BASICS NEW YEAR WORKSHOP

25-26 JANUARY, 2015

目录

Contents

Call for Participation

尊敬的老师、同学，

BASICS新年研讨会是BASICS实验室举办的在每年元月召开的学术交流活动。今年的研讨会将于2015年1月25-26日在衡山宾馆举行。我们诚邀您参加此次活动！

为了更好地安排本次活动，请您填写下面的回执，并于1月16日前发至 basics@sjtu.edu.cn。电话：021-34205060转602，或13524340749。

姓名		单位	
手机号		电邮	
是否做报告			
若做报告，请提供**英文**报告题目和摘要			
是否安排住宿			

友情提示：

(1) 报告题目和摘要（英文）最迟在1月22日17:00之前提交。
(2) 交通及食宿全部自理。需要安排住宿的，请注明日期。
(3) 日程将于1月19日公布（http://basics.sjtu.edu.cn）。

BASICS2015新年研讨会组委会

Schedule

	25 JANUARY, 2015	
08:30-09:00	Xiaojuan Cai	On the Expressiveness of Well-Structured PD Systems
09:00-09:30	Yijia Chen	A Strong AC^0 Version of the Planted Clique Conjecture
09:30-10:00	Yuxin Deng	Program Equivalence in Linear Contexts
10:00-10:30		Tea Break
10:30-11:00	Xiaotie Deng	Nash Equilibrium Computing
11:00-11:30	Hongfei Fu	Maximal Cost-Bounded Reachability Probability on Continuous-Time Markov Decision Processes
11:30-12:00	Yuxi Fu	Arithmetizing Concurrency
12:00-13:30		Lunch
13:30-14:00	Chaodong He	The Branching Bisimilarity of nBPA is EXPTIME-Complete
14:00-14:30	Ying Jiang	Cut-Elimination and the Decidability of Reachability in Alternating Pushdown Systems
14:30-15:00	Ugo Dal Lago	Towards a Coinductive Characterization of Computationa l Indistinguishability
15:00-15:30		Tea Break
15:30-16:00	Guoqiang Li	Time-Sensitive Pushdown Systems
16:00-16:30	Xingfu Li	Approximation Algorithms for the Maximum Internal Spanning Tree Problem
16:30-17:00	Xinxin Liu	Capture Divergence with Induction in Coinduction
17:00-17:30	Fu Song	Extending Temporal Logics with Data Variable Quantifications
18:00-20:00		Dinner
	26 JANUARY, 2015	
08:30-09:00	Pinyan Lu	Optimal Competitive Auctions
09:00-09:30	Frederic Mallet	Safety Issues in CCSL Specifications
09:30-10:00	Dominik Scheder	The Power of Communication without Memory
10:00-10:30		Tea Break

10:30-11:00	Xiaoming Sun	On the Sensitivity Conjecture
11:00-11:30	Xian Xu	Names in Process-Passing
11:30-12:00	Yitong Yin	Richness, Expansion, and Cell-Sampling
12:00-13:30		Lunch
13:30-14:00	Naijun Zhan	Invariant-based Verification and Synthesis for Hybrid Systems
14:00-14:30	Chihao Zhang	The Complexity of Ferromagnetic Two-Spin Systems
14:30-15:00	Lijun Zhang	Probably Safe or Live
15:00-15:30		Tea Break
15:30-16:00	Min Zhang	A Formal Approach to the Design of Property-Based Dynamic Software Updates
16:00-16:30	Xinyu Feng	Compositional Verification of Termination-Preserving Refinement of Concurrent Programs
16:30-17:00	Vania Joloboff	SimSoC: A Fast, Proven Faithful, Full System Virtual Prototyping Framework
17:00-17:30	Xingwu Liu	Top-k Sorting on Dynamic Data

Abstract

XIAOJUAN CAI

- Well-structured pushdown systems (WSPDS) are pushdown systems with well-quasi-ordered set of states and stack alphabets. As a general extension of Pushdown systems and Vector addition systems with states (VASS), WSPDSs are aimed at st udying concurrent recursive computations. In this talk, we first give some resu lts on the powerfulness of WSPDS by showing several concurrent models can be e ncoded into WSPDS, including Branching VASS, Alternating VASS, VASS with one z ero-test, multi-set pushdown systems and pushdown timed systems. In the second part, we illustrate that the termination problem and boundness problem of WSPD S are decidable, which excludes WSPDS from Turing powerful models. However, ex cept for termination and boundness problems, very little is known about the de cidability of many problems. We expect WSPDS to be a practical model with powe rful expressiveness and also some decidable model-checking problems.

