



# Introduction

Property Testing is the study of super-fast (randomized) algorithms for approximate decision making. These algorithms are given direct access to items of a huge data set, and determine whether this data set has some predetermined (global) property or is far from having this property. Remarkably, this approximate decision is made by accessing a small portion of the data set. Property Testing has been a subject of intensive research in the last couple of decades, with hundreds of studies conducted in it and in closely related areas. Indeed, Property Testing is closely related to Probabilistically Checkable Proofs (PCPs), and is related to Coding Theory, Combinatorics, Statistics, Computational Learning Theory, Computational Geometry, and more. The mini-workshop, hosted by the Institute for Theoretical Computer Science (ITCS) at Tsinghua University (Beijing), aims to bring together a couple of dozen of leading international researchers in Property Testing and related areas.



# Committee

## Program Co-Chair

Amy Yuexuan Wang (Tsinghua University, China)  
Oded Goldreich (Weizmann Institute of Science, Israel)

## Organization Committee

Amy Yuexuan Wang (Chair) (Tsinghua University, China)  
Oded Goldreich (Weizmann Institute of Science, Israel)  
Xiaoming Sun (Tsinghua University, China)  
Meizhi Hu (Tsinghua University, China)  
Xiang Li (Tsinghua University, China)  
Yuying Chang (Tsinghua University, China)  
Jing Liu (Tsinghua University, China)  
Yan Zhang (Tsinghua University, China)  
Changxia Liu (Tsinghua University, China)

## Workshop Secretary

Yuying Chang (Tsinghua University, China)

## Local Arrangements

Amy Yuexuan Wang (Chair) (Tsinghua University, China)  
Xiaoming Sun (Tsinghua University, China)  
Meizhi Hu (Tsinghua University, China)  
Xiang Li (Tsinghua University, China)  
Yuying Chang (Tsinghua University, China)  
Jing Liu (Tsinghua University, China)  
Yan Zhang (Tsinghua University, China)  
Changxia Liu (Tsinghua University, China)  
Di Sun (Tsinghua University, China)  
Yanping Wang (Tsinghua University, China)  
Haiseng Liang (Tsinghua University, China)  
Yue Xu (Tsinghua University, China)

## **Workshop Secretary**

Yuying Chang (Tsinghua University, China)

## **Registration**

Yuying Chang (Tsinghua University, China)

Yanping Wang (Tsinghua University, China)

## **Publicity**

Xiang Li (Tsinghua University, China)

Haisheng Liang (Tsinghua University, China)

Yue Xu (Tsinghua University, China)

## **Finance**

Di Sun (Tsinghua University, China)

## **Technical Support**

Xiang Li (Tsinghua University, China)

Haisheng Liang (Tsinghua University, China)

Yue Xu (Tsinghua University, China)

# **Institute for Theoretical Computer Science (ITCS)**

<http://itcs.tsinghua.edu.cn/>

The Institute for Theoretical Computer Science (ITCS) is a new institute headed by Professor Andrew Chi-Chih Yao at Tsinghua University. Its mission is to nurture and develop the talents of students and researchers and to create knowledge for the advancement of computer science. It also aims to become one of the leading research centers on theoretical computer science in the world. The Institute already has an elite graduate student body and enjoys frequent visits by world-renowned scientists all year round. With a vibrant research environment and impressive research outputs, ITCS provides an ideal setting for fruitful interactions and collaborations among its members.

The Institute has a small number of permanent members and a large number of visiting members staying for varying duration, much in the same spirit as the Institute for Advanced Study at Princeton. For the fall of 2009, in residence are four permanent members, eleven post-doctors, plus many short-term visitors; there is also a Chair Professor Team whose members are frequent visitors of the Institute. Their research interests include complexity theory, quantum computation, combinatorial algorithms, wireless network theory and applications.



**Andrew Chi-Chih Yao**

Director, Institute for Theoretical Computer Science

2000 Turing Award Winner

<http://itcs.tsinghua.edu.cn/yao>

Professor Andrew Chi-Chih Yao, world-renowned computer scientist, was educated at Taiwan University and at Harvard, where he received a PhD in Physics in 1972. He decided to switch to computer science, foreseeing the unprecedented changes that computer science would bring to the global community. In 1975, he received his second PhD, in computer science, from the University of Illinois. His research interests include analysis of algorithms, computational complexity, cryptography and quantum computing. After serving on the faculty at the Massachusetts Institute of Technology (1975-1976), Stanford University (1976-1981, 1982-1986) and the University of California at Berkeley (1981-1982), he joined Princeton University in 1986 as the William and Edna Macaleer Professor of Engineering and Applied Science. In 2004, he left Princeton to become a Professor at Tsinghua University in Beijing and a Distinguished Professor-at-Large at the Chinese University of Hong Kong.

Professor Yao was awarded the A.M. Turing Award in 2000 for his contributions to the theory of computation, including communication complexity, pseudorandom number generation, and quantum communication. He is the first Chinese scientist to receive the prestigious Turing Award of the Association for Computing Machinery, the highest honor in computer science, widely regarded as the Nobel Prize of computing. Prof. Yao has received numerous other honors and awards including the George Polya Prize, and the Donald E. Knuth Prize, and honorary degrees from the Chinese University of Hong Kong, the Hong Kong University of Science and Technology, the City University of Hong Kong, and the University of Waterloo. He is a member of the US National Academy of Sciences, the American Academy of Arts and Sciences and the Chinese Academy of Sciences.



# Overall Program

	Jan. 7 Thursday	Jan. 8 Friday	Jan. 9 Saturday	Jan. 10 Sunday
09:00-10:15		Session 1	Session 4	Session 7
10:15-10:45		Group Photo Coffee Break	Coffee Break	
10:45-12:00		Session 2	Session 5	Session 8
12:00-14:00		Lunch		
14:00-15:30	Registration	Session 3	Session 6	Session 9
15:30-16:00		Coffee Break		
16:00-17:00		Panel 1	Panel 2	Panel 3
18:00-20:00	Banquet	Dinner	Dinner	Dinner

## Thursday January 7, 2010

TIME	ACTIVITIES	VENUE
14:00-17:00	Registration	Wenjin Hotel
18:00-20:00	Banquet	Grand Ball Room Wenjin Hotel

## Friday January 8, 2010

TIME	ACTIVITIES		VENUE
09:00-09:15	Welcoming Comments		
09:15-10:15	Session 1 Chair: Oded Goldreich	Title: Testing by Implicit Learning <b>Rocco Servedio</b> Title: Testing (subclasses of) Linear Threshold Functions <b>Kevin Matulef</b>	Room 1-315 FIT Building Tsinghua University
10:15-10:45	Group Photo + Coffee Break		Photo at Main Gate of FIT Building
10:45-12:00	Session 2 Chair: Avrim Blum	Title: Testing Juntas and Function Isomorphism <b>Eric Blais</b> Title: Hierarchy Theorems for Property Testing <b>Michael Krivelevich</b>	Room 1-315 FIT Building Tsinghua University
12:00-14:00	Lunch		Wenjin Hotel
14:00-15:30	Session 3 Chair: Bernard Chazelle	Title: A Survey on Property Testing in the 'Underlying Graph' or 'Massively Parametrized' Model <b>Ilan Newman</b> Title: Transitive-Closure Spanners with Applications to Monotonicity Testing <b>Sofya Raskhodnikova</b> Title: Testing Euclidean Spanners <b>Christian Sohler</b>	Room 1-315 FIT Building Tsinghua University
15:30-16:00	Coffee Break		
16:00-17:00	Panel 1	On the Connection of Property Testing to Computational Learning Theory and Computational Geometry <b>Avrim Blum, Bernard Chazelle, Rocco Servedio</b>	
18:00-20:00	Dinner		Wenjin Hotel

