Livro de Resumos:

I WEITC

I Workshop Escola de Inverno em Teoria da Computação

Livro de resumos: I WEITC

I Workshop Escola de Inverno em Teoria da Computação

1 a 4 de agosto de 2017
Niterói, Brasil

Comitê de Programa

Alexandre Rademaker (IBM Research, Brasil)
Aline Paes (UFF, Brasil)
Bruno Lopes (co-chair - UFF, Brasil)
Carlos Olarte (UFRN, Brasil)
Christiano Braga (co-chair - UFF, Brasil)
Cláudia Nalon (UnB, Brasil)
Edward Hermann Haeusler (PUC-Rio, Brasil)
Elaine Pimentel (UFRN, Brasil)
Fábio Protti (UFF, Brasil)
Guilherme Lima (PUC-Rio, Brasil)
Lew Gordeev (Universität Tübingen, Alemanha)
Mario Benevides (UFRJ, Brasil)
Petrucio Viana (UFF, Brasil)
Raquel Bravo (UFF, Brasil)
Renata de Freitas (UFF, Brasil)
Ueverton Souza (UFF, Brasil)
Valeria de Paiva (Nuance Communications, EUA)

Comitê Organizador

Bruno Lopes (UFF, Brasil)
Christiano Braga (UFF, Brasil)

Apoio

Universidade Federal Fluminense

ISBN 978-85-94029-04-1

Lopes, Bruno & Braga, Christiano.

Livro de Resumos: I WEITC/ I Workshop Escola de Inverno em Teoria da Computação.

51 pp. : il.

Livro de resumos: I WEITC 2017. Niterói, 2017.

1. Teoria da Computação. 2. Computação. 3. Lógica. 4. Algoritmos. 5. Livro de resumos. I. Título.

CDD: 160

2017
Instituto de Computação
Universidade Federal Fluminense
Av. Gal. Milton Tavares, s/n
24210-346 Niterói-RJ, Brasil

Conteúdo

Prefácio

Este volume contém os resumos das palestras, mini-cursos e comunicações apresentados no I WEITC: I Workshop Escola de Inverno em Teoria da Computação de 1 a 4 de agosto de 2017 no Instituto de Computação da Universidade Federal Fluminense em Niterói.

O WEICT foi projetado para que alunos de graduação, pós-graduação e pesquisadores em Teoria da Computação em todo o país pudessem se encontrar e trocar idéias e experiências num ambiente amigável e prolífico. Em particular, para que os alunos pudessem apresentar seus trabalhos, receber comentários construtivos de professores e pesquisadores experientes em suas áreas de conhecimento e conhecer o estado-da-arte em pesquisa em Teoria da Computação.

Todas as áreas de Teoria da Computação e afins foram bem-vindas no evento. Foram 24 submissões por alunos de graduação e pós-graduação, sete palestrantes convidados ministradas por Alfio Martini (UFRGS), Eduardo Uchoa (UFF), Edward Hermann Haeusler (PUC-Rio), Gilles Dowek (INRIA), Luís Lamb (UFRGS), Maurício Ayala-Rincón (UnB) e Narciso Martí-Oilet (UCM), além de 4 mini-cursos proferidos por Cláudia Nalon (UnB), Jean-Baptiste Joinet (Univ. Lyon III), Luciana Buriol (UFRGS) e Petrucio Viana (UFF).

Agradecemos aos estudantes por sua participação no evento, aos autores por enviarem seus trabalhos, e aos nossos palestrantes convidados por compartilharem seu conhecimento e experiência conosco. Agradecemos também à UFF por apoiar o evento. O sistema EasyChair foi utilizado no apoio a submissão de resumos e preparação destes anais.

1 de agosto de 2017

Bruno Lopes *(UFF, Brasil)*
Christiano Braga *(UFF, Brasil)*
Organizadores do I WEITC

Preface

This volume contains the papers presented at I WEITC: I Winter School and Workshop in Theoretical Computer Science held on August 1-4, 2017 in Niterói, Brazil, at Instituto de Computação of Universidade Federal Fluminense.

WEITC aimed at bringing together students and researchers from all over the country in Theoretical Computer Science to discuss their work in a friendly and live environment. In particular, WEITC wishes to provide a constructive environment for students, where they may present their work, have comments and suggestions from experienced researchers, and get to know the state-of-the-art in Theoretical Computer Science.

All areas related with Theoretical Computer Science were welcome. We had 24 submissions by graduate and undergraduate students. WEITC had also seven invited talks by Alfio Martini (UFRGS), Eduardo Uchoa (UFF), Edward Hermann Haeusler (PUC-Rio), Gilles Dowek (INRIA), Luís Lamb (UFRGS), Maurício Ayala-Rincón (UnB) and Narciso Martí-Oilet (UCM). Also, four short-courses were given by Cláudia Nalon (UnB), Jean-Baptiste Joinet (Univ. Lyon III), Luciana Buriol (UFRGS) and Petrucio Viana (UFF).

We would like to thank our students for their participation, the authors for submitting their work, and our invited speakers for taking their time to share their expertise with us. We acknowledge the support from UFF. The EasyChair system was used to for submissions and proceedings preparation.

August 1st, 2017

Bruno Lopes *(UFF, Brasil)*
Christiano Braga *(UFF, Brasil)*
Charis of I WEITC

Palestrantes convidados

Simulation of physical phenomena with cellular automata

Gilles Dowek*†

* INRIA

† École normale supérieure de Paris-Saclay
gilles.dowek@ens-paris-saclay.fr

Discrete physics investigates the hypothesis that natural phenomena can be described using finite mathematics only. This hypothesis has a deep connection with another: that the density of information in nature is bounded. In this talk, I will present examples of such descriptions in Newtonian physics, Special Relativity, and General Relativity and discuss whether it is possible to measure the complexity of physical phenomena by the amount of information their description requires.

A discussion on the conjectures NP vs PSPACE and NP vs coNP

Edward Hermann Haeusler*

* Pontifícia Universidade Católica do Rio de Janeiro
hermann@inf.puc-rio.br

The aim of this talk is to open a discussion on the justification of the conjectures NP = coNP and NP = PSPACE by means of purely proof-theoretical arguments. It is well-known, that a positive answer and proof for the later conjecture implies the former one. For strategic reasons, we firstly discuss how to show that NP = coNP by providing polynomial upper-bounds for minimal logic tautologies αG that express that G, a graph, is non-hamiltonian. αG is a valid purely implicational formula in minimal logic. NP = PSPACE, follows by observing in a more subtle way that general purely implicational minimal logic tautologies have polynomial upper-bounds too. The choice for providing a particular proof at first, namely NP = coNP, is pedagogical/strategic and rhetorical. Having proved that NP=SPACE, we can use SAT solvers to solve PSPACE-complete problems, such as testing that a NFA (non-deterministic finite automata) is universal and that a two-person game has winning-strategy. A less straightforward application of our work is to provide a polynomial upper-bound on the minimization of boolean logic circuits up to the third-level (or even higher) since the polynomial hierarchy collapses to the fisrt-level if NP=CoNP.

A logical approach to the verification of concurrent systems

Narciso Martí-Oliet*

* Universidad Complutense de Madrid
narciso@ucm.es

Maude is a high-level language and high-performance system supporting both equational and rewriting computation for a wide range of applications. Maude also provides a model checker for linear temporal logic. The first goal of this talk is to introduce Maude as a framework for modeling concurrent systems and model checking their properties.

The model-checking procedure can be used to prove properties when the set of states reachable from an initial state in a system is finite; when this is not the case, it may be possible to use an equational abstraction technique for reducing the size of the state space. Abstraction reduces the problem of whether an infinite state system satisfies a temporal logic property to model checking that property on a finite state abstract version of the original infinite system.

Thus the second goal is to present a simple method for defining quotient abstractions by means of equations identifying states, and to illustrate this method with several detailed examples, whose proof obligations guaranteeing executability can be discharged with the help of tools available in the Maude formal environment.

Finally, at the end of the talk we will comment recent developments introducing new features like unification, narrowing, SMT constraints, and their combinations.

An Introduction to Interactive Theorem Proving with Isabelle/HOL

Alfio Martini*

* Pontifícia Universidade Católica do Rio Grande do Sul
alfio.martini@pucrs.br

Formal verification is the act of proving or disproving the correctness of algorithms, software and hardware models with respect to a given formal specification. A proof assistant or interactive theorem prover is a software tool to assist with the development of such formal proofs by human-machine col- laboration (Geuvers2009, Harrison2009). Important proof assistants include Isabelle/HOL (Tobias Nipkow and Wenzel 2002), Coq (Bertot and Caste'ran 2004), Agda (Bove et al. 2009) and the HOL family of theorem provers (Gordon 2008). Isabelle is a generic proof assistant. Isabelle/HOL is the specialization of Isabelle for Higher Order Logic (Tobias Nipkow and Wenzel 2002). It allows mathematical formulas to be expressed in a formal language and provides tools for proving those formulas in a logical calculus. In this talk we introduce fundamental constructions for defining logical theories in Isabelle/HOL: inductive types, primitive recursive functions, inductive sets and several proof techniques associated to these powerful specification tools. Proofs are written in a structured proof language that is both human readable and machine-checkable. These concepts are illustrated with the development of an operational semantics for a simple imperative language along the lines of (Nipkow and Klein 2014).