YIJIA CHEN

- Our main result states that AC^0 circuits asymptotically almost surely can no t distinguish between a random graph and this graph with a randomly planted c lique of any size \le n^\xi (where 0\le \xi<1). In particular, this implies t hat AC^0 circuits cannot decide whether the clique number of a graph is at le ast k(n) for every unbounded function k(n)\le n^\xi (for k(n)=O(\log n) this was shown by [Beame, 90]). We may allow that in the main result the depth of the circuits increases moderately. Using this generalization we show that AC ^0 circuits cannot approximate the clique problem by any nontrivial ratio in terms of the clique number.

YUXIN DENG

- Program equivalence in linear contexts, where programs are used or executed e xactly once, is an important issue in programming languages. However, existing techniques like those based on bisimulations and logical relations only targe t at contextual equivalence in the usual (non-linear) functional languages, an d fail in capturing non-trivial equivalent programs in linear contexts, parti cularly when non-determinism is present. We propose the notion of linear conte

xtual equivalence to formally characterize such program equivalence, as well as a novel and general approach to studying it in higher-order languages, based on labeled transition systems specifically designed for functional languages. We show that linear contextual equivalence indeed coincides with trace equivalence. We illustrate our technique in both deterministic (a linear version of PCF) and non-deterministic (linear PCF in Moggi's framework) functional languages.

XINYU FENG

- Many verification problems can be reduced to refinement verification. However, existing work on verifying refinement of concurrent programs either fails to prove the preservation of termination, allowing a diverging program to trivially refine any programs, or is difficult to apply in compositional thread-local reasoning. In this talk, we first propose a new simulation technique, which establishes termination-preserving refinement and is a congruence with respect to parallel composition. We then give a proof theory for the simulation, which is the first Hoare-style concurrent program logic supporting termination-preserving refinement proofs. We show two key applications of our logic, i.e., verifying linearizability and lock-freedom together for fine-grained concurrent objects, and verifying full correctness of optimizations of concurrent algorithms.

HONGFEI FU

- In this talk, we consider maximal cost-bounded reachability probability over continuous-time Markov decision processes (CTMDPs). Firstly, we derive an integral characterization which states that the maximal cost-bounded reachability probability function is the least fixed-point of a system of integral equations. Secondly, we prove that the maximal cost-bounded reachability probability can be attained by a measurable deterministic cost-positional scheduler. Thirdly, we provide a numerical approximation algorithm for maximal cost-bounded reachability probability.

YUXI FU

- We show that the name-passing communication mechanism is subsumed by the value-passing communication mechanism. Technically we prove that a secure version of the π-calculus is a submodel of a variant of the well-known value-passing calculus. The value-passing calculus we use has a unique universal process, which provides a positive answer to a question left open in previous research.

CHAODONG HE

- We put forward an exponential-time algorithm for deciding branching bisimilarity on normed BPA systems based on the partition refinement approach. The decidability of branching (or weak) bisimilarity on normed BPA was once a long standing open problem which was closed by Yuxi Fu in 2013. The EXPTIME-hardness is an inference of a slight modification of the reduction presented by Richard Mayr.

YING JIANG

- We propose a new approach to formalize alternating pushdown systems as natural-deduction style inference systems. In this approach, the decidability of reachability can be proved as a simple consequence of a cut-elimination theorem for the corresponding inference system. Then, we show how this result can be used to extend an alternating pushdown system into a complete system where, for every configuration A, either A or $\neg A$ is provable. The key idea is that cut-elimination permits to build a system where a proposition of the form $\neg A$ has a co-inductive (hence possibly infinite) proof if and only if it has an inductive (hence finite) proof. (joint work with Gilles Dowek)

VANIA JOLOBOFF

- In this talk, I will presents the SimSoC virtual prototyping framework. SimSoC is a full system simulation framework, based on SystemC and Transaction Level Modeling. It is using dynamic binary translation to simulate the target platform software, which can be a a full operating system, on the host system. A potential issue with simulators is that they might not accurately simulate the real hardware. As part of the SimSoC project, we have tried to fill this gap by proving that the ARM instruction set simulator coded in C is a high fidelity i

mplementation of the ARM architecture, using the Coq theorem prover, starting from a formal architectural model in Coq. The first part of the paper presents the general architecture of SimSoC. The second part describes the approach taken for the proof of the ARM simulator.

