BASICS Symposium 2018

25 January, 2018		
09:00-09:30	Chen, Yijia	A Parameterized Halting Problem, the Linear Time Hierarchy, and the MRDP Theorem
09:30-10:00	Li, Angsheng	Structural Information Theory and Its Applications: Principles for Distinguishing Order from Disorder
10:00-10:30	Deng, Yuxin	Logical Characterizations of Probabilistic Bisimilarity
10:30-11:00	**Tea Break**	
11:00-11:30	Lu, Pinyan	The Value of Information Concealment
11:30-12:00	Zhang, Peng	Max k-Uncut, Densest k-Subgraph, and Unique Games
12:00-12:30	Gravin, Nick	Separation in Correlation-Robust Monopolist Problem with Budget
12:30-13:30	**Lunch**	
13:30-14:00	Sun, Xiaoming	Exact Quantum Algorithms for Weight Decision Problem
14:00-14:30	Li, Lvzhou	Quantum Algorithms for Powers of a Matrix
14:30-15:00	Zheng, Shenggen	On Advantages of Several Exact Quantum Computing Models
15:00-15:30	Yan, Jun	Quantum Zero-Knowledge Proof for NP
15:30-16:00	**Tea Break**	
16:00-16:30	Fu, Yuxi	Final Remark on the Decidability of PDA
16:30-17:00	Jansen, David	An O(m log n) Algorithm for Computing Stuttering Equivalence and Branching Bisimulation
17:00-17:30	Chen, Zhe	Parametric Runtime Verification is NP-Complete and coNP-Complete
17:30-18:00	Yin, Qiang	Two Lower Bounds for BPA
26 January, 2018		
09:00-09:30	Wang, Hanpin	Logic for Reasoning about Cloud Storage Systems
09:30-10:00	Feng, Xinyu	Progress of Concurrent Objects with Partial Methods
10:00-10:30	Cheng, Tong	Analyzing Probabilistic Programs with Dynamic Logic
10:30-11:00	**Tea Break**	
11:00-11:30	Xia, Mingji	About Variable Lovász Local Lemma
11:30-12:00	Lin, Yuan	Assessing Percolation Threshold Based on High-Order Non-backtracking Matrices
12:00-12:30	Scheder, Dominik	The PPSZ k-SAT Algorithm on Formulas with Many Solutions
12:30-13:30	**Lunch**	
13:30-14:00	Jiang, Ying	Towards Combining Model Checking and Proof Checking
14:00-14:30	Liao, Chao	Counting Hypergraph Colorings in the Local Lemma Regime
14:30-15:00	Yang, Qizhe	Counting Finite Computations
15:00-15:30	**Tea Break**	
15:30-16:00	Fang, Zhixuan	Prices and Subsidies in the Sharing Economy
16:00-16:30	Zhang, Tianyi	Improved Distance Sensitivity Oracles via Tree Partitioning
16:30-17:00	Wang, Zihe	An Improved Welfare Guarantee for First Price Auctions
17:00-17:10	**Closing Speech**	

1. 会议地点：上海交通大学 徐汇校区（华山路 1954 号） 总办公厅二楼。
2. 午餐：教师活动中心 一楼自助餐厅。
3. 自驾：从广元西路校门进入地下车库
4. 公交：地铁 10 号线 上海交通大学站。

Talk Abstract

- **Chen, Yijia 陈翌佳**
- **Title: A parameterized halting problem, the linear time hierarchy, and the MRDP theorem**
- **Abstract:** The complexity of the parameterized halting problem for nondeterministic Turing machines p-Halt is known to be related to the question of whether there are logics capturing various complexity classes. Among others, if p-Halt is in para-AC^0, the parameterized version of the circuit complexity class AC^0, then AC^0 has a logic. Although it is widely believed p-Halt\notin para-AC^0, we show that the problem is hard to settle by establishing a connection to a question in classical complexity of whether NE\notsubseteq LINH. Here, LINH denotes the linear time hierarchy. On the other hand, we suggest an approach toward proving NE\notsubseteq LINH using bounded arithmetic. More specifically, we demonstrate that if the much celebrated MRDP (for Matiyasevich-Robinson-Davis-Putnam) theorem can be shown in a certain fragment of arithmetic, then NE\notsubseteq LINH. Interestingly, another parameterized problem plays an important role in the proof of this result.
  This is joint work with Moritz Mueller (Vienna), Jan Pich (Vienna), and Keita Yokoyama (JAIST).