References

Bertot, Y. and Caste'ran, P. (2004). Coq'Art: The Calculus of Inductive Constructions. Texts in Theoretical Computer Science. Springer Verlag.

Bove, A., Dybjer, P., and Norell, U. (2009). A Brief Overview of Agda - A Functional Language with Dependent Types. In TPHOLs, pages 73–78.

Geuvers, H. (2009). Proof Assistants: history, ideas and future. Sadhana Journal, 34:3– 25.

Gordon, M. (2008). Twenty years of theorem proving for hols past, present and future. In TPHOLs, pages 1–5.

Harrison, J. (2009). Handbook of Practical Logic and Automated Reasoning. Cambridge University Press.

Nipkow, T. and Klein, G. (2014). Concrete Semantics - With Isabelle/HOL. Springer.

Tobias Nipkow, L. P. and Wenzel, M. (2002). Isabelle/HOL – A Proof Assistant for Higher-Order Logic. In Lectute Notes in Computer Science, vol. 2283. Springer-Verlag.

Intratabilidade e Otimização: uma Homenagem a David S. Johnson[‡]

Eduardo Uchôa[*] Luciana Salete Buriol[†]

[*] Universidade Federal Fluminense
uchoa@producao.uff.br

[†] Universidade Federal do Rio Grande do Sul
buriol@inf.ufrgs.br

Faremos uma homenagem a David S. Johnson (1945–2016), destacando as suas contribuições para a análise teórica e experimental de algoritmos. Ao longo da sua carreira de 40 anos na AT&T Bell Labs, foi chefe do departamento de Fundamentos Matemáticos de Computação e do departamento de Algoritmos e Otimização. Liderou a ACM na área de Algoritmos e Teoria da Computação, através da criação da conferência ACM-SIAM SODA e do grupo de interesse ACM SIGACT. O seu livro "Computers and Intractability: A Guide to the Theory of NP-Completeness" (com M. Garey) e a série "An Ongoing Guide on NP-completeness" são as referências básicas da teoria que identifica os problemas difíceis. Foi criador dos DIMACS Implementation Challenges e um grande defensor de padrões para garantir o rigor científico na avaliação empírica de algoritmos.

[‡]Trabalho em conjunto com a Profa. Celina Figueiredo (UFRJ)

Treating the undecidable — the case of termination

Maurício Ayala-Rincón*

* Universidade de Brasília
ayala@unb.br

Despite the fact that termination is undecidable, discovering "clues"about termination of algorithms is of great interest in order to decide the correctness of computational processes. In functional programming, proving the totality of recursive specifications is directly related with proving their termination. In this talk, several techniques will be discussed that were and are being specified in the proof assistant PVS and that are crucial for increasing the grade of automation of this property.

50 anos de "Alan M. Turing Award (1966-2016)": Uma Análise do Impacto dos Pesquisadores Premiados na Ciência da Computação e na Sociedade

Luís Lamb*

* Universidade Federal do Rio Grande do Sul
lamb@inf.ufrgs.br

O ano de 2016 marca o Cinquentenário do Prêmio Científico mais importante de Ciência da Computação. A premiação "ACM Alan M. Turing Award", concedida anualmente pela Association for Computing Machinery (ACM), é considerada como equivalente a um "Prêmio Nobel" de Ciência da Computação. Ao longo dessas décadas, pesquisadores de impacto em diversas áreas de pesquisa foram reconhecidos pelo mérito do seu trabalho científico. Estes trabalhos tiveram não somente impacto científico - pois avançaram significativamente as tecnologias usadas por todos - mas transformaram a Ciência da Computação em alavanca de progresso das sociedades mais avançadas, com impactos sociais, culturais e econômicos. Será realizada uma apresentação da evolução da Ciência da Computação nos últimos 50 anos, a partir da contribuição dos vencedores do "Turing Award'. Utilizando como referência as significativas contribuições desses grandes pesquisadores, serão apresentados os impactos científicos nas diversas áreas de conhecimento, a partir do trabalho desses premiados, ilustrando a significativa evolução e relevância da Ciência da Computação. Os trabalhos também serão contextualizados historicamente, ilustrando o seu impacto tecnológico. Finalmente, apresentaremos os impactos sociais, culturais e econômicos que a Ciência da Computação proporciou ao ser humano no último século, a partir das notáveis contribuições desses cientistas.

Mini-cursos

Modal Reasoning through Resolution

Cláudia Nalon*

* Universidade de Brasília
nalon@unb.br

In this tutorial we will examine resolution-based proof methods for propositional modal logics based on the axioms K, T, D, B, 4 and 5. We will briefly review the proof method proposed by Robinson for classical propositional logic as well as the basics of modal logics. We will discuss what needs to be taken into consideration when adapting the classical method to deal with the satisfiability problem for modal languages and look at two different resolution-based methods for families of mono-modal logics: the clausal method proposed by Mints and the non-clausal destructive procedure proposed by Fitting.

Indução, iteração, recursão e boa ordem

Petrucio Viana*

* Universidade Federal Fluminense
petrucio_viana@id.uff.br

Com frequência, usamos os termos “indução”, "iteração"e “recursão” na definição de conjuntos e funções e nas provas das propriedades dos conjuntos e funções definidos por estes processos. Muitas vezes empregamos estes termos como sinônimos e não prestamos atenção nas distinções que devem ser feitas, quando estamos definindo ou provando por indução, iteração ou recursão. Nesta palestra, vamos exemplificar estas diferenças e mostrar como elas se manifestam nas provas das equivalências dos quatro “princípios básicos” que estão por trás das “definições e provas indutivas”: o princípio de indução matemática, o teorema da iteração de funções, o teorema da recursão e o princípio da boa ordem.

Formulações Matemáticas para Problemas de Programação Linear Inteira

Luciana Salete Buriol*

* Universidade Federal do Rio Grande do Sul
buriol@inf.ufrgs.br

Este curso apresenta e discute formulações the Programação Inteira para problemas combinatórios. Inicialmente são apresentadas restrições típicas, e a seguir diversos problemas são formulados. Ao longo do curso são apresentadas formulações de problemas em grafos (conjunto independente, coloração de grafos, caminhos mínimos, fluxo em grafos), o problema do caixeiro viajante, roteamento de veículos, uma variante de timetabling, entre outros problemas. Finalmente, ao final do curso, uma discussão sobre cortes em formulações será apresentada, com exemplos. Além de formular problemas, o curso também tem o objetivo de motivar uma abordagem de resolução de problemas iniciando com modelagem matemática, para depois resolver o problema de forma heurística ou exata. Para tal discussão, são apresentadas diversas situações onde formulações são usadas, e os benefícios que se têm com tal metodologia.

An introduction to Linear Logic[‡]

Jean-Baptiste Joinet*

* Université Jean Moulin – Lyon III
Jean-Baptiste.Joinet@ens.fr

In this three hours lecture, Linear Logic will be presented from a proof-theoretic point of view as a computational decomposition of Classical Logic. In a first part, the main steps leading from Classical Natural Deduction to Classical Sequent Calculus will be presented. The computational nature of the normalization proofs in Intuitionistic Logic (Curry-Howard isomorphism, proofs-as-programs paradigm) will then be recalled. A presentation of Linear Logic, its main fragments and its main computational properties will the be given. A short presentation of the computational dynamics of the exponentials will then be sketched.

[‡]Supported by CAPES and COFECUB (French/Brazilian Program Sh-873-17)

Comunicações

Formal reasoning on KT45n

Victor Ferreira Christiano Braga

* Universidade Federal Fluminense
victorfts@id.uff.br, cbraga@ic.uff.br

A multi-agent system (MAS) Wooldridge (2009) is a collection of autonomous entities, called agents, that collaborate with one another to solve a problem that a single agent could not. Reasoning about knowledge (Fabin et al., 2003, Ch. 4) refers to the idea that agents in a group take into account not only the facts of the world, but also the knowledge of other agents in the group. Applications Huth & Ryan (2004) of this idea include: games, economics, cryptography and protocols. Modal Logic is a suitable formalism to model and reason on MAS, both from knowledge and time perspectives (Fabin et al., 2003, Ch. 4). Logic KT45n is an extension of basic modal logic as follows.

Definition 1 *A model $M = (W, (R_i)_{i \in A}, L)$ of the multi-modal logic KT45n with the set A of n agents is specified by three things:*

1. *a set W of possible worlds;*
2. *for each $i \in A$, an equivalence relation R_i on $W (R_i \subseteq W \times W)$, called the accessibility relations; and*
3. *a labelling function $L : W \to \mathcal{P}(Atoms)$.*

In this work we propose a practical implementation of the logic KT45n so we can prove properties about KT45 theories and use all the tools provided by the logic in a more algorithmic manner. The aim is to then build upon this logic implementation to expand various ideas. The tool lean-prover Avigad et al. (n.d.) has been chosen for the formalization of the logic KT45n, for its robust features assisting theorem proving and also as a case study on the tool itself.

References

Avigad, J., de Moura, L. & Kong, S. (n.d.), *Theorem Proving in Lean*, Microsoft Research, `https://leanprover.github.io/tutorial/tutorial.pdf`.

Fabin, R., Halpern, J. Y., Moses, Y. & Vardi, M. Y. (2003), *Reasoning about knowledge*, MIT Press.