UGO DAL LAGO

- Computational indistinguishability is one of the most central concepts in modern cryptography, and many other definitions (e.g.pseudorandomness, security of cryptographic schemes) can be formulated in terms of CI. We present the results of a study directed towards giving a direct and precise characterization of computational indistinguishability in a higher-order functional language for polynomial time computability, in which tools from implicit computational complexity and coinduction both play a central role.

GUOQIANG LI

- A time-sensitive pushdown system is a framework for time-awareness program modeling and analysis. This talk begins with NeTAs, a time-sensitive pushdown system with only local clocks, discussing its decidability on reachability, and then gives a whole picture on the time-sensitive pushdown systems, revealing the decidability, undecidability, and unknown results, with reasonable conjectures.

XINGFU LI

- We study the maximum internal spanning tree problem (MIST for short). Given an undirected simple graph G, the task for the maximum internal spanning tree problem is to find a spanning tree of G with maximum number of internal vertices. We present an approximation algorithm with performance ratio $\frac{4}{3}$ for MIST, which improves upon the best known approximation algorithm with performance ratio $\frac{3}{2}$. Our algorithm benefits from a new observation for bounding the number of internal vertices of a spanning tree. The new observation reveals that the number of internal vertices in a spanning tree of an undirected simple graph is less than the number of edges in a maximum path-cycle cover of the same graph. Finally, we show that the maximum internal spa

nning tree problem is Max-SNP-Hard. This implies that there is no polynomial t ime approximation scheme (PTAS) for this problem unless P=NP.

XINXIN LIU

- Divergence (or rather absence of which) is an important property of a system. Usually it refers to the existence of infinite internal computation sequences. In thiswork we examine divergence preserving equivalence relations defined by co-induction, in particular a variation of branching bisimulation equivalence. It turns out that induction can play an important part in capturing divergence property of corresponding states in co-inductive definitions. Besides a charac terization of the concerned equivalence relation in terms of infinite runs, we also give it a modal characterization in the style of Hennessy-Milner logic. A partition algorithm for deciding equality of states for finite state labeled t ransition systems is presented.

XINGWU LIU

- We investigate the top-k-selection problem, i.e. determine and sort the larg est k elements, under the dynamic data model. Here dynamics means that the o rderof elements evolves over time, and that the change can be probed only by p airwise comparisons. It is assumed that in each time step, only one pair of ob jects can be compared. This assumption of restricted data access is reasonable under dynamic model, especially for massive data set where it is simply imposs ible to access all the data before the next change occurs. Previously only two special cases were studied under this model: finding the largest element and t he median; and sorting all elements. This paper systematically deals with all $k\in [n]$ and solves the problem completely. Specifically, we identify the cr itical point k^* such that the top-k-selection problem can be solved error -free with probability $1-o(1)$ if and only if $k=o(k^*)$. A lower bound of th e error when $k=\Omega(k^*)$ is also determined, which actually is tight under some condition. On the other hand, it is shown that the top-k-set problem, w hich means finding the set of the largest k elements, can be solved error-fr ee for all $k\in [n]$ with probability $1-o(1)$.

PINYAN LU

- We study the design of truthful auctions for selling identical items in unlimited supply (e.g., digital goods) to n unit demand buyers. This classic problem stands out from profit-maximizing auction design literature as it requires no probabilistic assumptions on buyers' valuations and employs the framework of competitive analysis. Our objective is to optimize the worst-case performance of an auction, measured by the ratio between a given benchmark and revenue generated by the auction. We establish a sufficient and necessary condition that characterizes competitive ratios for all monotone benchmarks. The characterization identifies the worst-case distribution of instances and reveals intrinsic relations between competitive ratios and benchmarks in the competitive analysis. With the characterization at hand, we show optimal competitive auctions for two natural benchmarks. The most well-studied benchmark F^2 measures the envy-free optimal revenue where at least two buyers win. Goldberg et al. showed a sequence of lower bounds on the competitive ratio for each number of buyers n. They conjectured that all these bounds are tight. We show that optimal competitive auctions match these bounds. Thus, we confirm the conjecture and settle a central open problem in the design of digital goods auctions. As one more application we examine another economically meaningful benchmark, which measures the optimal revenue across all limited-supply Vickrey auctions. We identify the optimal competitive ratios to be (n/({n-1})^{n-1}-1 for each number of buyers n, that is e-1 as n approaches infinity.Joint work with Ning Chen and Nick Gravin.