## Saturday January 9, 2010

TIME	ACTIVITIES		VENUE
09:00-10:15	Session 4 Chair: Shafi Goldwasser	Title: Invariance in Property Testing <b>Madhu Sudan</b> Title: Testing Linear-Invariant Non-Linear Properties <b>Victor Chen</b>	Room 1-315 FIT Building Tsinghua University
10:15-10:45	Coffee Break		
10:45-12:00	Session 5 Chair: Michael Saks	Title: Testing Linear Invariant Properties <b>Asaf Shapira</b> Title: On Constant Time Approximation of Invariants of Bounded Degree Graphs <b>Noga Alon</b> Title: Maintaining A Large Matching or A Small Vertex Cover <b>Ronitt Rubinfeld</b> Title: External Sampling <b>Krzysztof Onak</b>	Room 1-315 FIT Building Tsinghua University
12:00-14:00	Lunch		Wenjin Hotel
14:00-15:30	Session 6 Chair: Noga Alon	Title: Sublinear Graph Approximation Algorithms <b>Krzysztof Onak</b> Title: Local Monotonicity Reconstruction <b>Michael Saks</b> Title: Testing Properties of Distributions: A Survey <b>Ronitt Rubinfeld</b>	Room 1-315 FIT Building Tsinghua University
15:30-16:00	Coffee Break		
16:00-17:00	Panel 2	On the Connection of Property Testing to Coding Theory, Combinatorics, and Statistics <b>Madhu Sudan, Noga Alon, Ronitt Rubinfeld</b>	
18:00-20:00	Dinner		Wenjin Hotel



## Sunday January 10, 2010

TIME	ACTIVITIES	VENUE
09:00-10:15	<p>Session 7 Chair: Ronitt Rubinfeld</p> <p>Title: Composition of Low-error 2-query PCPs Using Decodable PCPs <b>Prahladh Harsha</b></p> <p>Title: A Hypergraph Dictatorship Test with Perfect Completeness <b>Victor Chen</b></p> <p>Title: Comparing the Strength of Query Types in Property Testing <b>Michael Krivelevich</b></p>	Room 1-315 FIT Building Tsinghua University
10:15-10:45	Coffee Break	
10:45-12:00	<p>Session 8 Chair: Michael Krivelevich</p> <p>Title: Some Recent Results on Testing of Sparse Linear Codes <b>Shubhangi Saraf</b></p> <p>Title: Optimal Testing of Reed-Muller Codes <b>Swastik Kopparty</b></p>	Room 1-315 FIT Building Tsinghua University
12:00-14:00	Lunch	Wenjin Hotel
14:00-15:30	<p>Session 9 Chair: Madhu Sudan</p> <p>Title: Limiting the Rate of Locally Testable Codes <b>Eli Ben-Sasson</b></p> <p>Title: Symmetric LDPC Codes and Local Testing <b>Tali Kaufman</b></p> <p>Title: Testing Monotone Continuous Distributions on High-dimensional Real Cubes <b>Artur Czumaj</b></p> <p>Title: The Query Complexity of Edit Distance <b>Krzysztof Onak</b></p> <p>Title: Testing and Reconstruction of Lipschitz Functions with Applications to Privacy <b>Sofya Raskhodnikova</b></p> <p>Title: Algorithmic Aspects of Property Testing in the Dense Graphs Model <b>Oded Goldreich</b></p>	Room 1-315 FIT Building Tsinghua University
15:30-16:00	Coffee Break	
16:00-17:00	<p>Panel 3</p> <p>On Decoding in the Low-error Regime <b>Prahladh Harsha</b></p> <p>On Algorithmic vs Complexity Theoretic Aspects <b>Oded Goldreich</b></p>	Room 1-315 FIT Building Tsinghua University
18:00-20:00	Dinner	Wenjin Hotel



# Speech Information

## Invited Attendees:

Noga Alon (Tel Aviv University, Israel)  
Eli Ben-Sasson (Technion - Israel Institute of Technology)  
Eric Blais (CMU, USA)  
Avrim Blum (CMU, USA)  
Bernard Chazelle (Princeton University, USA)  
Victor Chen (Tsinghua University, China)  
Artur Czumaj (University of Warwick, UK)  
Oded Goldreich (Weizmann Institute of Science, Israel)  
Shafi Goldwasser (MIT, USA)  
Praladh Harsha (University of Texas at Austin, USA)  
Tali Kaufman (MIT, USA)  
Swastik Kopparty (MIT, USA)  
Michael Krivelevich (Tel Aviv University, Israel)  
Kevin Matulef (Tsinghua University, China)  
Ilan Newman (Haifa University, Israel)  
Krzysztof Onak (MIT, USA)  
Sofya Raskhodnikova (Pennsylvania State University, USA)  
Ronald L. Rivest (MIT, USA)  
Ronitt Rubinfeld (MIT, USA)  
Michael Saks (Rutgers University, USA)  
Shubhangi Saraf (MIT, USA)  
Rocco Servedio (Columbia University, USA)  
Asaf Shapira (Georgia Tech, USA)  
Christian Sohler (TU Dortmund, Germany)  
Madhu Sudan (MIT, USA)



## **Noga Alon**

Tel Aviv University, Israel  
<http://www.cs.tau.ac.il/~nogaa/>

Title:

On Constant Time Approximation of Invariants of Bounded Degree Graphs

### **Abstract:**

How well can the maximum size of an independent set, or the minimum size of a dominating set of a graph in which all degrees are at most  $d$  be approximated by a randomized constant time algorithm? Motivated by results and questions of Nguyen and Onak, and of Parnas, Ron and Trevisan, we show that the best approximation ratio that can be achieved for the first question (independence number) is between  $\Omega(d/\log d)$  and  $O(d \log \log d / \log d)$ , whereas the answer to the second (domination number) is  $(1+o(1)) \ln d$ .

### **Biography:**

Noga Alon is a Baumritter Professor of Mathematics and Computer Science in Tel Aviv University, Israel and also holds a special long term visiting position in the Institute for Advanced Study, Princeton. He works in Combinatorics and Theoretical Computer Science, and contributed to the development of probabilistic and algebraic methods in Discrete Mathematics, the study of derandomization and expander graphs, the design of streaming algorithms, and the solution of problems in Combinatorics, Information Theory and Discrete Geometry. He has given plenary addresses in the European Congress of Mathematics and in the International Congress of Mathematicians, is a member of the Israel National Academy of Sciences and of the Academia Europaea, and received the Erdos Prize, the Feher Prize, the Polya Prize, the Bruno Memorial Award, the Landau Prize, the Godel Prize and the Israel Prize.



### Eli Ben-Sasson

Technion – Israel Institute of Technology  
<http://www.cs.technion.ac.il/~eli/>

Title:  
Limiting the Rate of Locally Testable Codes

#### Abstract:

Motivated by the question of whether an asymptotically good family of locally testable codes (LTCs) exists, we show a number of results that have a common theme. They all give subconstant upper bounds on the rate of certain families of LTCs, showing these families are not asymptotically good.

+ Locally Testable Codes Require Redundant Testers (joint work with Venkatesan Guruswami, Tali Kaufman, Madhu Sudan and Michael Viderman): Linear LTCs that have a very small number of tests (a test for a linear LTC is a word in the dual code that has small support), barely more than the minimal number needed to characterize the code (i.e., to span the dual code), have exponentially bad rate.

At the opposite extreme we get:

+ Dense locally testable codes have exponentially small rate (joint work with Michael Viderman, unpublished): A family of locally testable codes with query complexity  $q$  is called dense if a constant fraction of all  $(q - 1)$ -tuples participate in some test. (For instance, Hadamard codes are dense because every pair of indices is involved in some 3-query test). Using recent results from additive combinatorics we show that such codes have exponentially small rate.

+ Affine Invariant locally testable codes have exponentially small rate (joint work with Madhu Sudan, unpublished): In this work we show that all affine-invariant locally testable codes are essentially families of low-degree polynomials. This implies that the rate of families of affine invariant codes (discussed in Madhu's entry of this webpage) is exponentially small.