Huth, M. R. A. & Ryan, M. D. (2004), *Logic in Computer Science: Modelling and Reasoning About Systems*, 2nd. ed., Cambridge University Press. ISSN 1471-0684.

Wooldridge, M. (2009), *Introduction to MultiAgent Systems*, 2 ed., Wiley.

Uma avaliação computacional de prova de teoremas em Dedução Natural assistida por computador para lógicas proposicionais[‡]

Bernardo Alkmim* Edward Haeusler†

* Pontifícia Universidade Católica do Rio de Janeiro
bpalkmim@gmail.com

† Pontifícia Universidade Católica do Rio de Janeiro
edward.haeusler@gmail.com

Provar teoremas em lógica proposicional é uma tarefa árdua, mesmo considerando o auxílio de assistentes de prova computacionais. Saber se uma fórmula é um teorema é um problema na classe PSPACE, posto que a lógica em questão admite o princípio da sub-fórmula. A lógica minimal puramente implicacional (MIMP) é PSPACE-completa. Em Dedução Natural [Prawitz (1965)], MIMP tem somente duas regras, transmitindo a falsa impressão que provar teoremas nela é mais fácil que nas outras lógicas proposicionais, não sendo este o caso. MIMP é portanto uma excelente escolha para avaliar provadores de teoremas para lógicas proposicionais.

Nosso trabalho utiliza-se de MIMP como instrumento de medida na avaliação de assistentes disponíveis na Web. Dentre os critérios usados, o uso do recurso computacional será fortemente considerado, assim como um mínimo de interação Humano-Computador. Em relação ao uso de recurso computacional, destacamos o armazenamento e manipulação de provas super-polinomiais.

Os principais fatores que afetam o tamanho de uma prova são as heurísticas utilizadas na demonstração [Seldin (1998)], e que afetam o espaço em memória são as estruturas de dados utilizadas. Daremos destaque ao provador NatDProver do laboratório TecMF da PUC-Rio, explicitando a importância de uma representação interna da árvore de demonstração como um grafo, evitando a repetição de nós que representam predicados lógicos atômicos, tendo como exemplo [Haeusler (2014)].

Palavras-chave:**Lógica Minimal Implicacional**, **Dedução Natural**, **Provadores Automatizados de Teoremas**.

Referências

Haeusler, E. H. (2014), 'How many times do we need an assumption to prove a tautology in minimal logic? examples on the compression power of classical reasoning', *CoRR*.

Prawitz, D. (1965), Natural deduction: a proof-theoretical study, PhD thesis, Almqvist & Wiksell.

Seldin, J. (1998), Manipulating proofs, Unpublished manuscript. URL: `http://people.uleth.ca/%7Ejonathan.seldin/MPr.pdf`.

[‡]Agradecemos à CAPES e ao Cnpq por fundarem nossa pesquisa.

Dominação Vetorial na Família dos Cordais: Um Estudo da Complexidade Computacional

Rodrigo Lamblet Mafort* rodrigomafort@id.uff.br
Fábio Protti* fabio@ic.uff.br

* Instituto de Computação
Universidade Federal Fluminense
Niterói, RJ, Brasil

O problema abordado neste trabalho, denominado Problema da Dominação Vetorial, busca encontrar o menor conjunto de vértices $S \subseteq V(G)$ tal que todo vértice do grafo ou está contido em S ou possui um número previamente estabelecido de vizinhos neste conjunto. Todo vértice que atende a essa restrição é marcado como convertido. Para representar os requisitos necessários para que cada vértice seja convertido utiliza-se um vetor de números naturais onde cada posição armazena o número de vizinhos necessários para a conversão de um vértice do grafo. Este problema também é encontrado na literatura como *Interval Set Selection* e *Target Set Selection*. Para grafos quaisquer, o problema da dominação vetorial é reconhecidamente NP-Completo.

Existem na literatura demonstrações a respeito da complexidade para algumas classes de grafos, dentre elas a família dos cordais. Por exemplo, Booth & Johnson (1982) demonstra que uma restrição ao problema da dominação vetorial, conhecida como *Dominating Set* (todos os vértices demandam apenas um vizinho em S para sua conversão), já é NP-Completo para grafos cordais.

Em contrapartida, a literatura apresenta algoritmos polinomiais para outras classes, como, por exemplo, grafos bloco. O algoritmo proposto por Lan & Chang (2013) encontra em tempo linear um conjunto mínimo capaz de converter grafos bloco (cada componente biconexa é uma clique).

Sendo assim, o foco deste trabalho é estabelecer, na família dos grafos cordais, limiares onde a dominação vetorial deixa de ser NP-Completo, fornecendo algoritmos polinomiais para estes casos, e demonstrar para quais subfamílias este problema permanece intratável computacionalmente.

Uma contribuição deste trabalho é um algoritmo para encontrar um conjunto mínimo capaz de converter grafos split-indiferença. A classe dos grafos split-indiferença é definida pela interseção de duas outras classes: Grafos *Split* e Grafos de Intervalo Próprio. Essa contribuição representa um dos limiares buscados por este trabalho, uma vez que o problema é reconhecidamente NP-Completo para grafos *split*. Por outro lado, um dos problemas que permanecem em aberto, e, portanto, alvo deste trabalho, é determinar qual a complexidade deste problema quando restrito aos grafos de intervalo próprio.

Referências

Booth, K. S. & Johnson, J. (1982), 'Dominating sets in chordal graphs', *SIAM Journal on Computing* **11**(1), 191–199.

Lan, J. K. & Chang, G. J. (2013), 'Algorithmic aspects of the k-domination problem in graphs', *Discrete Applied Mathematics* **161**(10-11), 1513–1520.

Formalizando a teoria de linguagens regulares com o Coq[‡]

Erick Simas Grilo* Bruno Lopes * Aline Paes *

* UFF - Universidade Federal Fluminense
simas_grilo@id.uff.br
bruno@ic.uff.br
alinepaes@ic.uff.br

A teoria das linguagens formais desempenha um papel fundamental na computação, tanto teórica quanto prática. Em particular, a teoria das linguagens regulares possui aplicações importantes, tais como na análise léxica de um compilador e o uso do conceito de máquina de estados finita (um autômato finito) para a execução de instruções de uma máquina.

Assistentes de provas são softwares que fornecem um ambiente computacional seguro para a elaboração de provas. Nesses softwares, como o Coq (Barras et al., 1997) e o HOL4 é possível formalizar teorias, programas, provar tais teorias e provar propriedades acerca de programas em um ambiente onde é exigido menos esforço braçal do usuário e que fornece aspectos de segurança que facilitam a confecção da prova, como evitar erros causados por erros de escrita e evitar passos indevidos tomados durante a prova.

Dentro do conhecimento dos autores, não há muito trabalho feito no sentido de formalizar a teoria das linguagens regulares em assistentes de provas: o trabalho mais recente e mais completo é o de Kaiser (2012), onde é formalizado aspectos como autômatos finitos e expressões regulares, usando a biblioteca SSReflect (http://math-comp.github.io/math-comp/). Outro trabalho é o de Filliâtre (1997), onde o objetivo era provar a equivalência entre expressões regulares e autômatos finitos. Tal biblioteca hoje encontra-se descontinuada.

Nesse espectro, este trabalho visa formalizar os principais aspectos da teoria das linguagens regulares na versão mais atual do Coq, fornecendo uma biblioteca que permite executar os formalismos, verificar teoremas e provar propriedades sobre eles, podendo ser útil para diversos fins. O desenvolvimento pode ser encontrado em https://github.com/simasgrilo/RGCoq.

Referências

Barras, B., Boutin, S., Cornes, C., Courant, J., Filliatre, J.-C., Gimenez, E., Herbelin, H., Huet, G., Munoz, C., Murthy, C. et al. (1997), The Coq proof assistant reference manual: Version 6.1, PhD thesis, Inria.

Filliâtre, J.-C. (1997), Finite automata theory in coq: A constructive proof of kleene's theorem, Technical report, Research Report 97–04, LIP-ENS Lyon.

Kaiser, J.-O. (2012), Constructive Formalization of Regular Languages, PhD thesis, Saarland University.

[‡]Os autores agradecem às agencias de fomento CNPq e FAPERJ pelo apoio à pesquisa

Verification of B Machines through Narrowing

Mauricio Pires Christiano Braga

* Universidade Federal Fluminense
mspires@id.uff.br, cbraga@ic.uff.br

Formal methods are techniques for the specification and validation of systems that uses a mathematical formalism to represent and reason about them. These methods are essential for complex systems where testing is unfeasible, either for financial or security reasons for example. Moreover, now a days many automated formal techniques, such SMT solving De Moura & Bjørner (2011) and model checking Clarke et al. (1999) are part of mainstream software development processes.

The B-method Abrial & Abrial (2005) is a specification and verification method based in Zermelo-Frankel set theory and a variant of classical logic. This method is based on component-based development process. The process begins with an abstract specification of the system and, at each development stage, we non-deterministically choose an action that leads us to a new component, therefore refining it. This new component must preserve the specification of the refined one.

Rewriting Logic Meseguer (1992) is a logical and semantic framework suitable for the specification and verification of concurrent systems. The Maude language and system is a high-performance implementation of Rewriting Logic that supports in an effective way rewriting modulo axioms and model checking by identifying computations on a given system with rewrites in the associated term rewrite system. Recently, symbolic verification Bae et al. (2013) through narrowing (a relation that "answers" the question "which are the terms that rewrite to a given term?") has been incorporated into the system.

