á keyrslutíma. Loks er stefnt að því að sjálfvirknivæða uppbyggingu þessara vöktunarkerfa til að útrýma mannlegum mistökum alfarið. Árangur þessa verkefnis mun bæði hafa áhrif á rannsóknarhópa og auka möguleika formlegra sannprófunaraðferða á sviði samtímis keyrslu forrita.

1.2 Expert Panel assignment

Specify the expert panel you wish to review your application	Engineering and technical sciences
Expert Panel subcategory	Computer sciences
Other Scientific category	Computer sciences
Keywords in English	Process Algebra, Epistemic Logic, Equational Logic, Complete Axioms, Runtime Verification, Concurrency, Bisimulation
Keywords in Icelandic	Ferli Algebru, Þekkingarháttarrökfr, Jöfnurökfræði, Fullkomið kerfi, Keyrslutímasannprófu, Samtímis, Bisimulation
Has this proposal previously been submitted to IRF?	No
Is there another proposal for grant year 2022 that includes wages for the doctoral student?	No

1.3 Non-Preferred Reviewer

Non-Preferred reviewer

Name or ID*

Affiliation

Reason for request

1.4 Project Accounting

Institute	Reykjavik University-Department of Computer Science
Project accountant	Anna Lára Gísladóttir
Email	annal@ru.is

2.1 Doctoral student

Id Number	2510954939
Name	Elli Anastasiadi
Initials	EA
Email	elli19@ru.is
Gender	Female
Institute	Reykjavik University-Department of Computer Science
Intitutes initials	RU-DCS
Research Manager	Rannsóknarþjónusta HR
Research Manager Email	rannsoknir@ru.is

2.2 Supervisor(s)

Supervisor

Id Number	0207612459
Name	Luca Aceto
Initials	LA
Email	luca@ru.is
Gender	Male
Institute	Reykjavik University-Department of Computer Science
Intitutes initials	RU-DCS
Research Manager	Rannsóknarþjónusta HR
Research Manager Email	rannsoknir@ru.is

Supervisor

Id Number	1802523989
Name	Anna Ingólfsdóttir
Initials	AI
Email	annai@ru.is
Gender	Female
Institute	Reykjavik University-Department of Computer Science
Intitutes initials	RU-DCS
Research Manager	Rannsóknarþjónusta HR
Research Manager Email	rannsoknir@ru.is

3.1 Duration

One Year

3.2 Work Packages (WP)

Work Package

Name of WP	Ground complete axiomatizations over CCS modulo bisimilarity
Participant accountable for WP	
Start month of WP	1
End month of WP	7
Name of Milestone One	Proof of non finite axiomatic basis for open equations over CCS modulo strong bisimilarity
Month of First Milestone	1
Name of Milestone Two	A complete infinite equational basis for open terms over CCS for strong bisimilarity
Month of Second Milestone	2
Name of Milestone Three	Extension to equational basis for weak bisimilarity
Month of Third Milestone	4
Name of Milestone Four	Proof of independence of the axioms in the complete basis for weak bisimilarity
Month of Fourth Milestone	7

Description

In this WP, we investigate the equational theory of weak congruences over CCS. Weak bisimilarity does not induce a congruence since it is not closed with respect to the alternative composition (plus operator) of processes. To overcome this setback, we have chosen to work with the coarser relations of rooted weak bisimilarity (for the most part) and branching bisimilarity (secondarily). Moller's result for the strong case - that there is no finite ground complete equational basis for CCS - suggests the same will hold for the weak case, a belief that is enforced by our preliminary milestone for this WP that open terms do not afford a finite axiomatization over CCS modulo rooted weak bisimilarity. A way to therefore prove this objective would be to mimic Moller's proof in the weak setting. However, we have chosen to follow an alternative proof technique that provides more intermediate and diverse results. Our technique is as follows: First, we determine an infinite complete basis for CCS modulo strong bisimilarity over open terms, and second, we extend it to the weak setting. Since this basis is proven to be complete, we can then argue that any possible finite basis is a subset of it. Therefore we can construct a proof of the independence of the axioms and use said proof to show that there is no possible finite basis for the case of the closed terms. If this technique is deemed non-fruitful along the way, we can switch to a variation of Moller's proof.

Deliverables and contributing staff

The proposer, Elli Anastasiadi, will contribute five whole months and two part-time months of work in this WP. Luca Aceto and Anna Ingolfsdottir will be supervising her and providing guidance. The first five months are entirely dedicated to this WP, and the two final ones are shared with the following WP. The deliverable of this WP is a journal

paper witch will contain all results. Additionally, we expect more conference and workshop publications containing intermediate results associated with the milestones defined above. Namely, milestone #2 can act as a stand-alone result, which after being published through peer-reviewed processes, can be used as an established proof step for the final result.