+ Sound 3-query PCPPs are long (joint work with PRAHLADH HARSHA, ODED LACHISH and ARIE MATSLIAH): Every linear error correcting code can be converted into a LTC by appending to a codeword a PCP of proximity (PCPP). The rate of the resulting LTC is determined by the length of the PCPP appended to it.

Here we showed a rate-soundness tradeoff that roughly says that short PCPPs cannot have as good a soundness as long ones. In other words, better rate comes at the price of worse soundness.

#### Biography:

Eli Ben-Sasson completed his Ph.D. at the Hebrew University in 2001 (advisor: Avi Wigderson). Subsequently he was a postdoctoral fellow at Harvard (host: Salil Vadhan) and MIT (host: Madhu Sudan). After spending a year at the Radcliffe Institute for Advanced Study and another year at the Toyota Technological Institute at University of Chicago, he joined in 2005 the Department of Computer Science at the Technion – Israel Institute of Technology.



## Eric Blais

CMU, USA  
<http://www.cs.cmu.edu/~eblais/>

Title 1:  
Testing Function Isomorphism  
Title 2:  
Testing Juntas

### Abstract 1:

Given a boolean function  $g: \{0,1\}^n \rightarrow \{0,1\}$ , a  $g$ -isomorphism tester is an algorithm that distinguishes functions that are isomorphic to  $g$  (that is, functions that are identical to  $g$  up to permutation of the variables) from functions that are far from being isomorphic to  $g$  with high probability. Following standard conventions, we say that testing  $g$ -isomorphism is easy when it can be tested with a constant number of queries.

The  $g$ -isomorphism testing problem was first introduced by Fischer, Kindler, Ron, Safra, and Samorodnitsky (2004). They showed that testing isomorphism to a  $O(1)$ -junta (i.e., a function with a constant number of relevant variables) is easy, while testing isomorphism to the  $k$ -Parity function is hard when  $\omega(1) \leq k \leq o(n)$ .

We introduce two new lower bounds for testing function isomorphism:

1. We show that testing  $g$ -isomorphism is hard for every function  $g$  that is a  $k$ -junta and far from a  $(k-1)$ -junta, when  $\omega(1) \leq k \leq n - \omega(1)$ . This confirms a conjecture of Fischer et al.
2. We show that testing isomorphism to the Majority-on- $k$ -bits is hard when  $\omega(1) \leq k \leq n - \omega(1)$ , using a new invariance principle.

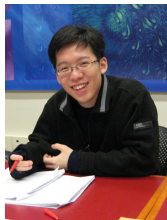
### Abstract 2:

A function on  $n$  variables is a  $k$ -junta if it depends on at most  $k$  of its variables. Fischer, Kindler, Ron, Safra, and Samorodnitsky (2004) showed that it is possible to test a function for the property of being a  $k$ -junta with  $\tilde{O}(k^2)$  queries. (All bounds in this abstract are presented in terms of a constant-valued  $\epsilon$  approximation parameter.)

In two recent works, we introduced new algorithms for testing juntas more efficiently. The first (2008) is a non-adaptive algorithm that tests  $k$ -juntas with  $\tilde{O}(k^{3/2})$  queries. The second (2009) is an adaptive one-sided error algorithm that tests  $k$ -juntas with  $O(k \log k)$  queries. Chockler and Gutfreund (2004) showed that  $\Omega(k)$  queries are required to test  $k$ -juntas, so the second algorithm is optimal up to a log factor.

### Biography:

Eric Blais is a fourth-year Ph.D. student in the School of Computer Science at Carnegie Mellon University. He completed a B.Math. in computer science at the University of Waterloo and a M.Sc. in computer science at McGill University. His advisor is Ryan O'Donnell. His research interests span theoretical computer science, the analysis of boolean functions, and probability theory. He is particularly interested in property testing over boolean functions.



### Victor Chen

Tsinghua University, China  
<http://itcs.tsinghua.edu.cn/~victor/>

Title 1:

A Hypergraph Dictatorship Test with Perfect Completeness

Title 2:

Testing Linear-Invariant Non-Linear Properties

#### Abstract 1:

A hypergraph dictatorship test is first introduced by Samorodnitsky and Trevisan and serves as a key component in their unique games based PCP construction. Such a test has oracle access to a collection of functions and determines whether all the functions are the same dictatorship, or all their low degree influences are  $\epsilon(1)$ . The test by Samorodnitsky and Trevisan makes  $q^{\Omega(1)}$  queries and has amortized query complexity  $1 + O\left(\frac{\log q}{q}\right)$  but has an inherent loss of perfect completeness. In this paper we give an (adaptive) hypergraph dictatorship test that achieves both perfect completeness and amortized query complexity  $1 + O\left(\frac{\log q}{q}\right)$ .

#### Abstract 2:

We consider the task of testing properties of Boolean functions that are invariant under linear transformations of the Boolean cube. Previous work in property testing, including the linearity test and the test for Reed-Muller codes, has mostly focused on such tasks for linear properties. The one exception is a test due to Green for “triangle freeness”: a function  $f: \{0,1\}^n \rightarrow \{0,1\}$  satisfies this property if  $f(x), f(y), f(x+y)$  do not all equal 1, for any pair  $x, y \in \{0,1\}^n$ . Here we extend this test to a more systematic study of testing for linear-invariant non-linear properties. We consider properties that are described by a single forbidden pattern (and its linear transformations), i.e., a property is given by  $k$  points  $v_1, \dots, v_k \in \{0,1\}^k$  and  $f: \{0,1\}^n \rightarrow \{0,1\}$  satisfies the property that if for all linear maps  $L: \{0,1\}^k \rightarrow \{0,1\}^n$  it is the case that  $f(L(v_1)), \dots, f(L(v_k))$  do not all equal 1. We show that this property is testable if the underlying matroid specified by  $v_1, \dots, v_k$  is a graphic matroid. This extends Green’s result to an infinite class of new properties. Our techniques extend those of Green and in particular we establish a link between the notion of “1-complexity linear systems” of Green and Tao, and graphic matroids, to derive the results.

#### Biography:

Victor Chen recently obtained his PhD in mathematics from the Massachusetts Institute of Technology. Previously, he completed his undergraduate studies at the University of Texas at Austin. His research interests lie in property testing, coding theory, and combinatorics.



## **Artur Czumaj**

University of Warwick, UK  
<http://www.dcs.warwick.ac.uk/~czumaj/>

Title:  
Testing Monotone Continuous Distributions on High-dimensional Real Cubes

### **Abstract:**

We study the task of testing properties of probability distributions. We consider a scenario in which we have access to independent samples of an unknown distribution  $D$  with infinite (perhaps even uncountable) support. Our goal is to test whether  $D$  has a given property or it is  $\epsilon$ -far from it (in the statistical distance, with the L1-distance measure).

It is not difficult to see that for many natural distributions on infinite or uncountable domains, no testing algorithm can exist and the central objective of our study is to understand if there are any nontrivial distributions that can be efficiently tested. For example, it is easy to see that there is no testing algorithm that tests if a given probability distribution on  $[0, 1]$  is uniform. We show however, that if some additional information about the input distribution is known, testing uniform distribution is possible. We extend the recent result about testing uniformity for monotone distributions on Boolean  $n$ -dimensional cubes by Rubinfeld and Servedio (STOC'2005) to the case of real  $[0, 1]^n$  cubes. We show that if a distribution  $D$  on  $[0, 1]^n$  is monotone, then one can test if  $D$  is uniform with the sample complexity  $O(n / \epsilon^2)$ . This result is optimal up to a polylogarithmic factor.

### **Biography:**

Artur Czumaj is a Professor of Computer Science and Director of the Centre for Discrete Mathematics and its Applications (DIMAP) at the University of Warwick. He received his Ph.D. in 1995 from the University of Paderborn in Germany. Before joining the University of Warwick in 2006, he was with the University of Paderborn and with the New Jersey Institute of Technology. His main research interest is in the broadly understood area of the design of randomized algorithms and their probabilistic analysis, with applications to property testing and sublinear algorithms, optimization algorithms, parallel and distributed computing, string matching, and algorithmic game theory.