This work proposes an approach for reasoning on refinement of B-specifications through the formal semantics of GSL language Braga et al. (2016), an intermediate language of the B method, using Rewriting Logic and verification techniques as symbolic model checking and narrowing on the Maude environment.

References

Abrial, J.-R. & Abrial, J.-R. (2005), *The B-book: assigning programs to meanings*, Cambridge University Press.

Bae, K., Escobar, S. & Meseguer, J. (2013), Abstract Logical Model Checking of Infinite-State Systems Using Narrowing, *in* F. van Raamsdonk, ed., '24th International Conference on Rewriting Techniques and Applications (RTA 2013)', Vol. 21, pp. 81–96.

Braga, C., Deharbe, D., Moreira, A. & Martı-Oliet, N. (2016), A rewriting logic semantics for the generalized substitution language, *in* 'Proceedings of School of Theoretical Computer Science and Formal Methods (ETMF 2016)', pp. 93–104.

Clarke, E., Grumberg, O. & Peled, D. (1999), *Model Checking*, MIT Press.

Caracterização por subgrafos proibidos dos grafos P_4-tidy quase-bipartidos[‡]

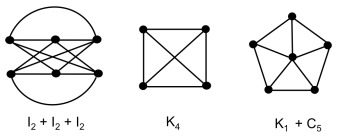
Fábio S. Júnior * Raquel S. F. Bravo * Rodolfo Oliveira *
Uéverton Souza *

* Universidade Federal Fluminense
fabiojunior@id.uff.br, raquel@ic.uff.br, inurao@yahoo.com.br,
ueverton@ic.uff.com

Neste trabalho consideraremos um problema de partição de grafos, estudo esse que tem despertado muito interesse devido às pesquisas em grafos perfeitos e também pela procura de algoritmos eficientes para o reconhecimento de determinadas classes de grafos. Recentemente, foi estudada por Yang & Yuan (2006), uma nova partição em grafos, denominada *quase-bipartição*. Nesse estudo os autores reconhecem grafos que podem ser particionados em um conjunto independente (grafo que não possui arestas entre seus vértices) e um grafo acíclico (grafo que não possui ciclo), denominados *grafos quase-bipartidos*, propondo uma caracterização para grafos com grau máximo 3 e diâmetro 2. Além disso, provaram que o reconhecimento dos grafos quase-bipartidos e NP-completo para grafos onde o grau máximo é 4 ou onde o diâmetro é 4. Com o intuito de reconhecer grafos quase bipartidos, alguns autores estudaram o problema quando restrito à subclasses de grafos. Brandstädt et al. (2013), provaram que o problema é NP-completo para a classe dos grafos P_4-esparso e apresentaram uma caracterização por subgrafos proibidos para a classe dos cografos.

Neste trabalho, apresentaremos uma caracterização por subgrafos proibidos para a classe dos grafos quase bipartidos quando restritos à classe dos grafos P_4-tidy (para qualquer P_4 induzido H de G, existe no máximo um vértice fora de H que juntamente com três vértices de H induzem um P_4). Esta classe de grafos possui o C_5 como subgrafo induzido, e por esta razão, tal classe não pertence a classe dos grafos perfeitos. A seguir, enunciaremos o teorema de caracterização dos grafos P_4-tidy:

Teorema 1 *Seja G um grafo P_4-tidy. G é um grafo quase-bipartido se e somente se G não contém nenhum dos grafos da Figura como subgrafo induzido.*



Referências

Brandstädt, A., Brito, S., Klein, S., Nogueira, L. & Protti, F. (2013), 'Cycle transversals in perfect graphs and cographs', *Theoretical Computer Science* **469**, 15–23.

Yang, A. & Yuan, J. (2006), 'Partitioning the vertices of a graph into one independent set and one acyclic set', *Discrete Mathematics* **306**, 1207–1216.

[‡]Parcialmente financiado pelo CNPq e FAPERJ

Towards natural deduction systems for non-deterministic finite-valued propositional logics

Cecilia Englander Hermann Haeusler

* Departamento de Informática - PUC-Rio

(cenglander, hermann)@inf.puc-rio.br

Resumo

Basically, what we want, is to take the truth-table of a non-deterministic finite-valued propositional logic and from this truth-table, to define a natural deduction system for this logic. For this, we extend [EHP13] on finite-valued propositional logics to non-deterministic finite-valued propositional logics. In [EHP13], a framework for defining natural deduction systems for finite-valued propositional logics was defined based on the methods shown in [Seg83] and [CM09]. In a non-deterministic logic, a k-ary constant may have more than one truth-value assigned for a given vector $\langle x_1, \ldots, x_k \rangle$. This kind of semantics has been recently used for formalizing some logics in a more concise and elegant way[1] (see [AL05, Avr06]).

In order to use the framework described in [EHP13], we interpret a non-deterministic truth-table (Nmatrix) of a logic $\mathcal{L}$ as a disjunction of deterministic truth-tables. Given a k-ary operator $\bigstar$, we are able to define rules for the introduction and elimination of $\bigstar$ based on its Nmatrix. The Natural Deduction system produced is shown to be complete and sound with respect to $\mathcal{L}$.

Referências

[AL05] Arnon Avron and Iddo Lev. Non-deterministic multiple-valued structures. *J. Log. and Comput.*, 15(3), 2005.

[Avr06] Arnon Avron. A non-deterministic view on non-classical negations. *Studia Logica*, 80(2-3), 2006.

[CM09] Carlos Caleiro and João Marcos. Classic-like analytic tableaux for finite-valued logics. In *Proceedings of the 16th International Workshop on Logic, Language, Information and Computation*, WoLLIC '09, pages 268–280. Springer-Verlag, 2009.

[EHP13] Cecilia Englander, Edward Hermann Haeusler, and Luiz Carlos Pereira. Finitely many-valued logics and natural deduction. *Logic Journal of IGPL*, 2013.

[Seg83] K. Segerberg. Arbitrary truth-value functions and natural deduction. *Mathematical Logic Quarterly*, 1983.

[1] Some logics that do not admit finitely matrices have sound and complete semantics for finite Nmatrices.

Coloração de grafos(r,l)

Matheus Souza D'Andrea Alves* Uéverton dos Santos Souza†

* Universidade Federal Fluminense - Instituto de Computação
matheusdandrea@hotmail.com, ueverton@ic.uff.br

A intenção do trabalho é a de explorar e elaborar uma dicotomia para o problema de Coloração mínima em Grafos(r,ℓ) (i.e. grafos que podem ser particionados em r conjuntos independentes e ℓ cliques) quanto a sua complexidade.

Para tanto começaremos os estudos a partir de conhecimentos simples sobre coloração e particionamento de grafos e avançaremos as descobertas demonstrando a intimicidade do problema de coloração mínima em grafos(r,ℓ) e lista coloração em grafos(r,ℓ), demonstraremos particulamente como a armação: Se lista coloração é NP-Completo para Grafos(r,ℓ) então coloração mínima é NP-Completo para Grafos(r,$\ell + 1$), é verdadeira.

Ao final do trabalho mostramos que existe uma dicotomia clara para o problema de coloração mínima na classe dos grafos(r,ℓ) e levantamos perguntas sobre suas características e possibilidade de resolução dos problemas NP-Completos no domínio parametrizado.

Cliques e Conjuntos Independentes em Grafos Prisma Complementares: Complexidade e Tratabilidade Parametrizada

Priscila Pereira de Camargo* Uéverton dos Santos Souza*

* Universidade Federal Fluminense - Instituto de Computação
pripereigo@gmail.com, ueverton@ic.uff.br

Haynes et al., 2007 (2) introduziram os grafos prismas complementares como um caso especial de um produto complementar mais geral e como uma variação do bem conhecido prisma (Hammack et al., 2011 (**?**)). Para um grafo G com um conjunto de vértices $V(G) = \{v_1, ..., v_n\}$ e um conjunto de arestas $E(G)$, o prisma complementar de G é um grafo denotado por $G\overline{G}$ composto por um conjunto de vértices:

$$V(G\overline{G}) = \{v_1, ..., v_n\} \cup \{\overline{v_1}, ..., \overline{v_n}\}$$

e por um conjunto de arestas

$$E(G\overline{G}) = E(G) \cup \{v_iv_j : 1 \leq i < j \leq n \text{ e } v_iv_j \ni E(G)\} \cup \{v_1\overline{v_1}, ..., v_n\overline{v_n}\}$$

Em Duarte et al., 2015 (1) foi estudado algumas questões referentes a complexidade de problemas combinatórios em prisma complementares, tais como clique, conjuntos independentes e k-dominação.

CLIQUE e CONJUNTO INDEPENDENTE são problemas clássicos da Teoria de NP-completude e suas versões parametrizadas são problemas centrais na Teoria da Complexidade Parametrizada, sendo ambos W[1]-completos. Dessa forma, questionamos se existe um algoritmo para resolvê-los cuja complexidade possa ser dividida em duas partes: uma primeira parte polinomial com relação ao tamanho da entrada; e uma segunda parte não polinomial que seja definida puramente em função de um determinado parâmetro que os tornam difíceis. Neste trabalho faremos uma análise da complexidade parametrizada de CLIQUE e CONJUNTO INDEPENDENTE em função do parâmetro k da entrada de ambos problemas. Esta análise será direcionada à classe dos grafos prisma complementares. Através de aplicações da Teoria de Ramsey mostraremos que os problemas CLIQUE e CONJUNTO INDEPENDENTE são tratáveis por parâmetro fixo (FPT) nesta classe de grafos.