FREDERIC MALLET

- The Clock Constraint Specification Language (CCSL) proposes a rich polychronous time model dedicated to the specification of constraints on logical clocks: i.e., sequences of event occurrences. A priori independent clocks are progressively constrained through a set of clock operators that define when an event may occur or not. These operators can be described as labeled transition systems that can potentially have an infinite number of states. A CCSL specification can be scheduled by performing the synchronized product of the transition systems for each operator. Even when some of the composed transition systems are infinite, the number of reachable states in the product may still be finite: the specification is safe. This talk discusses a condition to detect that the pr

oduct is actually safe. This is done by abstracting each CCSL constraint (rela tion and expression) as a marked graph.Detecting that some specific places, ca lled counters, in the resulting marked graph are safe is sufficient to guarant ee that the composition is safe.

DOMINIK SCHEDER

- We explore the power of communication with limited or no memory. In particular, we give a complete combinatorial characterization what can be achieved with me moryless communication and relate it to known communication models. We discuss several different approaches to modeling small-memory communication and show t hat they are all equivalent.

FU SONG

- Although data values are available in almost every computer system, reasoning about them is a challenging task due to the huge data size or even infinite da ta domains. Temporal logics are the well-known specification formalisms for re active and concurrent systems. Various extensions of temporal logics have been proposed to reason about data values, mostly in the last decade. Among them, one natural idea is to extend temporal logics with variable quantifications ra nging over an infinite data domain. In this paper, we focus on the variable ex tensions of two widely used temporal logics, Linear Temporal Logic (LTL) and C omputation Tree Logic (CTL). Grumberg, Kupferman and Sheinvald recently invest igated the extension of LTL with variable quantifications. They defined the ex tension as formulas in the prenex normal form, that is, all the variable quant ifications precede the LTL formulas. Our goal in this paper is to do a relativ ely complete investigation on this topic. For this purpose, we define the exte nsions of LTL and CTL by allowing arbitrary nestings of variable quantificat ions, Boolean and temporal operators (the resulting logics are called respecti vely variable-LTL, in brief VLTL, and variable-CTL, in brief VCTL), and identi fy the decidability frontiers of both the satisfiability and model checking pr oblem. In particular, we obtain the following results: 1) Existential variable quantifiers or one single universal quantifier in the beginning already entail s undecidability for the satisfiability problem of both VLTL and VCTL, 2) If o nly existential path quantifiers are used in VCTL, then the satisfiability pro blem is decidable, no matter which variable quantifiers are available. 3) Fo

r VLTL formulas with one single universal variable quantifier in the beginning, if the occurrences of the non-parameterized atomic propositions are guarded by the positive occurrences of the quantified variable, then its satisfiability problem becomes decidable. Based on these results of the satisfiability problem, we deduce the (un)decidability results of the model checking problem.

XIAOMING SUN

- The sensitivity conjecture of Nisan and Szegedy asks whether the maximum sensitivity of a Boolean function is polynomially related to the other major complexity measures of Boolean functions. Despite major advances in analysis of Boolean functions in the past decade, the problem remains wide open with no positive result toward the conjecture since the work of Kenyon and Kutin from 2004. In this work, we prove tighter upper bounds for various complexity measures in terms of sensitivity. More precisely, we show that deg(f)^{1−o(1)} = O(2^s(f)) and C(f) ⩽ 2^{s(f)−1} s(f); these in turn imply various corollaries regarding the relation between sensitivity and other complexity measures, such as block sensitivity, via known results. The gap between sensitivity and other complexity measures remains exponential but these results are the first improvement for this difficult problem that has been achieved in a decade.

XIAN XU

- In process-passing, names cannot be passed, but can be parameterized. This talk looks at several aspects concerning names in a purely higher-order setting: (1) behavioral equivalence; (2) expressiveness. We review some known results, and some open issues as well.

YITONG YIN

- In this talk I will briefly summarize two major techniques for data structure lower bounds: the classic richness lemma of Miltersen et al, and the more recent cell-sampling technique of Panigraphy et al and independently of Larsen. I will show how to unify them to prove stronger richness lemmas, which combining with existing isoperimetric inequalities in geometry implies improved lower bounds for nearest neighbor search. These lower bounds either match the state of the arts or are higher. In addition, these data structure lower bounds are str

onger in a sense that they give lower bounds to the costs for certifying the correct answers instead of computing them, so in fact they are certificate lower bounds, and for their randomized relaxations, the lower bounds are for the Arthur-Merlin games naturally defined in randomized data structures.