### Oded Goldreich

The Weizmann Institute of Science, Israel  
<http://www.wisdom.weizmann.ac.il/~oded/>

Title:  
Algorithmic Aspects of Property Testing in the Dense Graphs Model

#### Abstract:

In this paper we consider two refined questions regarding the query complexity of testing graph properties in the adjacency matrix model. The first question refers to the relation between adaptive and non-adaptive testers, whereas the second question refers to testability within complexity that is inversely proportional to the proximity parameter, denoted  $\epsilon$ . The study of these questions reveals the importance of algorithmic design (also) in this model. The highlights of our study are:

A gap between the complexity of adaptive and non-adaptive testers. Specifically, there exists a (natural) graph property that can be tested using  $\tilde{O}(\epsilon^{-1})$  adaptive queries, but cannot be tested using  $\Omega(\epsilon^{-3/2})$  non-adaptive queries.

In contrast, there exist natural graph properties that can be tested using  $\tilde{O}(\epsilon^{-1})$  non-adaptive queries, whereas  $\Omega(\epsilon^{-1})$  queries are required even in the adaptive case.

We mention that the properties used in the foregoing conflicting results have a similar flavor, although they are of course different.

KEYWORDS: Adaptivity vs Non-adaptivity, Graph Properties

#### Biography:

Oded Goldreich is a Professor of Computer Science at the Faculty of Mathematics and Computer Science of Weizmann Institute of Science, Israel. His research interests lie within the theory of computation. Specifically, his main research areas are the interplay of randomness and computation (specifically, various types of pseudorandomness and probabilistic proof systems) as well as the foundations of cryptography. In addition, he is interested in complexity theory at large.





## **Prahladh Harsha**

University of Texas at Austin, USA  
<http://www.cs.utexas.edu/~prahladh/>

Title :  
Composition of Low-error 2-query PCPs Using Decodable PCPs

### **Abstract:**

The main result of this is new generic, composition method for low error two-query probabilistically checkable proofs. Proof composition is an essential ingredient in all constructions of probabilistically checkable proofs (PCPs).

Earlier composition methods were either inapplicable in the low-error regime or non-modular (i.e., very much tailored to the specific PCPs that were being composed), if not both. Furthermore, until recently, composition in the low error regime suffered from incurring an extra consistency query, resulting in PCPs that are not two-query and hence, much less useful for hardness-of-approximation reductions. Also, generic composition was known only in the high error regime using a variant of PCPs called PCPs of proximity (PCPPs).

One of the critical components in the new composition is a new variant of PCP called “decodable PCP”. A decodable PCP, besides being locally checkable as a standard PCP, is also locally decodable, in the sense, that the original NP witness can be locally decoded from it.

The new composition theorem can be used to give a considerably simpler and modular proof of the recent break-through result of Moshkovitz and Raz [FOCS 2008]: construction of 2-query low-error PCPs of nearly linear length.

### **Biography:**

Prahladh Harsha received his B.Tech. degree in Computer Science and Engineering from the Indian Institute of Technology, Madras in 1998 and his S.M. and Ph.D. degrees in Computer Science from the Massachusetts Institute of Technology in 2000 and 2004 respectively. Starting Jan 2010, he will be joining the faculty of the School of Technology and Computer Science in the Tata Institute of Fundamental Research, Mumbai, India. Prior to this, he was a post-doctoral researcher at Microsoft Research, Silicon Valley and a research assistant professor at the Toyota Technological Institute at Chicago. He works in the area of algorithms and computational complexity.

### **Tali Kaufman**

MIT, USA

Title:

Symmetric LDPC Codes and Local Testing

#### **Abstract:**

In a work with Madhu Sudan we show that polynomial codes are testable, using the fact they have a characterization by a "single" short (local) constraint and its orbit under the affine group. This motivates the following question: Which other codes are characterized by a short constraint and its orbit under a certain group?

In a work with Avi Wigderson we present a framework we call "Cayley codes" for obtaining codes characterized by a short constraint and its orbit under some group. Using this framework we show new codes that are better than polynomial codes (the ratio between  $1/\text{rate}$  and the locality is better than in polynomial codes). However, it is still open whether these codes are testable. Additionally, we show that good codes (of constant rate and distance) that are characterized by a single constant-length constraint and its orbit under some group, if exist, must be seriously non-Abelian, i.e, they cannot be invariant even under a solvable group (a generalization of an Abelian group).

#### **Biography:**

Tali Kaufman was doing her PhD studies at Tel-Aviv University under the supervision of Prof. Noga Alon and Prof. Michael Krivelevich. Following that, she spent a few years as a postdoctoral fellow at MIT, Princeton, and the Weizmann Institute.



## **Swastik Kopparty**

MIT, USA

<http://web.mit.edu/swastik/www/>

Title:

Optimal testing of Reed-Muller codes

### **Abstract:**

We consider the problem of testing if a given function  $f: \mathbb{F}_2^n \rightarrow \mathbb{F}_2$  is close to any degree  $d$  polynomial in  $n$  variables, also known as the Reed-Muller testing problem. Alon, Kaufman, Krivelevich, Litsyn and Ron (AKKLR) proposed and analyzed a natural  $2^{d+1}$ -query test for this property and showed that it accepts every degree  $d$  polynomial with probability 1, while rejecting functions that are  $\Omega(1)$ -far with probability  $(1/(d \cdot 2^d))$ . We give an asymptotically optimal analysis of their test showing that it rejects functions that are (even only)  $\Omega(2^{-d})$ -far with  $\Omega(1)$ -probability (so the rejection probability is a universal constant independent of  $d$  and  $n$ ). Our proof works by induction on  $n$ , and yields a new analysis of even the classical Blum-Luby-Rubinfeld linearity test, for the setting of functions mapping  $\mathbb{F}_2^n$  to  $\mathbb{F}_2$ . The optimality follows from a tighter analysis of counterexamples to the inverse conjecture for the Gowers norm constructed by [Green & Tao] and [Lovett, Meshulam & Samorodnitsky]. Our result gives a new relationship between the  $(d+1)$ st-Gowers norm of a function and its maximal correlation with degree  $d$  polynomials. For functions highly correlated with degree  $d$  polynomials, this relationship is asymptotically optimal. Our improved analysis of the AKKLR-test also improves the parameters of an XOR lemma for polynomials given by Viola and Wigderson. Finally, the optimality of our result also implies a query-hierarchy result for property testing of affine-invariant properties: For every function  $q(n)$ , it gives a affine-invariant property that is testable with  $O(q(n))$ -queries, but not with  $o(q(n))$ -queries, complementing an analogous result of Goldreich et al. (GKNR08) for graph properties.

### **Biography:**

Swastik is a 6th year PhD student at MIT, advised by Madhu Sudan. He is interested in codes, pseudorandomness and complexity.



### Michael Krivelevich

Tel Aviv University, Israel  
<http://www.cs.tau.ac.il/~krivelev/>

Title 1:  
Hierarchy Theorems for Property Testing

Title 2:  
Comparing the Strength of Query Types in Property Testing

**Abstract 1:** The one-line summary is that hierarchy theorems do exist for the query complexity of property testing problems over several intensively studied function models. A more detailed summary follows.

Referring to the query complexity of property testing, we prove the existence of a rich hierarchy of corresponding complexity classes. That is, for any relevant function  $q$ , we prove the existence of properties that have testing complexity  $\Theta(q)$ . Such results are proven in three standard domains often considered in property testing: generic functions, adjacency predicates describing (dense) graphs, and incidence functions describing bounded-degree graphs. While in two cases the proofs are quite straightforward, the techniques employed in the case of the dense graph model seem significantly more involved. Specifically, problems that arise and are treated in the latter case include (1) the preservation of distances between graph under a blow-up operation, and (2) the construction of monotone graph properties that have local structure.