Referências

[1] Duarte, M. A., Penso, L., Rautenbach, D., dos Santos Souza, U. (2015).*Complexity properties of complementary prisms.* Journal of Combinatorial Optimization, 1-8.

[2] Haynes, T. W., Henning, M. A., Slater, P. J., van der Merwe, L. C. (2007).*The complementary product of two graphs.* Bulletin of the Institute of Combinatorics and its Applications, 51, 21-30.

Proof Search and Counter-model Generation in Propositional Minimal Implicational Logic[‡]

Jefferson de Barros Santos[*] Bruno Lopes Vieira[†]

Edward Hermann Haeusler[‡]

[*] FGV, Rio de Janeiro, Brazil
jefferson.santos@fgv.br

[†] UFF, Niterói, Brazil
bruno@ic.uff.br

[‡] PUC-Rio, Rio de Janeiro, Brazil
hermann@inf.puc-rio.br

This presentation presents a sequent calculus called $\mathbf{LMT}^{\rightarrow}$ that has the properties to be terminating, sound and complete for Propositional Implicational Minimal Logic ($\mathrm{M}^{\rightarrow}$). $\mathbf{LMT}^{\rightarrow}$ is aimed to be used for proof search in $\mathrm{M}^{\rightarrow}$, in a bottom-up approach. *Termination* of the calculus is guaranteed by a strategy of rule application that forces an ordered way to search for proofs such that all possible combinations are stressed. For an initial formula α, proofs in $\mathbf{LMT}^{\rightarrow}$ has an upper bound of $|\alpha| \cdot 2^{|\alpha|+1+2\cdot log_2|\alpha|}$, which together with the system strategy ensure decidability. System rules are conceived to deal with the necessity of hypothesis repetition and the context-splitting nature of $\rightarrow$-left, avoiding the occurrence of loops and the usage of backtracking. Therefore, $\mathbf{LMT}^{\rightarrow}$ steers the proof search always in a forward, *deterministic* manner. $\mathbf{LMT}^{\rightarrow}$ has the property to allow extractability of counter-models from failed proof searches (*bicompleteness*), i.e., the attempt proof tree of an expanded branch produces a Kripke model that falsifies the initial formula. $\mathbf{LMT}^{\rightarrow}$ is implemented as an interactive theorem prover based on the calculus proposed here.

References

Danos, V., Joinet, J.-B. & Schellinx, H. (1995), 'LKQ and LKT: sequent calculi for second order logic based upon dual linear decompositions of classical implication', *Advances in Linear Logic* **222**, 211–224.

Dowek, G. & Jiang, Y. (2006), 'Eigenvariables, bracketing and the decidability of positive minimal predicate logic', *Theoretical Computer Science* **360**(1), 193–208.

Dyckhoff, R. (1992), 'Contraction-free sequent calculi for intuitionistic logic', *The Journal of Symbolic Logic* **57**(03), 795–807.

Dyckhoff, R. (2016), Intuitionistic decision procedures since gentzen, *in* 'Advances in Proof Theory', Springer, pp. 245–267.

[‡]The authors thank to CNPq and CAPES for supporting this research

Alocação de professores em quadro de horários através de algoritmos de fluxo em redes

Victor Rangel Ramos* Simone de Lima Martins*
Uéverton dos Santos Souza*

* Universidade Federal Fluminense - Instituto de Computação
vrangelramos@gmail.com, simone@ic.uff.br, ueverton@ic.uff.br

Problemas de montagem de quadro de horários são recorrentes nas instituições de ensino e possuem requisitos gerais e específicos a serem atendidos em cada uma delas. Esse tipo de problema é comumente definido como um problema de timetabling Lara (2007) (Burke et al., 1997), o qual pertence ao universo de problemas de alocação descritos por Wren Wren (1996). Esses problemas são classificados como NP-difíceis Lara (2007), devido à complexidade de se obter uma solução computacional com tempo de execução satisfatória. Essa complexidade está ligada ao caráter combinatório do problema, pois existem muitas variáveis a serem atendidas (número de professores, número de disciplinas, horários disponibilizados, requisitos particulares para a alocação).

No timetabling, a alocação de professores pode ser considerada como um dos objetivos a serem atendidos. Embora a alocação de professores seja uma das consequências do resultado do problema de timetabling, ela não é o principal objetivo do problema. Além disso, na prática muitas vezes a tabela de horários das disciplinas é praticamente imutável durante longos períodos, havendo apenas a necessidade de mudança dos professores alocados nas disciplinas em cada semestre. Por essa razão, a utilização de soluções de timetabling, nestes casos, pode ser vista como um esforço desnecessário, pois estamos interessados em apenas uma parte da solução: a alocação dos professores a partir de um quadro de horários já fixado. Sendo assim, neste trabalho consideramos como dado de entrada os horários em que cada disciplina será ofertada e as preferências dos professores pelas disciplinas. Sendo assim o nosso objetivo será a partir de um quadro de horário pré-determinado, buscar uma solução para o problema de alocação de professores para as disciplinas de acordo com suas preferências de modo a maximizar a satisfação global.

Utilizando grafos para remodelar o problema de alocação de disciplinas, desenvolvemos um algoritmo baseado em fluxo em redes para resolver o problema em tempo polinomial.

Referências

Burke, E., Jackson, K., Kingston, J. H. & Weare, R. (1997), 'Automated university timetabling: The state of the art', *The computer journal* **40**(9), 565–571.

Lara, B. (2007), 'Alocação de professores em instituições de ensino superior: Um modelo matemático para o problema de único campus e para o multicampi'.

Wren, A. (1996), 'Scheduling, timetabling and rostering—a special relationship?', *Practice and theory of automated timetabling* pp. 46–75.

Cyber-Physical System Classification and Design Methods

André Metelo * Christiano Braga*

* UFF - Instituto de Computação
metelo@gmail.com
cbraga@ic.uff.br

Cyber-Physical Systems (CPS) [Alur (2015)] are ever present in our daily life. They can be intuitively described as systems that are controlled by one or more computer based components tightly integrated with a set physical ones, typically described as sensors and actuators. The Internet of Things (IOT) [Greengard (2015)] is a nice example of a subclass of CPS.

Due to their complexity, rigorous techniques for the specification, verification and validation of CPS are in ever growing need. The state-of-the art of such techniques include mathematical models such as dynamical systems [Brin & Stuck (2003)], formal models such as hybrid automaton and cellular automaton, verification techniques by simulation and validation by model checking. As a matter of fact, dynamical systems (DS) are a very suitable mathematical model for such systems as CPS depend on its interactions, some times intrusive, with the *physical world*, DS fits in perfectly to model them.

This work studies the state of affairs of such methods for the formal design of CPS. We are particularly interested in understanding how suitable Topoi theory [Goldblatt (1984)], a branch of Category Theory closely coupled with mathematical logic. The underlying logic of a topos, the so called Local Set Theory, appears as a natural candidate to model such complex systems.

Hopefully the models created in this work will lay down the foundation needed by the formal methods to develop advanced computer aided CPS verification techniques and tools.

References

Alur, R. (2015), *Principles of Cyber-Physical Systems*, The Mit Press.

Brin, M. & Stuck, G. (2003), *Introduction to Dynamical Systems*, Cambridge University Press.

Goldblatt, R. (1984), *Topoi: The Categorial Analysis of Logic*, Elsevier Science Punlisher.

Greengard, S. (2015), *The Internet of Things*, The MIT Press.

Estudo sobre propriedades de um sistema ciber-físico para controle de qualidade de água em ambientes industriais.

Diego Brandão* Christiano Braga† Fabricio Lopes e Silva*
Cristiano Carvalho*

* Centro Federal de Educação Tecnológica Celso Suckow da Fonseca
diego.brandao@eic.cefet-rj.br

† Instituto de Computação, UFF
cbraga@ic.uff.br

A água é um recurso essencial para existência e manutenção da vida, sendo sua preservação de suma importância para a sociedade. Os riscos ambientais e de saúde associados a uma possível escassez de água são inúmeros, o que deveria tornar crescente a busca de novas fontes de abastecimento, mas principalmente de novas medidas de proteção e controle da poluição. Nesse contexto, o gerenciamento dos recursos hídricos tem como objetivo principal garantir o suprimento de água em quantidade suficiente e qualidade satisfatória. Apesar de toda sua importância, o processo de monitoramento da qualidade de água no Brasil ainda é rudimentar, pesquisadores realizam esse controle de forma quase manual. No entanto, os enormes avanços em ciência e tecnologia oferecem ferramentas valiosas para enfrentar os desafios da sustentabilidade da água. As principais tecnologias, incluindo de detecção, comunicação sem fio, modelagem hidrodinâmica, análise de dados e o controle, permitem projetar sistemas ciber-físicos (CPS) que agregam inteligentemente sensores sem fio, processadores e atuadores capazes de sentir e interagir com o ambiente aquático (Wang et al., 2015), (Alur, 2015). No entanto, a interação entre os componentes "ciber" e "físicos" consiste em um problema crítico, pois a detecção, a rede, a computação e o controle precisam ser profundamente integrados em todos os componentes da CPS, além da necessidade de que todos os seus componentes sejam interoperáveis com um design correto. A complexidade de tais sistemas demandam métodos mais eficientes para garantir sua especificação precisa e garantia de correção. Nesse contexto, a verificação formal de sistemas permite que a partir de um modelo formal do sistema sejam estudadas propriedades que garantam o seu funcionamento correto. O presente trabalho apresenta algumas discussões sobre uma primeira abordagem formal decorrente de um modelo matemático para o problema de controle de qualidade de água em ambientes industriais.