- **Li, Angsheng 李昂生**
- **Title: Structural Information Theory and Its Applications: Principles for Distinguishing Order from Disorder**
- **Abstract:** It had been a great challenge to measure the information embedded in a graph or physical system such that the structural information determines and decodes the essential structure or functional structure of the graph or physical system. Such a missing metric was regarded as a fundamental gap in the theoretical underpinnings of information science and computer science. Recently, Li and Pan introduced the notion of coding tree of a graph which encodes a large-scale graph by a tree such that a vertex of the graph is encoded by a leaf node of the tree, defined the notion of structural entropy of the graph given by a coding tree as the amount of information required to determine the tree codeword of the vertex that is accessible from random walk in the graph, and defined the structural entropy of the graph as the minimum amount of information required to determine the codeword of a coding tree for the vertex that is accessible from random walk in the graph. The structural entropy of a graph defined in this way is hence the information embedded in the graph that determines and decodes the coding tree of the graph that minimizes the uncertainty of the positioning of the graph. The new notions build a new theory, the structural information theory. The theory has enormous applications in a wide range of disciplines, including data processing, network analysis, network algorithms etc. In this talk, I will introduce the basics of the theory and a few representative applications.

- **Deng, Yuxin 邓玉欣**
- **Title: Logical Characterizations of Probabilistic Bisimilarity**
- **Abstract:** For labeled Markov processes with continuous state space, van Breugel et al. provided a remarkable modal logic to characterize probabilistic bisimilarity without employing any modality indexed with numbers. The proof of this elegant characterization employs advanced machinery on topology theory. In the discrete case of finite state probabilistic processes, we prove that result with an elementary and more accessible proof. Moreover, our proof is constructive.

- **Lu, Pinyan 陆品燕**

- **Title：The Value of Information Concealment**
- **Abstract:** We consider a revenue optimizing seller selling a single item to a buyer, on whose private value the seller has a noisy signal. We show that, when the signal is kept private, arbitrarily more revenue could potentially be extracted than if the signal is leaked or revealed. We then show that, if the seller is not allowed to make payments to the buyer, the gap between the two is bounded by a multiplicative factor of 3, subject to fairly mild conditions on the joint distribution of the value and signal. Our examples show that both conditions are necessary for a constant bound to hold. We connect this scenario to multi-bidder single-item auctions where bidders' values are correlated. Results similar to the above are shown for the gap between the revenue of a Bayesian incentive compatible, ex post individually rational auction and that of a dominant strategy incentive compatible auction. Based on joint work with Hu Fu, Chris Liaw and Zhihao Gavin Tang.

- **Zhang, Peng 张鹏**
- **Title：Max k-Uncut, Densest k-Subgraph, and Unique Games**
- **Abstract：** We propose the Max k-Uncut problem in the study of network homophyly. Given an n-vertex undirected graph G = (V, E) with nonnegative weights defined on edges, and a positive integer k, the Max k-Uncut problem asks to find a partition {V1, V2, ..., Vk} of V such that the total weight of edges that are not cut is maximized. This problem is just the complement of the classic Min k-Cut problem. For Max k-Uncut (MkU), we present a randomized (1 − k/n)2-approximation algorithm, a greedy (1 − 2(k−1)/n)-approximation algorithm, and an α/2-approximation algorithm by reducing it to Densest k-Subgraph (DkS), where α is the approximation ratio for the DkS problem. More importantly, we show that MkU and DkS are in fact equivalent in approximability up to a factor of 2. We also prove an approximation hardness result for MkU under the assumption P ≠ NP.