**Abstract 2:** We study the power of four query models in the context of property testing in general graphs, where our main case study is the problem of testing  $k$ -colorability. Two query types, which have been studied extensively in the past, are pair queries and neighbor queries. The former corresponds to asking whether there is an edge between any particular pair of vertices, and the latter to asking for the  $i$ 'th neighbor of a particular vertex. We show that while for pair queries, testing  $k$ -colorability requires a number of queries that is a monotone decreasing function in the average degree  $d$ , the query complexity in the case of neighbor queries remains roughly the same for every density and for large values of  $k$ . We also consider a combined model that allows both types of queries, and we propose a new, stronger, query model, related to the field of Group Testing. We give one-sided error upper and lower bounds for all the models, where the bounds are nearly tight for three of the models. In some of the cases our lower bounds extend to two-sided error algorithms.

#### Biography:

Michael Krivelevich got his PhD in 1997 at Tel Aviv University under the supervision of Prof. Noga Alon. After a postdoc with the Institute for Advanced Study in Princeton, and the Center for Discrete Mathematics and Computer Science at Rutgers University, USA, he returned to Tel Aviv University in 1999 and is now a Full Professor with the School of Mathematical Sciences. During 2007-2009 he served as the Head of the School.

Prof. Krivelevich has authored more 120 papers in Combinatorics and its applications. He is a recipient of the 2007 Pazy Memorial Award (jointly with A. Frieze) of the United States - Israel Binational Science Foundation.



## **Kevin Matulef**

Tsinghua University, China

<http://itcs.tsinghua.edu.cn/postdoc/matulef/>

Title:

Testing (subclasses of) Linear Threshold Functions

### **Abstract:**

A halfspace over the  $n$ -dimensional Boolean cube is a Boolean function that is defined by a linear form  $w \cdot x + \theta$ . Given an input  $x$ , the value of the halfspace is  $\text{sign}(w \cdot x - \theta)$ , i.e. the sign (positive or negative) of the linear form. Halfspaces are a well studied class in learning theory and complexity theory.

We give an efficient testing algorithm for the class of halfspaces. Our algorithm uses  $\text{poly}(1/\epsilon)$  queries, independent of  $n$ , to test whether any given Boolean function is a halfspace versus  $\epsilon$ -far from every halfspace. Our testing algorithm uses new structural results about the Fourier representation of halfspaces.

We also show that while the class of all halfspaces is efficiently testable (with query complexity independent of  $n$ ), the same is not true for some natural subclasses of halfspaces. Specifically, we show that for the class of all “unate reorientations of majority” (halfspaces in which each weight  $w_i$  is  $\pm 1$  and the threshold  $\theta$  is 0), any nonadaptive testing algorithm must make  $\Omega(\log n)$  queries.

### **Biography:**

Kevin Matulef is a postdoctoral researcher at Tsinghua University. He received his Ph.D. in July 2009 from MIT under the supervision of Ronitt Rubinfeld. Prior to that, he received his undergraduate degree in mathematics and computer science from Brown University, and a certificate of advanced study from Cambridge University. His interests are in property testing, learning, and complexity.



### **Ilan Newman**

Haifa University, Israel  
<http://www.cs.haifa.ac.il/~ilan/>

**Title:**

A Survey on Property Testing in the 'Underlying Graph' or 'Massively Parametrized' Model

**Abstract:**

Co-authored (with some multiplicities, depending on the specific results) with S. Chakraborty, E. Fischer, S. Halevi, O. Lachish, A. Mastliah, D. Tzur, S. Yahalom.

In this model a property is a 'large' structure with some boolean/general variables, and the property is the set of assignments that satisfy some predicate. E.g., the structure is a graph with a boolean variable on each edge, interpreted together as defining a subgraph. The property contains all the subgraphs, so defined, that are connected.

I suggest to survey some testing results on such models.

**Biography:**

Ilan Newman has been on the faculty at Haifa University since 1992. He obtained his B. Sc., and M. Sc., at the Technion. He received his Ph.D., in 1992 at the Computer Science Department of the Hebrew University under the supervision of Avi Wigderson. The title of his thesis was "On the complexity of simple Boolean functions." His current research interests are in finite metric embeddings, combinatorial algorithms, property testing, and computational complexity.



## **Krzysztof Onak**

MIT, USA

<http://people.csail.mit.edu/konak/>

Title 1: External Sampling

Title 2: Sublinear Graph Approximation Algorithms

Title 3: The Query Complexity of Edit Distance

### **Abstract 1:**

We initiate the study of sublinear-time algorithms in the external memory model. In this model, the data is stored in blocks of a certain size  $B$ , and the algorithm is charged a unit cost for each block access. This model is well-studied, since it reflects the computational issues occurring when the (massive) input is stored on a disk. Since each block access operates on  $B$  data elements in parallel, many problems have external memory algorithms whose number of block accesses is only a small fraction (e.g.  $1/B$ ) of their main memory complexity.

However, to the best of our knowledge, no such reduction in complexity is known for any sublinear-time algorithm. One plausible explanation is that the vast majority of sublinear-time algorithms use random sampling and thus exhibit no locality of reference. This state of affairs is quite unfortunate, since both sublinear-time algorithms and the external memory model are important approaches to dealing with massive data sets, and ideally they should be combined to achieve best performance.

We show that such combination is indeed possible. In particular, we consider three well-studied problems: testing of distinctness, uniformity, and identity of an empirical distribution induced by data. For these problems we show random-sampling-based algorithms whose number of block accesses is up to a factor of  $1/\sqrt{B}$  smaller than the main memory complexity of those problems. We also show that this improvement is optimal for those problems.

Since these problems are natural primitives for a number of sampling-based algorithms for other problems, our tools improve the external memory complexity of other problems as well.

Joint work with Alexandr Andoni, Piotr Indyk, and Ronitt Rubinfeld.

### **Abstract 2:**

I will present two papers concerning sublinear approximation:

1. In the first paper, we give a technique for transforming a certain class of classical approximation algorithms into constant-time algorithms that approximate the size of the optimal solution. The main result is the first approximation algorithm that for the family of graphs with degree bounded by  $d$ , computes the maximum matching size to within  $\epsilon n$  in time that only depends on  $d$  and  $\epsilon$ . (Constant Time Approximation Algorithms via Local Improvements)

2. Such an approximation algorithm does not exist for some other combinatorial problems, including vertex cover and dominating set. Nevertheless, we show that an additive  $\epsilon n$  approximation can be computed in constant time for these two problems for any hyperfinite family of graphs. A byproduct of our techniques is a simple proof for the theorem of Benjamini, Schramm, and Shapira (STOC 2008) that every minor-closed property of bounded-degree graphs is testable in constant time. (Local Graph Partitions for Approximation and Testing)

Joint work with Avinatan Hassidim, Jonathan A. Kelner, and Huy N. Nguyen.

### **Abstract 3:**

We study the query complexity of estimating the edit distance between two strings. In our model, the algorithm knows one string entirely, and has only query access to the other string. The goal is to estimate (approximate) the edit distance between them using few queries. We give both upper and lower bounds for this problem. These bounds are near-tight in at least one regime of the approximation factor, and have further implications.

Joint work with Alexandr Andoni and Robert Krauthgamer

### **Biography:**

Krzysztof is a PhD student at MIT. He is advised by Ronitt Rubinfeld. Before coming to MIT, he obtained a Master of Science degree from the University of Warsaw. Krzysztof's main research interests are algorithms, especially algorithms for massive data sets, which includes sublinear-time algorithms, property testing, and streaming.





## **Sofya Raskhodnikova**

Pennsylvania State University, USA  
<http://www.cse.psu.edu/~sofya/>

Title 1: Transitive-Closure Spanners with Applications to Monotonicity Testing

Title 2: Testing and Reconstruction of Lipschitz Functions with Applications to Privacy

### **Abstract 1:**

This is an abstract for two related papers:

Transitive-Closure Spanners, Arnab Bhattacharyya, Elena Grigorescu, Kyomin Jung, Sofya Raskhodnikova, David Woodruff, Proceedings of the 20th ACM-SIAM SODA, 531–540, 2009.