Referências

Alur, R. (2015), *Principles of Cyber-Physical Systems*, The Mit Press.

Wang, Z., Song, H., Watkins, D., Ong, K., Xue, P., Yang, Q. & Shi, X. (2015), 'Cyber-physical systems for water sustainability: challenges and opportunities', *IEEE Green Communications and Computing Networks* pp. 216–222.

Exploring the SUO-KIF semantics

Fabricio Chalub* Alexandre Rademaker* Edward Hermann†

* IBM Research

† PUC-Rio

The Suggested Upper Merged Ontology (SUMO) [4] and its domain ontologies form the largest formal public ontology in existence today. They are being used for research and applications in search, linguistics and reasoning. SUMO is the only formal ontology that has been mapped to all of the WordNet lexicon [2]. SUMO is written in the SUO-KIF language , a knowledge representation and interchange format. SUO-KIF has its roots in the KIF language [3]. Although SUMO is commonly described as an ontology in classical first-order, many of its axioms appear to go beyond FOL, having some use of high-order logics and constructors for modalities such as: alethic, epistemic, deontic and temporal.

From a practical point of view, SUO-KIF and SUMO are not "executable" since there is no automated theorem prover capable of reading SUMO files directly. To overcome this limitation, the Sigma Knowledge Engineering Environment (Sigmakee) [4] was developed. It is a system for developing, viewing and debugging SUMO theories. Sigmakee can export SUMO theories to the TPTP FOF language . The TPTP (Thousands of Problems for Theorem Provers) [5] is a library of problems, in classical logic with an interpreted equality symbol, for Automated Theorem Proving (ATP) systems. It contains problems in typed higher-order form (THF) — simply typed lambda calculus, typed first-order form (TFF) — monomorphic typed first-order logic with predefined numeric types, first-order form (FOF) — classical first-order logic with quantifiers, and clause normal form (CNF) — first-order logic in conjunctive clausal form. This library supplies the automated reasoning community with a comprehensive library of the ATP test problems that are available today, in order to provide an overview and a simple, unambiguous reference mechanism.

In this article, we report our effort to understand the semantic of SUO-KIF language from a practical point of view. For that, we reimplemented [1] the SUMO to TPTP FOF transformation revisiting all design decisions implemented in Sigmakee such as how to deal with: variables in the predicate position, row variables, sort restriction in axioms and the impact of the high-order axioms. In our SUMO high-order translation, since we are not primarily focusing on automation, but mainly in the extensive investigation of SUMO semantics, we plan to develop an accurate mapping from SUMO to Lean Prover [1].

Referências

[1] Leonardo de Moura, Soonho Kong, Jeremy Avigad, Floris Van Doorn, and Jakob von Raumer. The lean theorem prover. In *25th International Conference on Automated Deduction (CADE-25)*, Berlin, 2015.

[2] Christiane Fellbaum, editor. *WordNet: An Electronic Lexical Database (Language, Speech, and Communication)*. The MIT Press, 1998.

[3] Michael R Genesereth and Richard E Fikes. Knowledge interchange format-version 3.0: reference manual. Technical report, Computer Science Department, Stanford University San Francisco, CA, 1992.

[1] `https://github.com/own-pt/cl-krr`

[4] Adam Pease. *Ontology: A Practical Guide*. Articulate Software Press, Angwin, CA, 2011.

[5] Geoff Sutcliffe. The tptp problem library and associated infrastructure. *Journal of Automated Reasoning*, 43(4):337, 2009.

Rank and Special Graph Classes[‡]

Moisés Teles Carvalho* Simone Dantas* Carlos Vinícius Lima*
Vinicius Linder* Vinícius Fernandes dos Santos†

* IME, Universidade Federal Fluminense
moisesteles@cos.ufrj.br
sdantas@im.uff.br
vlinder@id.uff.br
carloslima@dcc.ufmg.br

† ICEx, Universidade Federal de Minas Gerais
viniciussantos@dcc.ufmg.br

Several distributed computing models and information dissemination consider a initial set of "activated" nodes that spread some information over a network. In this way, many rules can be taken, where nodes are added to the initial activated node set. We consider a spread in a finite, undirected, and simple graph $G = (V, E)$ with n vertices and m edges such that vertices are activated according to the distances between them, i.e., given an initial vertex set $S \subseteq V(G)$, a vertex w is added to S whenever there exists a pair of vertices u and v such that w belongs to a shortest path between u and v. We consider the problem of finding the size of a largest set such that no elements can be activated by the others. Formally, a *convexity space* is defined as a pair (V, C), where V is a set and C is a collection of finite subsets of V, called *convex sets*, such that $\emptyset, V \in C$, and C is closed under intersection.

A *graph convexity* on a graph G is one whose convex sets are defined over the set of vertices and edges of G. The importance of a graph convexity comes from the structure of the considered convex sets. The more studied are based on *path convexities*, such as the *monophonic*, P_3, and *geodetic*. The last one is that considered here, which has received wide attention (see also Pelayo (2013)). Given a graph G and a set $S \subseteq V(G)$, the *hull* of S is the smallest convex set that contains S, denoted by $\langle S \rangle$. Such a set S is *convexly independent* if $v \notin \langle S \setminus \{v\} \rangle$, for every $v \in S$. The *rank* $rk(G)$ is the cardinality of a largest convexly independent set of G (see also Kanté et al. (2017)). Hence, it represents the size of a largest element set that cannot active any other in a dissemination model.

In this work, we determine the rank on the geodetic convexity for complete, complete k-partite graphs, cycles, and power of cycles. We show that $rk(G[S])$ is a lower bound for $rk(G)$, for a convex set S and of a simplicial vertex set.

References

Kanté, M. M., dos Santos, V. F. & Szwarficter, J. L. (2017), 'On the geodetic rank of a graph', *Journal of Combinatorics* **8**(2), 323 – 340.

Pelayo, I. M. (2013), 'Geodesic convexity in graphs', *Springer*.

[‡]Partially supported by CAPES, FAPERJ and CNPq/Brazil.

GERAÇÃO DE COGRAFOS COM ATRASO LINEAR

Átila Arueira Jones* Fábio Protti† Renata Raposo Del-Vecchio‡

* UFF / IF sudeste MG
atilajones@id.uff.br

† Instituto de Computação - UFF
fabio@ic.uff.br

‡ Instituto de Matemática e Estatística - UFF
renata@vm.uff.br

A classe dos *cografos*, introduzida por volta de 1970 por diferentes autores, como Corneil et al. (1981), é comumente conhecida como os grafos livres de P_4. Problemas provados como $NP-completo$ para grafos em geral, apresentam complexidade polinomial quando restritos a esta classe, dentre estes podemos citar: clique, isomorfismo e coloração. O que deixa claro a importância da classe. A área de combinatória enumerativa tem a finalidade de obter todas as maneiras que podemos formar um certo padrão e em Teoria dos Grafos o interesse é obter um algoritmo capaz de gerar todos os grafos com certa propriedade. Até então não é encontrado na literatura nenhum trabalho sobre geração de cografos, que é exatamente o tema desenvolvido neste trabalho. Mais especificamente, dado um inteiro n desenvolvemos um algoritmo eficiente capaz de gerar, sem repetição, todos cografos com n vértices, cuja eficiência é obtida ao provarmos que o tempo de geração entre dois cografos consecutivos é linear em n. Além da sua eficiência, dois outros pontos interessantes do nosso algoritmo é que se baseia unicamente na coárvore do cografo e que é facilmente adaptável para gerar apenas os cografos conexos.

São naturais as aplicações do nosso algoritmo, pois a geração de todos os cografos auxilia na formulação de novos resultados, em especial o procedimento também se mostra útil para encontrar contra-exemplos ou até validar conjecturas acerca dos cografos.

Atualmente, um dos pontos trabalhos na nossa tese é tentar generalizar a geração de cografos para outras classes que são vistas como generalização do cografo, classes conhecidas por possuírem poucos P_4, são elas: P_4-redutível, P_4-extensível e P_4-esparso.

Referências

Corneil, D. G., Lerchs, H. & Burlingham, L. S. (1981), 'Complement reducible graphs', *Discrete Applied Mathematics* **3**(3), 163–174.