Work Package

Name of WP	Concurent Runtime Verification Framework
Participant accountable for WP	
Start month of WP	6
End month of WP	12
Name of Milestone One	A specification logic and a synthesis procedure and monitorability analysis.
Month of First Milestone	9
Name of Milestone Two	A theoretical basis for communication among monitors and the corresponding expressivity increment
Month of Second Milestone	11
Name of Milestone Three	PhD Thesis
Month of Third Milestone	12

Description

In this WP, we investigate the theoretical aspects of concurrent runtime verification. The first step for our plan is to define an expressive enough multi-trace temporal logic for defining multi-component system properties. Then, we aim to determine which part of this logic is monitorable at runtime and under what guarantees. This also implies automating the monitor synthesis procedure for the relevant defined fragments.

In our current approach, each monitor observes only one component (we focus on real-time distributed executions). Therefore, information accumulation regarding the system is performed locally on each monitor and then put together via communication towards a higher level of analysis. This way, every communication increases the amount of knowledge gathered on the higher level about the system, enabling us to gather this information on logical gates and deduce the global properties of the system. However, this monitoring setup has limitations as to what kinds of properties it can detect at runtime. By analyzing this structure, we can deduce this fragment of monitorable properties, and through formula translation, we can automate the synthesis of a monitoring setup.

Our second step in this WP is to allow communication among same-level monitors simultaneously with the execution's observation. We expect this to heavily increment the monitoring capabilities as information about the order in which events took place is partially preserved.

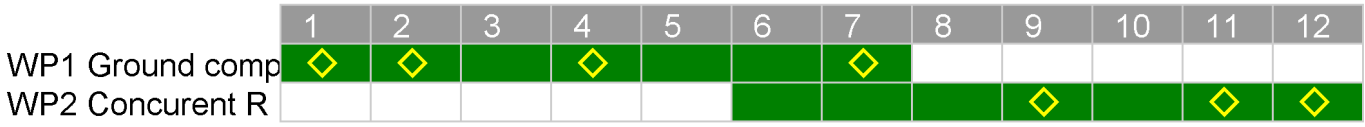
Deliverables and contributing staff

The proposer, Elli Anastasiadi, will contribute five whole months and two part-time months of work in this WP. The PhD thesis will be delivered at the end of the work package, with its text being written throughout the year of the project. Luca Aceto and Anna Ingolfsdottir will be supervising her and providing guidance in both the thesis writing and the research activities. Additionally, Antonios Achilleos, based in RU, and the foreign researchers Duncan Paul Attard, Adrian Francalanza, and Karoliina Lehtinen will collaborate and contribute to this WP. Specifically, this WP demands that many design choices are made, and therefore, it is imperative to have a wide circle of collaborators in

order to make these design choices as widely applicable as possible. Duncan Paul Attard has experience in implementing runtime verification tools, and he is providing valuable feedback regarding design choices that interact with computer architectures and programming language characteristics. Adrian Francalanza has substantial experience in runtime verification, both in theory and implementation, and has collaborated with various - and diverse - research teams. Therefore his feedback and advice ensure the broad applicability of our framework. Antonios Achilleos and Karoliina Lehtinen have a solid theoretical background in automata theory, mathematical logic, and recursion theory, which is invaluable due to the complexity of the mathematical setting we are exploring and the large amount of research published over the years regarding these subjects. In order to maintain this collaboration, we are having weekly virtual meetings and are planning scientific visits among the universities of the team members.

We expect one journal paper as a final deliverable for this WP, in addition to one intermediate conference publication by the end of milestone #1. The intermediate publication assists in establishing the baseline of the proposed framework since the peer-review process will give it credibility, availability, and publicity.

Year 1



3.3 Activity by region

Reykjavík capital area	97 %
Reykjanes peninsula	0 %
W-Iceland	0 %
West fjords	0 %
NV-Iceland	0 %
NE-Iceland	0 %
E-Iceland	0 %
S-Iceland	0 %
Abroad	3 %
Total	100 %

4 Budget - Summary

4.1 Budget Year 1

Total expenses Y1

Person-months & salaries (ISK) Y1

Participant	Institute	Role	Number of Person-months	Salaries per month*	Total
Elli Anastasiadi	RU-DCS	DS	12.0	494.400	5.932.800
Luca Aceto	RU-DCS	SUP	2.0	1.500.000	3.000.000
Anna Ingólfsdóttir	RU-DCS	SUP	1.0	1.200.000	1.200.000

Travel expenses (ISK) Y1

Institute	Total expenses	Explanation
RU-DCS	533.239	Federated Logic Conference (FLoC), 2022, Haifa, Israel. Approximated costs: Registration: Student registration for CAV: 150 euros. Student registration for LICS: 165 euros. Registration total= 315 euros = 46,369 isk Travel costs : Flights: 65.000 isk. According to the Directorate of Internal Revenue, the daily allowance (hotel and allowance) is 222 SDR or 42.187 ISK, for 10 days, 421.870 isk. Total travel cost is 46,369 isk + 65.000 isk + 421.870 isk = 533.239 isk. Total amount applied for : 300.000 isk