Transitive-Closure Spanners of the Hypercube and the Hypergrid, Arnab Bhattacharyya, Elena Grigorescu, Kyomin Jung, Sofya Raskhodnikova, David Woodruff, Electronic Colloquium on Computational Complexity, TR09--046, 2009. Work in progress.

We define the notion of a transitive-closure spanner of a directed graph. Given a directed graph  $G = (V, E)$  and an integer  $k \geq 1$ , a  $k$ -transitive-closure-spanner ( $k$ -TC-spanner) of  $G$  is a directed graph  $H = (V, E_H)$  that has (1) the same transitive-closure as  $G$  and (2) diameter at most  $k$ . These spanners were studied implicitly in access control, property testing, and data structures, and properties of these spanners have been rediscovered over the span of 20 years. We bring these areas under the unifying framework of TC-spanners. We abstract the common task implicitly tackled in these diverse applications as the problem of constructing sparse TC-spanners.

In the first paper above, we define transitive-closure spanners, explain several applications, including constructing fast monotonicity testers, give several approximation algorithms and hardness results. In the second paper, we study the number of edges in the sparsest 2-TC-spanners of the directed hypercube and the hypergrid. We also have new results (not in the archive version above) on  $k$ -TC-spanners for the hypercube and the hypergrid for  $k > 2$ , and more generally, of low-dimensional posets.

### **Abstract 2:**

A function  $f(x_1, \dots, x_d)$  is called Lipschitz if changing the value of one of the arguments by 1 changes the value of the function by at most 1. In other words, Lipschitz functions are not very sensitive to changes in the inputs. In this brief talk we will describe several results on testing if a function is Lipschitz and reconstructing Lipschitz functions. We will also mention applications to programs that operate with noisy inputs and to privacy. For the first application, the Lipschitz property of the function computed by a program corresponds to a notion of robustness to noise in the data. The application to privacy is based on the fact that Lipschitz functions of entries in a database of sensitive information can be released with very little added noise while preserving the privacy of individuals whose data is stored in the database [Dwork, McSherry, Nissim and Smith 2006].

**Biography:**

Sofya Raskhodnikova is an assistant professor in the Computer Science and Engineering department at Penn State University, USA. She received her PhD from MIT in 2003. Before joining Penn State, she was a postdoctoral researcher at the Hebrew University of Jerusalem and the Weizmann Institute of Science, and a visiting scientist at the Institute for Pure and Applied Mathematics at UCLA.

Sofya's areas of research are randomized algorithms and computational complexity. Her main interest is the design and analysis of sublinear-time algorithms for combinatorial problems. Recently, she also has been working on privacy-preserving methods for publishing aggregate statistical data.



### Ronitt Rubinfeld

MIT, USA

<http://people.csail.mit.edu/ronitt/>

Title 1:

Testing Properties of Distributions: a Survey

Title 2:

Maintaining a Large Matching or a Small Vertex Cover

#### Abstract 1:

We survey several works regarding the complexity of testing global properties of distributions, when given access to only a few samples from the distributions. Such properties might include testing if two distributions have small statistical distance, testing various independence properties, testing whether a distribution has a specific shape (such as monotone decreasing), and approximating the entropy. Classical techniques, such as the Chi-squared test or the straightforward use of Chernoff bounds, have sample complexities that are at least linear in the size of the support of the underlying discrete probability distributions. We will describe bounds for many such testing problems whose sample complexities are sublinear in the size of the support.

#### Abstract 2:

We consider the problem of maintaining a large matching or a small vertex cover in a dynamically changing graph. Each update to the graph is either an edge deletion or an edge insertion. We give the first data structure that simultaneously achieves a constant approximation factor and handles a sequence of  $k$  updates in  $k \cdot \text{polylog}(n)$  time. Previous data structures require a polynomial amount of computation per update. Our techniques are inspired by the sublinear time vertex cover algorithm of [Parnas Ron].

#### Biography:

Ronitt received her PhD from the University of California, Berkeley in 1991, and prior to that graduated from the University of Michigan with a BSE in Electrical and Computer Engineering. She then spent a year as a postdoctoral researcher at Princeton University, followed by a year at Hebrew University in Jerusalem. In 1992, she joined the faculty of the Computer Science Department at Cornell University, where she was an ONR Young Investigator, a Sloan Research Fellow, the 1995 Cornell Association for Computer Science Undergraduates Faculty of the Year, and a recipient of the Cornell College of Engineering Teaching Award. During this time, she also held visiting positions at MIT and IBM Almaden. From 1999 to 2003, Ronitt was a Senior Research Scientist at NEC Research Laboratories. In spring of 2004, she was a Fellow at the Radcliffe Institute for Advanced Study.

Since 2004, she has been on the faculty at MIT, in the Department of Electrical Engineering and Computer Science. In Fall 2008, Ronitt joined the school of Computer Science at Tel Aviv University.



### Michael Saks

Rutgers University, USA  
<http://www.math.rutgers.edu/~saks/>

Title:  
Local Monotonicity Reconstruction

#### Abstract:

We investigate the problem of monotonicity reconstruction, as defined by Ailon, Chazelle, Comandur and Liu (2004) in a localized setting. We have oracle access to a non-negative real-valued function  $f$  defined on the domain  $[n]^d = \{1, \dots, n\}^d$  (where  $d$  is viewed as a constant). We would like to closely approximate  $f$  by a monotone function  $g$ . This should be done by a procedure (a `filter`) that given as input a point  $x \in [n]^d$  outputs the value of  $g(x)$ , and runs in time that is polylogarithmic in  $n$ . The procedure can (indeed must) be randomized, but we require that all of the randomness be specified in advance by a single short random seed. We construct such an implementation where the time and space per query is  $(\log n)^{O(1)}$  and the size of the seed is polynomial in  $\log n$  and  $d$ . Furthermore, with high probability, the ratio of the (Hamming) distance between  $g$  and  $f$  to the minimum possible Hamming distance between a monotone function and  $f$  is bounded above by a function of  $d$  (independent of  $n$ ).

This allows for a local implementation: one can initialize many copies of the filter with the same short random seed, and they can autonomously handle queries, while producing outputs that are consistent with the same approximating function  $g$ .

#### Biography:

Michael Saks is a professor in the Mathematics Department at Rutgers University. His interests range over a number of areas of theory of computing and discrete mathematics. Most recently he's been thinking about lower bounds in concrete computational models (decision trees, communication complexity), polynomial identity testing, exponential algorithms for NP hard problems, and various algorithmic problems related to monotonicity.



## Shubhangi Saraf

MIT, USA

<http://web.mit.edu/shibs/www/>

Title:

Some Recent Results on Local Testing of Sparse Linear Codes

### Abstract:

We study the local testability of linear codes. Our approach is based on a reformulation of this question in the language of tolerant linearity testing under a non-uniform distribution. We then study the question of linearity testing under non-uniform distributions directly, and give a sufficient criterion for linearity to be tolerantly testable under a given distribution. We show that several natural classes of distributions satisfy this criterion (such as product distributions and low Fourier-bias distributions), thus showing that linearity is tolerantly testable under these distributions. This in turn implies that the corresponding codes are locally testable.

For the case of random sparse linear codes, we show the testability and decodability of such codes in the presence of very high noise rates. More precisely, we show that any linear code in  $\mathbb{F}_2^n$  which is:

- \* sparse (i.e., has only  $\text{poly}(n)$  codewords)

- \* unbiased (i.e., each nonzero codeword has Hamming weight in  $(1/2 - n^{-\gamma}, 1/2 + n^{-\gamma})$  for some constant  $\gamma > 0$ ) can be locally tested and locally list decoded from  $(1/2 - \epsilon)$ -fraction errors using only  $\text{poly}(1/\epsilon)$  queries to the received word. This simultaneously simplifies and strengthens a result of Kaufman and Sudan, who gave a local tester and local (unique) decoder for such codes from some constant fraction of errors.