Proving Total Correctness of a Sorting Algorithm with Hoare Logic and Temporal Logic of Actions

João Pianta[1], **Barbara Kudiess**[1], **Alfio Martini** [1]

[1]Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS)
Faculdade de Informática – Av. Ipiranga, 6681 – Prédio 32
Porto Alegre - RS – CEP: 90619-900

{joao.pianta,barbara.kudiess}@acad.pucrs.br, alfio.martini@pucrs.br

Two established logical systems widely used for formal specification and verification of computing systems are *Hoare Logics* [Hoare 1983] and *Temporal Logic of Actions* (TLA^+) [Lamport 1994]. Hoare logic is a formal system with a set of logical rules for reasoning rigorously about the correctness of (imperative) programs and it is an excellent tool for introducing formal methods for computer scientists. It is also especially useful for programmers, since it provides a conceptual and solid foundation for the well-known *design by contract specification methodology*, currently supported by almost every mainstream programming language. On the other hand, TLA^+ is a formal language for specifying the behavior of concurrent and distributed algorithms and asserting properties of those abstract systems. However, it can also be a great tool for introducing and teaching formal specification of sequential algorithms due to its rich and friendly set-theory based specification language. Nonetheless, TLA^+ provides no way to write proofs of those properties. An extension of TLA^+, called TLA^{+2} supports writing proofs in natural deduction style and permits invoking existing automated and interactive proof systems to check those proofs [Chaudhuri et al. 2008]. Moreover, proofs in TLA^{+2} can be written in a hierarchical style that is crucial for managing the complexity of correctness proofs of computational systems. In this work, we formalize and prove the total correctness of a sorting algorithm written in a simple imperative language using both Hoare Logic and TLA^{+2}. Firstly, we show how to use the TLA^{+2} model checker to investigate the satisfaction of all proof obligations and intermediate assertions generated by the proof rules of the Hoare system. Secondly, the deductive verification of those proof obligations are then formally verified within the TLA Proof System (TLAPS). Here, a varied degree of proof refinement can be achieved. Finally, we conclude discussing the adequacy of the underlying computational model of TLA^+ as a formal model of the simple imperative language used in this example and also present a set of guidelines that can be helpful when using TLA^{+2} together with Hoare Logic for the formal specification and verification of sequential algorithms.

References

Chaudhuri, K., Doligez, D., Lamport, L., and Merz, S. (2008). A TLA+ proof system. *CoRR*, abs/0811.1914.

Hoare, C. A. R. (1983). An axiomatic basis for computer programming (reprint). *Commun. ACM*, 26(1):53–56.

Lamport, L. (1994). The temporal logic of actions. *ACM Trans. Program. Lang. Syst.*, 16(3):872–923.

Investigations on the axiomatic presentation of $\mathcal{ALC}$ Description Logic

Alexandre Rademaker* Edward Hermann Haeusler†

Fabricio Chalub* Christiano Braga‡

* IBM Research

† PUC-Rio, Dep. Informática

‡ UFF, Intituto de Computação

Description Logics (DLs) is a family of formalisms used to represent knowledge of a domain. It is equipped with a formal logic-based semantics. Knowledge representation systems based on description logics provide various inference capabilities that deduce implicit knowledge from the explicitly represented knowledge.

In Rademaker (2012) some of the authors investigate the proof theory of DL. Sequent Calculi and Natural Deduction-style deductive systems were proposed for the description logics ALC and ALCQ. The most important meta-theoretic results about semantics and proofs for these systems were proven: soudness, completeness, cut-elimination and normalization. It is argued that those systems can improve the extraction of computational content from DLs proofs, for proof explanation purposes.

The completeness of the Sequent Calculus for ALC ($\mathrm{SC}_{\mathcal{ALC}}$) was first presented in Rademaker et al. (2008). It was shown relative to the axiomatic presentation of ALC presented by Schild in Schild (1991), that is, in order to prove the $\mathrm{SC}_{\mathcal{ALC}}$ completeness, we had only to derive the axioms.

Nevetheless, soundness and completeness of $\mathrm{SC}_{\mathcal{ALC}}$ was not really made by Schild. Schild assumed they are correct citing Lemmon (1966*a*). This turns out to be a mistake, Schild was surely intended to cite Halpern & Moses (1992). Both Lemmon (1966*a*) and Lemmon (1966*b*) address only uni-modal logics, clearly not directly related to description logics. On the other hand, although the syntax translation of $\mathcal{ALC}$ concepts to K_n formulas are considered obvious by many authors, and their intuition described by Schild (1991); Baader et al. (2011), Halpern & Moses (1992) didn't really explained how he obtained, from the k_n multi-modal logic axioms, the $\mathcal{ALC}$ axioms that he presented.

In this work, we aim to start a discussion about a detailed mapping from the K_n multi-modal logic from Halpern & Moses (1992) to the $\mathcal{ALC}$ axiomatic presentation presented by Schild (1991).

Referências

Baader, F., Calvanese, D., McGuinness, D. L., Nardi, D. & Patel-Schneider, P. F. (2011), *The Description Logic Handbook: Theory, Implementation and Applications*, Cambridge University Press.

Halpern, J. Y. & Moses, Y. (1992), 'A guide to completeness and complexity for modal logics of knowledge and belief', *Artificial Intelligence* **54**, 311–379.

Lemmon, E. J. (1966*a*), 'Algebraic semantics for modal logics I', *The Journal of Symbolic Logic* **31**(1), 46–65. ISSN 00224812. URL http://www.jstor.org/stable/2270619.

Lemmon, E. J. (1966*b*), 'Algebraic semantics for modal logics II', *Journal of Symbolic Logic* **31**(2), 191–218. DOI 10.2307/2269810.

Rademaker, A. (2012), *A Proof Theory for Description Logics*, SpringerBriefs in Computer Science, Springer. URL http://dx.doi.org/10.1007/978-1-4471-4002-3.

Rademaker, A., Haeusler, E. H. & Pereira, L. C. (2008), On the proof theory of ALC, *in* 'Proceedings of the XV Brazilian Logic Conference', Unicamp, Campinas.

Schild, K. (1991), A correspondence theory for terminological logics: Preliminary report, Technical Report 91, Technische Universitat Berlin: IJCAI.

Theorem provers for Dolev-Yao multi-agent epistemic logic[‡]

Mario R. F. Benevides[*†] Luiz C. F. Fernandez[†]

Anna C. C. M. de Oliveira[†]

[*] Instituto de Matemática
Universidade Federal do Rio de Janeiro

[†] Programa de Engenharia de Sistemas e Computação
COPPE - Universidade Federal do Rio de Janeiro
{mario, lcfernandez, acoliveira}@cos.ufrj.br

In Benevides et al. (2017) are briefly presented an extension to multi-agent epistemic logic, which is based on Dolev & Yao (1983), for reasoning about security protocols. This is done introducing a new semantics based on structured propositions: instead of building formulas from atomic propositions, they are built from expressions. The main aim is to keep the logic propositional.

In this work we propose two diferent tools for Dolev-Yao multi-agent epistemic logic, named $S5_{DY}$: a tableau method, presenting the set of general rules for S5 (extended from Fitting (1983) and Massacci (2000) methods) and the additional ones. We also prove soundness and completeness of this proof system, inspired by Costa (1992); and we translate the $S5_{DY}$ to STRIPS, an artificial intelligence planner developed by Fikes & Nilsson (1971). Then, we present an implementation of model checking for the system.

References

Benevides, M. R. F., Fernandez, L. C. F. & Oliveira, A. C. C. M. (2017), Epistemic Logic Based on Dolev-Yao Model, *in* 'Anais do XXXVII Congresso da Sociedade Brasileira de Computação - II ETC', Sociedade Brasileira de Computação.

Costa, M. M. C. (1992), *Introdução à Lógica Modal Aplicada à Computação*, VIII Escola de Computação, Gramado - RS, Informática UFRGS, Universidade Federal do Rio Grande do Sul, Porto Alegre, Rio Grande do Sul.

Dolev, D. & Yao, A. C. (1983), 'On the Security of Public Key Protocols', *Information Theory, IEEE Transactions on* **29**(2), 198–208.

Fikes, R. & Nilsson, N. J. (1971), STRIPS: A new approach to the application of theorem proving to problem solving, *in* 'Proceedings of the 2nd International Joint Conference on Artificial Intelligence. London, UK, September 1-3, 1971.', pp. 608–620.

Fitting, M. (1983), *Proof methods for modal and intuitionistic logics*, Synthese library ; v. 169., D. Reidel, Dordrecht, Holland ; Boston, U.S.A. Hingham, MA.

Massacci, F. (2000), 'Single Step Tableaux for Modal Logics', *Journal of Automated Reasoning* **24**(3), 319–364.

[‡]The authors thanks to CNPq, that partially funded this work.

Tableau e Cálculo de Sequentes para a Lógica Combinada CIPL[‡]

Ranieri Batista da Costa*

* Departamento de Informática - PUC-RIO
rbcosta@inf.puc-rio.br

Em (Caleiro & Ramos, 2007), é apresentada uma combinação dos fragmentos implicacionais das lógicas proposicionais clássica (CPL) e intuicionista (IPL), à qual nos referimos como CIPL. Esta lógica não colapsa os conectivos intuicionistas nos conectivos clássicos, e preserva o *modus ponens* para ambas as implicações. Neste artigo apresentamos um tableau rotulado e um cálculo de sequentes para a lógica CIPL, que em (Caleiro & Ramos, 2007) foi definida apenas em um sistema axiomático.

Referências

Caleiro, C. & Ramos, J. (2007), *Combining Classical and Intuitionistic Implications*, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 118–132. URL `http://dx.doi.org/10.1007/978-3-540-74621-8_8`.

[‡]Agradecimentos: ao CNPq pelo apoio financeiro e concessão de bolsa.