- **Gravin, Nick**
- **Title：Separation in Correlation-Robust Monopolist Problem with Budget**
- **Abstract：** We consider a monopolist seller that has n heterogeneous items to sell to a single buyer. The seller's goal is to maximize her revenue. We study this problem in the correlation-robust framework recently proposed by Carroll [Econometrica 2017]. In this framework, the seller only knows marginal distributions for each separate item but has no information about correlation across different items in the joint distribution. Any mechanism is then evaluated according to its expected profit in the worst-case, over all possible joint distributions with given marginal distributions. Carroll's main result states that in multiitem monopoly problem with buyer, whose value for a set of items is additive, the optimal correlation-robust mechanism should sell items separately. We use alternative dual Linear Programming formulation for the optimal correlation-robust mechanism design problem. This LP can be used to compute optimal mechanisms in general settings. We give an alternative proof for the additive monopoly problem without constructing worst-case distribution. As a surprising byproduct of our approach, we get that separation result continues to hold even when buyer has a budget constraint on her total payment. Namely, the optimal robust mechanism splits the total budget in a fixed way across different items independent of the bids, and then sells each item separately with a respective per item budget constraint. Based on joint work with Pinyan Lu.

- **Sun, Xiaoming 孙晓明**
- **Title: Exact quantum algorithms for weight decision problem**
- **Abstract:** The weight decision problem, which requires to determine the Hamming weight of a given binary string, is a natural and important problem, with applications in cryptanalysis,

coding theory, fault-tolerant circuit design and so on. In particular both Deutsch-Jozsa problem and Grover search problem can be interpreted as special cases of weight decision problems. In this work, we investigate the exact quantum query complexity of weight decision problems, where the quantum algorithm must always output the correct answer. More specifically, we consider a partial Boolean function which distinguishes whether the Hamming weight of the length-n input is k or it is l. Our contribution includes both upper bounds and lower bounds for the precise number of queries. Furthermore, for most choices of k, l and sufficiently large n, the gap between our upper and lower bounds is no more than one. To get the results, we first build the connection between Chebyshev polynomials and our problem, then determine all the boundary cases of with matching upper and lower bounds, and finally we generalize to other cases via a new quantum padding technique. This quantum padding technique can be of independent interest in designing other quantum algorithms.

- **Li, Lvzhou 李绿周**
- **Title：Quantum algorithms for powers of a matrix**
- **Abstract：** We first introduce the quantum algorithm for linear systems of equations, which has attracted much attention in recent years, and has accelerated the development of quantum machine learning. Then, we present our recent work on quantum algorithms for powers of a matrix.

- **Zheng, Shenggen 郑盛根**
- **Title: On advantages of several exact quantum computing models**
- **Abstract:** Quantum computing is one of the most intensively studied research fields in recent years. Quantum computing models can be divided into bounded-error and exact versions in terms of their outputs. In the bounded-error setting, quantum complexity is now relatively well understood. The model of exact quantum computing, where the algorithms must output the correct answer with certainty for every input, seems to be more intriguing. It is much more difficult to come up with exact quantum algorithms that outperform classical exact algorithms. In this talk, we will show some of our newest results on exact quantum computing for several computing models, including query complexity, communication complexity, time-space complexity and state complexity of finite automata.

  Publication

  1) arXiv:1603.06505 ,
  2) Theoretical Computer Science, 666, 48-64 (2017)
  3) Mathematical Structures in Computer Science, 27, 311-331 (2017)
  4) Time-space complexity advantages for quantum computing, LNCS 10687 05-317 (2017)
  5) Exact quantum algorithms have advantage for almost all Boolean functions, Quantum Information and Computation, 15, 0435-0452 (2015)
  6) Potential of quantum finite automata with exact acceptance, International Journal of Foundation of Computer Science, 26, 381-398 (2015)
  7) On the state complexity of semi-quantum finite automata, RAIRO-Inf. Theor. Appl., 48, 187-207 (2014)
  8) From quantum query complexity to state complexity, LNCS, 8808 231-245 (2014).

- **Yan, Jun 颜俊**
- **Title：Quantum Zero-Knowledge Proof for NP**
- **Abstract:** Zero-knowledge is an important notion in both complexity theory and cryptography. Zero-knowledge proof for a language L in NP is an interactive proof for L that yields nothing but the membership of the input in L. Quantum zero-knowledge proof is a kind of zero-

knowledge proof that is realized by quantum mechanism; that is, both the prover and the verifier are quantum polynomial-time algorithms, and they can exchange quantum messages. In this talk, I will show how to generalize the classical zero-knowledge proof to the quantum setting, and how to circumvent new difficulties incurred by quantum mechanism.