For the case of Dual BCH codes, these algorithms can also be made to run in sub-linear time. We also give sub-exponential time algorithms for list-decoding arbitrary unbiased (but not necessarily sparse) linear codes in the high-error regime.

Joint work with Swastik Kopparty.

### Biography:

Shubhangi is a third year PhD student at MIT, advised by Madhu Sudan. Before this, she did her undergrad in mathematics at MIT. She is interested in problems in computational complexity and pseudorandomness with an algebraic flavor.



### Rocco Servedio

Columbia University, USA  
<http://www.cs.columbia.edu/~rocco/>

Title:  
Testing by Implicit Learning

#### Abstract:

We describe a general approach to testing classes of Boolean functions. The method extends the early observation of Goldreich, Goldwasser and Ron that any proper learning algorithm can be used as a testing algorithm. This observation by itself does not typically give rise to constant-query (independent of  $n$ , the number of input variables) testing algorithms because virtually every interesting class of  $n$ -variable functions requires a superconstant (as a function of  $n$ ) number of examples for proper learning. Our “implicit learning” approach works essentially by running a proper learning algorithm over  $k$ -dimensional examples where  $k$  is a function independent of  $n$ . The learning is “implicit” because the testing algorithm never actually knows which  $k$  of the  $n$  input variables are the ones that are being used for learning; this is accomplished using ingredients from the junta test of Fischer et al.

Our approach can be used to test whether a Boolean function on  $n$  input variables has a “concise representation” in several different senses. Specifically, we obtain property testers that make  $\text{poly}(s/\epsilon)$  queries (independent of  $n$ ) for Boolean function classes such as  $s$ -term DNF formulas (answering a question posed by Parnas et al.), size- $s$  decision trees, size- $s$  Boolean formulas, and size- $s$  Boolean circuits. The method extends to classes of Boolean functions that have sparse Fourier representations, and also to non-Boolean classes such as  $s$ -sparse polynomials, size- $s$  algebraic circuits, and size- $s$  algebraic computation trees over finite fields of bounded size.

While the algorithms obtained by our approach typically have  $\text{poly}(s)$  query complexity, their running time is usually exponential in  $s$  because of a brute-force search that is used to do the learning. We have been able to achieve a better running time of  $\text{poly}(s)$  for the class of  $s$ -sparse  $\text{GF}(2)$  polynomials, using more sophisticated computationally efficient algorithms from learning theory for learning  $s$ -sparse  $\text{GF}(2)$  polynomials.

#### Biography:

Rocco Servedio is an Associate Professor of Computer Science at Columbia University in New York. He received his A.B. in Mathematics and Ph.D. in Computer Science from Harvard, where he studied under Les Valiant, and he was an NSF Mathematical Sciences postdoc at Harvard before joining Columbia.

Rocco’s research interests are centered around computational learning theory and computational complexity. He is interested in the study of Boolean functions and “low-level” computational models such as decision trees, shallow circuits, and low-degree polynomials as a strand connecting learning theory and complexity theory.



## **Asaf Shapira**

Georgia Tech, USA  
<http://www.cs.tau.ac.il/~asafico/>

Title:  
Testing Linear Invariant Properties

### **Abstract:**

Given a set of linear equations  $Mx = b$ , we say that a set of integers  $S$  is  $(M,b)$ -free if it contains no solution to this system of equations. Motivated by questions related to testing linear-invariant properties of boolean functions, as well as recent investigations in additive number theory, the following conjecture was raised (implicitly) by Green and by Bhattacharyya, Chen, Sudan and Xie: we say that a set of integers  $S \subseteq [n]$ , is  $\epsilon$ -far from being  $(M,b)$ -free if one needs to remove at least  $\epsilon n$  elements from  $S$  in order to make it  $(M,b)$ -free. The conjectures above are that for any system of homogenous linear equations  $Mx = 0$  and for any  $\epsilon > 0$  there is a constant time algorithm that can distinguish with high probability between sets of integers that are  $(M,0)$ -free from sets that are  $\epsilon$ -far from being  $(M,0)$ -free. Or in other words, that for any  $M$  there is an efficient testing algorithm for the property of being  $(M,0)$ -free. In this paper we confirm the above conjecture by showing that such a testing algorithm exists even for non-homogenous linear equations. As opposed to most results on testing boolean functions, which rely on algebraic and analytic arguments, our proof relies on results from extremal hypergraph theory, such as the recent hypergraph removal lemmas.

### **Biography:**

Asaf Shapira is an Assistant Professor at the School of Mathematics and the College of Computing at Georgia Institute of Technology. Prior to that he was a post-doc researcher at the Theorem Group of Microsoft Research.



### Christian Sohler

TU Dortmund, Germany  
<https://ls2-www.informatik.uni-dortmund.de/~sohler/>

Title:  
Testing Euclidean Spanners

#### Abstract:

A geometric graph is a graph whose vertices have locations in a Euclidean space  $\mathbb{R}^d$ . The length of an edge  $(p,q)$  in a geometric graph is the Euclidean distance between its end points, i.e.  $\|p-q\|_2$ . A geometric graph  $G=(P,E)$  is called  $(1+\delta)$ -spanner, if for every pair  $(p,q)$  of vertices the shortest path distance in  $G$  is at most  $(1+\delta) \|p-q\|_2$ . Geometric spanners are basic tools in the design of geometric approximation algorithms, for example, to compute approximate Euclidean minimum spanning trees. They are also often used in application areas like mobile and sensor networks. It is known that for constants  $\delta$  and  $d$  Euclidean spanners of linear size exist. We are studying the problem of testing in the bounded degree graph model whether a given graph is a geometric  $(1+\delta)$ -spanner.

(Ongoing work with Frank Hellweg and Melanie Schmidt)

#### Biography:

Christian Sohler studied Computer Science at Saarland University and obtained his Ph.D. from the University of Paderborn.

Since 2009 he is associate professor for complexity theory and efficient algorithms at the Technical University of Dortmund.

His main research areas are randomized algorithms, sublinear time algorithms, streaming algorithms, clustering, and computational geometry.





## **Madhu Sudan**

MIT, USA

<http://people.csail.mit.edu/madhu/>

Title:

Invariance in Property Testing

### **Abstract:**

This is a quick advertisement for a series of works that I have been involved with. Possibly over time my co-authors will include self-contained abstracts of some of the individual works also.

This series of works was triggered by a question/conjecture in a work of Alon, Kaufman, Krivelevich, Litsyn and Ron (AKKLR) who asked if every 2-transitive code with a local constraint was locally testable. On thinking about the question we realized that no one seemed to have explicitly studied the role of invariance of a property when testing it. In retrospect, this property seems to be crucial in (a) defining graph-properties (these are properties that remained unchanged when we renumber the vertices), (b) separating the new (i.e., twentieth century) work in property testing from the classical domain of statistics: Statistics typically deal with properties which enjoy a full symmetry group (names of all participants can be changed and this should not affect the statistics), whereas property testing tries to determine satisfiability of properties which do not enjoy a full symmetry group (e.g., graph properties are not invariant under arbitrary movement of edges), and (c) algebraic properties also have nice (and much smaller) symmetry groups. The AKKLR question/conjecture could be generalized in this sense to asking: When can you take property described by a local forbidden pattern (constraint) and the symmetry group of the property and use them to characterize and test the property? We explored this question in a series of works.

[1] Algebraic Property Testing: The Role of Invariance (with Tali Kaufman, ECCC TR07-111): In this work we considered properties of functions that formed a linear vector space over some field  $F$ , where the domain of the functions were of the form  $K^n$  where  $K$  was a (small) field extending  $F$ , and where the property was invariant under linear transformations of  $K^n$ . We gave necessary and sufficient conditions for such properties to be testable with constant queries (when  $K$  was of constant size). While the motivation for these families were low-degree polynomials, we showed not all properties here were low-degree polynomials and the degree did not characterize the locality of the test.