NAIJUN ZHAN

- Hybrid systems (now also called cyber-Physical systems) are quite omnipresent in our daily life, many of them are safety-critical. "How can we design cyber-physical systems people can bet their lives on" is a grand challenge for computer science and control theory. Formal methods is thought an effective solution to the challenge, and has been widely and successful used in practice. Invariant generation plays a key role in the formal design of hybrid systems. In this talk, I will first report our recent work on a complete approach to synthesizing semi-algebraic invariants for polynomial hybrid systems, which gave a confirmative answer to the open problem if there is a complete method to discover all semi-algebraic invariants for polynomial hybrid systems. Then, I will show how to use the results to synthesize controllers in the design of hybrid systems. I also discuss how to extend the results to deal with non-polynomial hybrid systems. Finally, I will demonstrate how to apply the results to solve real-world problems, such as the controller synthesis of oil pump, and the verification of the descent control program of a lunar lander, etc.

CHIHAO ZHANG

- We study the approximability of computing the partition function for ferromagnetic two-state spin systems. The remarkable algorithm by Jerrum and Sinclair showed that there is a fully polynomial-time randomized approximation scheme (FPRAS) for the special ferromagnetic Ising model with any given uniform external field. Later, Goldberg and Jerrum proved that it is #BIS-hard for Ising model if we allow inconsistent external fields on different nodes. In contrast to these two results, we prove that for any ferromagnetic two-state spin systems except the Ising model, there exists a threshold for external fields beyond which the problem is #BIS-hard, even if the external field is uniform.

LIJUN ZHANG

- We present a formal characterisation of safety and liveness properties for fully probabilistic systems. As for the classical setting, it is established that any (probabilistic tree) property is equivalent to a conjunction of a safety and liveness property. A simple algorithm is provided to obtain such a property decomposition for flat probabilistic CTL (PCTL). A safe fragment of PCTL is identified that provides a sound and complete characterisation of safety properties. For liveness properties, we provide two PCTL fragments, a sound and a complete one, and show that a sound and complete logical characterisation of liveness properties hinges on the (open) satisfiability problem for PCTL. We show that safety properties only have finite counterexamples, whereas liveness properties have none. We compare our characterisation for qualitative properties with the one for branching time properties by Manolios and Trefler, and present sound and complete PCTL fragments for characterising the notions of strong safety and absolute liveness coined by Sistla.

MIN ZHANG

- Even though software systems in some domains are expected to provide continuous services, most of them must undergo some form of changes. It leads to the emergence of dynamic software updating, a technique for updating a running software system without incurring any downtime. One of the challenges of designing a correct dynamic update is to identify a set of update points where the update can be safely applied to a running system. In this talk, we will introduce a novel counterexample-guided approach to identifying safe update points. In our approach, we formalize dynamic updates as state machines, and verify by model checking a set of desired properties which should be satisfied by the system after being updated. If counterexamples are found, we exclude those states that cause the counterexamples, and do model checking again. We repeat the process until all the desired properties are successfully verified, and finally obtain a set of safe update points. We show the feasibility of the proposed approach with a case study.

Venue

The workshop will take place in Heng Shan Hotel.

研讨会在衡山宾馆举行。

1. 浦东机场乘机场专线车3号线到徐家汇站后步行10分钟可达宾馆。全程约90分钟。
2. 虹桥国际机场直接选乘计程车（出租）到宾馆里程约15公里，耗时25分钟左右，计费白天32元左右，夜间42元左右（具体费用以当天实际路况为准，以上价格仅作参考）。
3. 无论是上海站还是上海南站均可乘地铁一号线至衡山路站，出站后步行8分钟左右到达宾馆。上海火车站乘地铁一号线到衡山宾馆需时约20分钟，上海南站乘地铁一号线到衡山宾馆需时约15分钟。

Contact Us

Xiaoju DONG 董笑菊

Room 327, No. 3 SEIEE Building,

800 Dongchuan Road

Shanghai Jiao Tong University,

Shanghai, 200240, China

Email: basics@sjtu.edu.cn

Tel: 021-34205060 EXT 602

MP: 13524340749

Annual Events of BASICS Lab

- BASICS New Year Workshop
- BASICS Summer School

http://basics.sjtu.edu.cn