Publication:

1) Jun Yan, Jian Weng, Dongdai Lin, and Yujuan Quan. Quantum Bit Commitment with Application in Quantum Zero-Knowledge Proof (Extended Abstract). In ISAAC 2015, 555-565.
2) Jun Yan. How to Argue Security Based on the Statistical-Binding Property of Quantum Bit Commitment. In preparation.

- **Fu, Yuxi. 傅育熙.**
- **Title: Final Remark on the Decidability of PDA**
- **Abstract:** We will summarize the decidability results achieved over the last couple of years, focusing on (i) a simplified proof of Senizergues' well-known proof, and (ii) its extensions for new results.

- **Jansen, David**
- **Title: An O(m log n) algorithm for computing stuttering equivalence and branching bisimulation**
- **Abstract:** We provide a new algorithm to determine stuttering equivalence with time complexity O(m log n), where n is the number of states and m is the number of transitions of a Kripke structure. This algorithm can also be used to determine branching bisimulation in O(m log m) time. Theoretically, our algorithm substantially improves upon existing algorithms, which have time complexity of the form O(mn) at best. Moreover, it has better or equal space complexity. Practical results confirm these findings: they show that our algorithm can outperform existing algorithms by several orders of magnitude, especially when the Kripke structures are large. The importance of our algorithm stretches far beyond stuttering equivalence and branching bisimulation. The known O(mn) algorithms were already far more efficient than most other algorithms to determine behavioral equivalences (including weak bisimulation), and therefore they were often used as an essential preprocessing step. This new algorithm makes this use of stuttering equivalence and branching bisimulation even more attractive.

  Publication: This is a joint work with J. F. Groote, J. J. A. Keiren, and A. Wijs， published in: ACM Transactions on Computational Logic 18(2)2017: article 13.

- **Chen, Zhe 陈哲**
- **Title：Parametric runtime verification is NP-complete and coNP-complete**
- **Abstract：** In this article, we solve an important open problem – the computational complexity of parametric runtime verification against regular properties. To achieve this, we first formulate the membership problem of existential and universal parametric languages, then show that the membership problem of existential parametric regular languages is NP-complete, and the membership problem of universal parametric regular languages is coNP-complete. These computational complexity results show that parametric runtime verification of regular properties is NP-complete and coNP-complete. This gives a rigorous proof and a formal explanation of the inherent intractability of parametric runtime verification, which has been shown by the empirical experiments in the literature. In this sense, our work has moved one significant step on the theoretical aspect of runtime monitoring and verification.

  Publication: Information Processing Letters, Volume 123, July 2017.

- **Yin, Qiang 尹强**
- **Title: Two Lower Bounds for BPA**
- **Abstract:** Branching bisimilarity of normed Basic Process Algebra (nBPA) was claimed to be EXPTIME-hard in previous papers without any explicit proof. Recently it has been pointed out by Petr Jančar that the claim lacked proper justification. In this work, we develop a new complete proof for the EXPTIME-hardness of branching bisimilarity of nBPA. We also prove that the associated regularity problem of nBPA is PSPACE-hard. This improves previous P-hard result.

  Publication： Mingzhang Huang and Qiang Yin. Two Lower Bounds for BPA. CONCUR 2017

- **Wang, Hanpin 王捍贫**
- **Title: Logic for Reasoning about Cloud Storage Systems**
- **Abstract:** Cloud storage devices are elementary parts in many cloud computing systems. Cloud Storage Systems (CSS) have more features than traditional storage systems. An important one is that data are stored in blocks in CSSs. And each block is considered as a storage unit. Hence, CSSs usually have two kinds of storage units: ordinary locations and block locations. It makes CSSs very different from ordinary storage systems. Then how do we appeal formal methods to model, describe and reason about CSSs? In this presentation, based on Separation Logic, we propose a systematic method to verify the correctness of management programs in CSSs. The main contributions are as follows. (1) A language is introduced to describe the cloud storage management. (2) Assertions in Separation Logic are extended to describe the properties of blocks in CSSs. (3) Hoare-style rules are proposed to reason about the CSSs. Pre- and post-conditions are pairs of assertions.Using these methods, the partial correctness of cloud storage management can be verified.