Contracted services (ISK) Y1

Institute	Total expenses	Explanation
RU-DCS	0	

Publication expenses (ISK) Y1

Institute	Total expenses	Explanation
RU-DCS	0	

Purchase of Equipment Y1

Institute	Total expenses	Explanation
RU-DCS	0	

Other Financing Y1

Participant	Matching funds	Explanation	Amount
RU-DCS	Salaries	Luca Aceto's salary	3.000.000
RU-DCS	Salaries	Anna Ingolfsdottir's salary	1.200.000
RU-DCS	Travel expenses	Excess Travel cost for FLoC conferences	233.239

RANNSÓKNAMIÐSTÖÐ ÍSLANDS • Borgartún 30 • 105 Reykjavík • Sími 515 5800 • www.rannis.is.
THE ICELANDIC CENTRE FOR RESEARCH • Borgartún 30 • 105 Reykjavík • Tel. (354) 515 5800;

Total expenses Y1

Institute	RU-DCS								Total
Salaries	10.132.800	0	0	0	0	0	0	0	**10.132.800**
Travel expenses	533.239	0	0	0	0	0	0	0	**533.239**
Total	**10.666.039**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**10.666.039**

Own Contribution Y1

Institute	RU-DCS								Total
Salaries	4.200.000	0	0	0	0	0	0	0	**4.200.000**
Travel expenses	233.239	0	0	0	0	0	0	0	**233.239**
Total	**4.433.239**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**4.433.239**

RANNSÓKNAMIÐSTÖÐ ÍSLANDS • Borgartún 30 • 105 Reykjavík • Sími 515 5800 • www.rannis.is.
THE ICELANDIC CENTRE FOR RESEARCH • Borgartún 30 • 105 Reykjavík • Tel. (354) 515 5800;

Applied to IRF Y1

Institute	RU-DCS								Total
Applied %	58	0	0	0	0	0	0	0	**58**
Applied	6.232.800	0	0	0	0	0	0	0	**6.232.800**
Overhead	1.558.200	0	0	0	0	0	0	0	**1.558.200**
Applied with overhead	7.791.000	0	0	0	0	0	0	0	**7.791.000**

RANNSÓKNAMIÐSTÖÐ ÍSLANDS • Borgartún 30 • 105 Reykjavík • Sími 515 5800 • www.rannis.is.
THE ICELANDIC CENTRE FOR RESEARCH • Borgartún 30 • 105 Reykjavík • Tel. (354) 515 5800;

Summary All Years

Total expenses Y

Institute	RU-DCS								Total
Salaries	10.132.800	0	0	0	0	0	0	0	**10.132.800**
Travel expenses	533.239	0	0	0	0	0	0	0	**533.239**
Total	**10.666.039**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**10.666.039**

Own Contribution Y

Institute	RU-DCS								Total
Salaries	4.200.000	0	0	0	0	0	0	0	**4.200.000**
Travel expenses	233.239	0	0	0	0	0	0	0	**233.239**
Total	**4.433.239**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**4.433.239**

RANNSÓKNAMIÐSTÖÐ ÍSLANDS • Borgartún 30 • 105 Reykjavík • Sími 515 5800 • www.rannis.is.
THE ICELANDIC CENTRE FOR RESEARCH • Borgartún 30 • 105 Reykjavík • Tel. (354) 515 5800;

Applied to IRF Y

Institute	RU-DCS								Total
Applied %	58	0	0	0	0	0	0	0	**58**
Applied	6.232.800	0	0	0	0	0	0	0	**6.232.800**
Overhead	1.558.200	0	0	0	0	0	0	0	**1.558.200**
Applied with overhead	7.791.000	0	0	0	0	0	0	0	**7.791.000**

RANNSÓKNAMIÐSTÖÐ ÍSLANDS • Borgartún 30 • 105 Reykjavík • Sími 515 5800 • www.rannis.is.
THE ICELANDIC CENTRE FOR RESEARCH • Borgartún 30 • 105 Reykjavík • Tel. (354) 515 5800;

5.1 Attachments

Project Description template	elli_anastasiadi_Irf_phd_grant_project_descprition_2022.pdf
Project Description Reference list (Bibliography)	elli_anastasiadi_Irf_phd_grant_referrenses_2022.pdf
Cv PhD Student	elli_anastasiadi_irf_phd_grant_CV_2022.pdf
Doctoral student admission statement	Confirmation of registration-PhD in Computer Science-2019 (1).pdf
Cv Supervisor	resume.pdf
Cv Supervisor	CV_2020__1_.pdf