Uma abordagem lógica para Reo[‡]

André Luiz Pereira Jr.* Bruno Lopes*

* Universidade Federal Fluminense
andrelpoj@id.uff.br
bruno@ic.uff.br

A modelagem e certificação de sistemas é uma tarefa de alto teor de complexidade no processo de desenvolvimento de software. O uso de ferramentas que isentem desenvolvedores de parte da complexidade possibilita maior agilidade no processo de desenvolvimento, bem como simplifica a certificação de requisitos. Enxergar o sistema como componentes independentes que se comunicam através de conectores é uma maneira de simplificar o entendimento do sistema, além de facilitar sua verificação.

Reo é uma linguagem gráfica para a modelagem de sistemas baseada em conectores de canais. Esses conectores regem o fluxo de dados entre componentes do sistema e são criados a partir da composição de conectores mais simples. Conectores atômicos são chamados de canais e com um conjunto pequeno de canais pode-se modelar diversos comportamentos de transmissão de dados. A utilização de Reo possibilita que aspectos formais, apesar de presentes, sejam transparentes aos desenvolvedores, mas a verificação de propriedades ainda carece da interação dos desenvolvedores.

Constraint Automata, de forma simplificada, são conjuntos de estados, transições entre esses estados e *data constraints* (condições lógicas) que devem ser respeitadas para que uma transição possa acontecer. A proposta aqui apresentada consta da investigação acerca de uma abordagem lógica para Reo: traduzir um modelo Reo para o modelo de Constraint Automata, sobre o qual será utilizado um formalismo lógico, através de um assistente de provas para automatizar a verificação formal de propriedades. São passos iniciais a um arcabouço para certificação de *software* que reduza a complexidade do processo ao desenvolvedor.

Referências

ARBAB, F. (2004), 'Reo: a channel-based coordination model for component composition', *Mathematical Structures in Computer Science* **14**(3), 329–366.

Arbab, F. (2006), 'Coordination for component composition', *Electronic Notes in Theoretical Computer Science* **160**, 15 – 40. ISSN 1571-0661, Proceedings of the International Workshop on Formal Aspects of Component Software (FACS 2005).

Kokash, N. & Arbab, F. (2009), *Formal Behavioral Modeling and Compliance Analysis for Service-Oriented Systems*, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 21–41.

[‡]Os autores agradecem ao CNPq pelo apoio parcial a este projeto.

Ordered Monoid Automata and Normative Multi-Agent Systems

Christiano Braga Jean Zahn

* Instituto de Computação
Universidade Federal Fluminense
{cbraga,jzahn}@ic.uff.br

A normative multi-agent system (NorMAS) (Broersen et al. (2013)) is a regulated concurrent, possibly distributed, system where computation is performed by autonomous entities called agents. Regulation is essentially the application of rules to control the interaction among agents. There is a strong motivation for such systems now-a-days due to the so-called cyber-physical systems (Alur (2015)) that, not surprisingly, has a closed-coupled relation between software and the physical system, where reactive concurrent agents not only interact among each other but also change the physical system. A simple example is to consider a surveillance drone that can only move *after* taking a picture of the site being monitored, that is, a dependence or *order* among actions.

Automata theory (Hopcroft et al. (2001)), as a cornerstone of Computer Science, may be chosen as the underlying theory of NorMAS. A finite-state automaton, that specifies state change through transitions may model a NorMAS by representing the collective state of the agents as the state of the automaton and the transition relation of the automaton being the union of the transition relation of each agent. A logical perspective, more precisely, a temporal logic (Clarke et al. (1999)) perspective can also be applied since Kripke structures, the models of many modal logics, including temporal logics, are closely connected with automata. NorMAS verification by model checking (Clarke et al. (1999)) than presents itself quite naturally.

The contribution of this work is *twofold*. First, we propose *ordered monoid automata*. Its intuition is quite simple: *concurrent systems are constrained monoids*. In this work, constraints are given by structuring the words of the language accepted by the automaton according to a preorder, which appears to be a significant subclass of concurrent systems. This leads to our second contribution: we interpret of Normative Multi-Agent systems as ordered monoid automata. The monoidal structure captures the autonomy of an agent, allowing it to behave freely if no constraints are given. The ordered monoidal structure thus captures precisely the standard normative requirement that every action can be executed unless there exists a constraint over such an action. In the drone example, it may *freely* (in the precise algebraic meaning of the word) perform any composition of actions, such as recharging or taking samples from a surveilled site, as long as it only moves after shooting a picture of the site. We define our framework mathematically and also formalize it in the rewriting logic language Maude (Clavel et al. (2007)).

Referências

Alur, R. (2015), *Principles of Cyber-Physical Systems*, The Mit Press.

Broersen, J., Cranefield, S., Elrakaiby, Y., Gabbay, D., Grossi, D., Lorini, E., Parent, X., van der Torre, L. W. N., Tummolini, L., Turrini, P. & Schwarzentruber, F. (2013), Normative reasoning and consequence, *in* G. Andrighetto, G. Governatori, P. Noriega & L. W. N. van der Torre, eds, 'Normative Multi-Agent Systems', Vol. 4, Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, pp. 33–70.

Clarke, E., Grumberg, O. & Peled, D. (1999), *Model Checking*, MIT Press.

Clavel, M., Eker, S., Durán, F., Lincoln, P., Martí-Oliet, N. & Meseguer, J. (2007), *All about Maude - A High-performance Logical Framework: how to Specify, Program, and Verify Systems in Rewriting Logic*, Springer-Verlag.

Farias, H., Braga, C. & Menezes, P. B. (2016), Massive open online courses and monoids, *in* R. L. & L. T., eds, 'Formal Methods: Foundations and Applications. SBMF 2016', Vol. 10090, Springer, DOI:10.1007/978-3-319-49815-7_11, pp. pp 179–195.

Hopcroft, J. E., Motwani, R. & Ullman, J. D. (2001), *Introduction to Automata Theory, Languages, and Computation*, 2 ed., Addison-Wesley.

Blockchain model checking

Bruno Olímpio* Bruno Lopes*

* Instituto de Computação
Universidade Federal Fluminense
brunoolimpio@id.uff.br
bruno@ic.uff.br

The Nakamoto's Bitcoin blockchain Nakamoto (2009) emerged in early 2009 and have been treated as the most relevant IT disruption on the world since the internet revolution. More than creating a completely electronic cash system, Nakamoto had grouped several well known technologies and created an entire new potencial way of doing human relationships through the information technology.

A blockchain is a record of transactions in chronological order. Each block is connected with its predecessor in an unchangeable way, and all the data contained in each block is encrypted, but public and verifiable, which establishes a unconfidence-based confidence. In other words, every connected entity can check all the informations, so nobody needs to know who are the others. This eliminates the need of a third parties to ensure the truthfulness of the individuals and their informations.

The model checking is an automatic alternative to verify state systems through the establishment of a high level representation of the model and the specifications to be checked. The model checking algorithm returns a boolean response and, in case of false, counterexamples. These set of tools are very useful in order to avoid, or locate, several types of problems that are hard to find in a program testing, like concurrency issues.

The main objective of this work is to use a model checker, namely NuXSMV Bozzano et al. (2016), a symbolic model checker, to analise a blockchain as specified by Nakamoto looking for formal validation of critical points to the network and the consensus operations.

References

Bozzano, M., Cavada, R., Cimatti, A., Dorigatti, M., Griggio, A., Mariotti, A., Micheli, A., Mover, S., Roveri, M. & Tonetta, S. (2016), 'nuxmv 1.1.1 user manual'. URL `https://nuxmv.fbk.eu`.

Nakamoto, S. (2009), 'Bitcoin: A peer-to-peer electronic cash system'. URL `http://bitcoin.org/bitcoin.pdf`.

Problema da árvore Geradora com Representação Mínima

Elio David Zaldivar Linares* Luiz Satoru Ochi*

Thiago Gouveia da Silva†

* Universidade Federal Fluminense
ezaldivar@ic.uff.br
satoru@ic.uff.br

† Instituto Federal da Paraíba
thiago.gouveia@ifpb.edu.br

O presente trabalho estará enfocado no Problema da árvore Geradora com Representação Mínima (MRSTP, do inglês *Minimum Representation Spanning Tree Problem*), na sua variante de otimização que pertence à classe NP-difícil.

Formalmente, o MRSTP pode ser descrito como segue: dado um (multi)grafo não orientado $G = (V, E, L)$, sendo V o conjunto de vértices, E o conjunto de arestas e L o conjunto de rótulos sobre E, no qual cada aresta $e \in E$ possui um rótulo $L(e)$ associado; seja $c(v)$ o número de rótulos representados no vértice v e $R(G) = \sum_{v \in V} c(v)$, o objetivo é encontrar uma árvore geradora $T = (V, E', L')$, tal que $E' \subset E$ e $R(T)$ seja minimizado. Visto que T é uma árvore de cobertura, temos que para todo $v \in V, d(v) \geq 1$ e por conseguinte $c(v) \geq 1$. Por conveniência, utilizaremos a função $Rt(G) = \sum_{v \in V}(c(v) - 1)$, denominada **representação**, como objetivo para o MRSTP. O MRSTP tem utilidade em projetos de redes de transporte público com o objetivo de buscar a minimização das transferências que os passageiros realizariam entre os modos de transporte, visto que cada transferência significa tempo/custo extra no deslocamento causando atraso e incovenientes.

Índice