- **Feng, Xinyu 冯新宇**
- **Title:** Progress of Concurrent Objects with Partial Methods
- **Abstract:** Various progress properties have been proposed for concurrent objects, such as wait-freedom, lock-freedom, starvation-freedom and deadlock-freedom. However, none of them applies to concurrent objects with partial methods, i.e., methods that are supposed not to return under certain circumstances. A typical example is the lock_acquire method, which must not return when the lock has already been acquired. In this work we propose two new progress properties, partial starvation-freedom (PSF) and partial deadlockfreedom (PDF), for concurrent objects with partial methods. We also design four patterns to write abstract specifications for PSF or PDF objects under strongly or weakly fair scheduling, so that these objects contextually refine the abstract specifications. Our Abstraction Theorem shows the equivalence between PSF (or PDF) and the progress-aware contextual refinement. Finally, we generalize the program logic LiLi to have a new logic to verify the PSF (or PDF) property and linearizability of concurrent objects. This is joint work with Hongjin Liang. The paper has been published at POPL 2018.

- **Cheng, Tong 程通**
- **Title: Analyzing Probabilistic Programs with Dynamic Logic**
- **Abstract:** We present a unified framework for the analysis of probabilistic programs based on Dynamic Logic in which both iterative and recursive programs can be analyzed. We augment the traditional rules of probabilistic Dynamic Logic with rules for reasoning about assignments, as well as proof rules for recursive programs with call-by-value parameters. We show soundness of our system with respect to a standard Markov kernel semantics. We give an

example of their use in the analysis of the Coupon Collector's Problem.
Publication: 2017 Logic and Computational Complexity Workshop (co-located with LICS)

- **Xia, Mingji 夏盟佶**
- **Title: About variable Lovász local lemma**
- **Abstract:** Lovász local lemma shows that given a dependency relation of random events, under which probabilities boundary, these events cannot cover the whole space. In the applications, the events are related, usually because they share random variables. In such a corresponding more specific variable-event dependency relation, the events maybe need higher probabilities to cover the whole space. For some cases we show the new probabilities boundary, to answer whether there is a gap between two boundaries.

- **Lin, Yuan 林苑**
- **Title： Assessing percolation threshold based on high-order non-backtracking matrices**
- **Abstract：** Percolation threshold of a network is the critical value such that when nodes or edges are randomly selected with probability below the value, the network is fragmented but when the probability is above the value, a giant component connecting a large portion of the network would emerge. Assessing the percolation threshold of networks has wide applications in network reliability, information spread, epidemic control, etc. The theoretical approach so far to assess the percolation threshold is mainly based on spectral radius of adjacency matrix or non-backtracking matrix, which is limited to dense graphs or locally treelike graphs, and is less effective for sparse networks with non-negligible amount of triangles and loops. In this paper, we study high-order non-backtracking matrices and their application to assessing percolation threshold. We first define high-order non-backtracking matrices and study the properties of their spectral radii. Then we focus on the 2nd-order non-backtracking matrix and demonstrate analytically that the reciprocal of its spectral radius gives a tighter lower bound than those of adjacency and standard non-backtracking matrices. We further build a smaller size matrix with the same largest eigenvalue as the 2nd-order non-backtracking matrix to improve computation efficiency. Finally, we use both synthetic networks and 42 real networks to illustrate that the use of the 2nd-order non-backtracking matrix does give better lower bound for assessing percolation threshold than adjacency and standard non-backtracking matrices.

- **Scheder, Domink**
- **Title：The PPSZ k-SAT Algorithm on Formulas with Many Solutions**
- **Abstract：** PPSZ is the fastest known algorithm for k-SAT, a central NP-complete problem. The algorithm is famous for being very simple to state and quite difficult to analyze. I will present recent work on the behavior of PPSZ on input formulas with many solutions.

- **Jiang, Ying 蒋颖**
- **Title: SCTL: Towards Combining Model Checking and Proof Checking**
- **Abstract:** Model checking and automated theorem proving are two pillars of formal methods. This work investigates model checking from an automated theorem proving perspective, aiming at combining the expressiveness of automated theorem proving and the complete automaticity of model checking. The focus of this work is on the verification of temporal logic properties of Kripke models. The main contributions of this paper are: first the definition of an extended computation tree logic that allows polyadic predicate symbols, then a proof system for this logic, taking Kripke models as parameters, then, the design of a proof-search algorithm for this calculus and a new automated theorem prover to implement it. The verification process

is completely automatic, and produces either a counterexample when the property does not hold, or a certificate when it does. The experimental result compares well to existing state-of-the-art tools on some benchmarks, including an application to air traffic control and the design choices that lead to this efficiency are discussed. This is a joint de work with G. Dowek, J. Liu and K. Ji.

- **Liao, Chao 廖超**
- **Title: Counting hypergraph colourings in the local lemma regime**
- **Abstract:** The local lemma is a powerful tool to show the existence of q-colourings for k-uniform hypergraphs under a simple degree bound. The original lemma is non-constructive, but Moser-Tardos' algorithm allows us to efficiently find such a colouring. However, if we want to uniformly at random generate one, the classic Markov chain approach does not work any longer in the said regime. In this talk, we will present an alternative approach to approximately counting and sampling hypergraph colorings in the local lemma regime. It is based on the recent work of Moitra (STOC, 2017). Our main contribution is to remove certain restrictions in Moitra's approach. Based on joint work with Heng Guo, Pinyan Lu, and Chihao Zhang.

- **Yang, Qizhe 杨启哲**
- **Title: Counting Finite Computations**
- **Abstract:** We report on a research progress to derive a closed formula for the number of finite state nondeterministic computations.

- **Fang, Zhixuan 房智轩**
- **Title: SCTL: Prices and Subsidies in the Sharing Economy**
- **Abstract:** The growth of the sharing economy is driven by the emergence of sharing platforms, e.g., Uber and Lyft, that match owners looking to share their resources with customers looking to rent them. The design of such platforms is a complex mixture of economics and engineering, and how to ``optimally'' design such platforms is still an open problem. In this paper, we focus on the design of prices and subsidies in sharing platforms. Our results provide insights into the tradeoff between revenue maximizing prices and social welfare maximizing prices. Specifically, we introduce a novel model of sharing platforms and characterize the profit and social welfare maximizing prices in this model. Further, we bound the efficiency loss under profit maximizing prices, showing that there is a strong alignment between profit and efficiency in practical settings. Our results highlight that the revenue of platforms may be limited in practice due to supply shortages; thus platforms have a strong incentive to encourage sharing via subsidies. We provide an analytic characterization of when such subsidies are valuable and show how to optimize the size of the subsidy provided. Finally, we validate the insights from our analysis using data from Didi Chuxing, the largest ridesharing platform in China.

- **Zhang, Tianyi 张天翼**
- **Title: SCTL: Improved distance sensitivity oracles via tree partitioning**
- **Abstract:** We introduce an improved structure of distance sensitivity oracle (DSO). The task is to preprocess a non-negatively weighted graph so that a data structure can quickly answer replacement path length for every triple of source, terminal and failed vertex. The previous best algorithm [Bernstein and Karger, 2009] constructs in time $\tilde{O}(mn)$ a distance sensitivity oracle of size $O(n^2 \log n)$ that processes queries in constant time. As an improvement, our oracle takes up$O(n^2)$space, while preserving constant query efficiency and $\tilde{O}(mn)$ preprocessing time. One should notice that space complexity and query time of our novel data structure are asymptotically optimal.

- **Wang, Zihe** 王子贺
- **Title： An Improved Welfare Guarantee for First Price Auctions**
- **Abstract：** Because equilibria in the first-price auction are notoriously difficult to compute theoretically, the first-price auction presents a daunting obstacle to classical economic analysis. In this talk, I will prove that the welfare of the first price auction in Bayes-Nash equilibrium is at least a .743-fraction of the welfare of the optimal mechanism assuming agents' values are independently distributed. The previous best bound was $1 - 1/e \approx .63$ using smoothness, the standard technique for reasoning about welfare of games in equilibrium.