[2] 2-Transitivity is insufficient for Property Testing (with Elena Grigorescu and Tali Kaufmann, ECCC TR08-033): In this work we used some of the functions explored in paper [1] above, but over large fields  $K$ , to get a counterexample to the AKKLR conjecture (this clearly shows that affine/linear-invariance is not just syntactic variations on polynomials, which were well-understood by AKKLR).

[3] Testing Linear-Invariant Non-Linear Properties (with Arnab Bhattacharyya, Victor Chen, and Ning Xie, ECCC TR08-088): In this work we explored some properties that were not vector spaces (so functions that were not closed under addition), but still linear invariant. This led to a nice bridge between combinatorial property testing and algebraic property testing.

[4] Succinct Representation of Codes with Applications to Testing (with Elena Grigorescu and Tali Kaufmann, ECCC TR09-043): The paper [1] showed that if some properties were characterized by a single local constraint and its rotations under the group of affine transformations, then it was locally testable by the natural test. In this work we showed that many codes, including sparse affine-invariant codes over fields of the form  $2^{\text{prime}}$  have this property.

[5] Limits on the rate of locally testable affine-invariant codes (with Eli Ben-Sasson, unpublished): In this work we show that (despite its richness) affine-invariance is not going to lead to much denser locally testable codes than already known. While the result is disappointing, if one cares about property testing beyond just the construction of locally testable codes, then this results adds to the body of knowledge on algebraic property testing.

Finally let me list a few other results in this direction (though I won't describe them due to lack of time):

- Shapira - STOC 2009
- Kaufman and Wigderson - ICS 2010
- Bhattacharyya, Kopparty, Schoenebeck, Sudan, and Zuckerman - ECCC TR09-086

### **Biography:**

Madhu Sudan recently joined Microsoft Research at their New England Research Center as a Principal Researcher. He is currently on leave from MIT where he was the Fujitsu Professor of EECS. Madhu Sudan got his Bachelor's degree from IIT Delhi in 1987 and his Ph.D. from UC Berkeley in 1992.

From 1992-1997 he was a Research Staff Member at IBM's Thomas J. Watson Research Center. He joined MIT in 1997 where among other roles he was an Associate Director of MIT's CSAIL from 2007-2009.

Madhu Sudan's research lies in the fields of computational complexity theory, algorithms and reliable communication. He is best known for his works on probabilistic checking of proofs, and on the design of list-decoding algorithms for error-correcting codes. His current research interests include semantic communication and property testing.

In 2002, Madhu Sudan was awarded the Nevanlinna Prize, for outstanding contributions to the mathematics of computer science, at the International Congress of Mathematicians in Beijing.



## General Information

### Name Badges

For identification purposes, badges are expected to be worn at all times during the conference. The badges are color-coded as follows: Participant-ORANGE, Audience-BLUE, Staff-PURPLE

### Registration Desk and Conference Secretariat

Jan. 7th: Registration desk is located at Wenjin Hotel. Open from 14:00-17:00.

Jan. 8th: Registration desk is located in Room 1-208, FIT Building. Open from 08:30-09:00.

Jan. 8th-10th: The secretariat is located in Room 1-208, FIT Building. Open from 08:00-20:00.

The reimbursement desk is also located in Room 1-208, FIT Building.

### Dining

You are expected to show your meal coupons at the entrance to the restaurant. The coupons vary in color with the dinner.

### Coffee Break

Time: 10:15-10:45, 15:30-16:00

Place: Lounge outside Room 1-315

### Charges

The Institute will cover accommodation fees for the nights of Jan. 7th-10th, 2010. Participants are responsible for additional charges, such as mini-bar, laundry, and phone charges. You may consult the detailed charge information on the guideline in your room.

### Electricity

Voltage is 220V in China.

### Transportation

#### Shuttle Bus:

Shuttle bus services (Wenjin Hotel - FIT Building) are available during the conference. The shuttle bus carries a sign with the conference name and ITCS Logo for identification. The schedule is as follows:

Jan. 08, 2010	08:45	Departs at Wenjin Hotel
Jan. 08, 2010	12:00	Departs at FIT Building
Jan. 08, 2010	13:45	Departs at Wenjin Hotel
Jan. 08, 2010	17:00	Departs at FIT Building
Jan. 09, 2010	08:45	Departs at Wenjin Hotel
Jan. 09, 2010	12:00	Departs at FIT Building
Jan. 09, 2010	13:45	Departs at Wenjin Hotel
Jan. 09, 2010	17:00	Departs at FIT Building
Jan. 10, 2010	08:45	Departs at Wenjin Hotel
Jan. 10, 2010	12:00	Departs at FIT Building
Jan. 10, 2010	13:45	Departs at Wenjin Hotel
Jan. 10, 2010	17:00	Departs at FIT Building

#### Taxi:

The price of a taxi is ¥2/kilometer with an initial price of ¥10. An additional fuel fee of ¥1 will be charged if the distance exceeds 3 kilometers. The charge would be 20% higher after 15 kilometers or during the night time (11p.m - 5a.m). Please pay according to the mile meter. Please ask for a receipt from your taxi driver in case you accidentally leave something in the car.

### Airport

It is advisable that you arrive at the airport three hours in advance for international flights and two hours in advance for domestic flights.

### Currency & Exchange

Most currencies and travelers check can be exchanged into Chinese RMB at major banks, including the Bank of China. The exchange rate in China is maintained by the government and should be the same at both hotels and banks.

Major credit cards such as Master Card, Visa, JCB, Diners and American Express can be used to pay for hotel rooms, purchasing goods in large shopping centers, and for meals in some restaurants, however, they are not accepted at many small-scale shops and restaurants.

### Tips & Tax

In Beijing, tipping is not commonly practiced and is considered unnecessary. Taxes are included in the stated prices.

### Phone Call in the Hotel

The country code for China is 86, while the regional code for Beijing is 10.

Local calls: dial the prefix "0"  
Domestic Long Distance Calls: dial the prefix "00"  
International Calls: dial the prefix "000"

### Weather

The climate in Beijing is of the continental type, with cold winters and hot summers. During the winter, the weather is always chilly, with January and February being the coldest and driest months. Normally in January, the average high temperature is 1°C, and the average low temperature is -6°C.

Day	Description	Temp.	Wind Speed/Dir.
Jan. 05	A full day of sunshine	-6~4°C	5mph / NW
Jan. 06	Partly sunny	-7~1°C	6mph / WNW
Jan. 07	Colder with clouds and sun	-6~-3°C	14mph / NW
Jan. 08	Sunny and cold	-7~-3°C	13mph / NW
Jan. 09	Sunny and cold	-10~-3°C	5mph / NW
Jan. 10	Sunny and warmer	-8~4°C	2mph / WSW

### Internet

Free internet is available in your room. Internet service is also provided in Room 1-315 at FIT Building among sessions for occasional research and email access.

Wireless Network Configuration for Mini-workshop

SSID: ITCS

WPA Enabled

KEY: tsinghua2010

### Equipment

We will provide laptops with Windows and Mac system, together with remoter and laser pointer. Also, there are two laptops provided in Room 1-315 for temporary use. Printers, scanners, and photocopiers are available in Room 1-208, FIT Building.

### Flight Reconfirmation

Departure air tickets should be reconfirmed 72 hours in advance if needed. You may call the airline to reconfirm your ticket. Please be aware that airline offices do not open on the weekend.

### Emergency Contacts

Ambulance 120

Police 110

For real emergencies only

### Contact us

If you have any questions, please contact us:

*Yuying Chang (Workshop Secretary, Foreign Affairs)*

13681245496 | 62782765 | 62781693 ext.1285

*Yanping Wang (Foreign Affairs)*

13581954903 | 62782373 | 62781693 ext.1289

*Xiang Li (Technical Support)*

15810000156 | 62794954 | 62781693 ext.1287

*Changxia Liu (Workshop Administration Affairs)*

13269635256 | 62794954 | 62781693 ext.1286

## Principal Airline Office

Air Code	Airline	Telephone	Reconfirmation
AC	Air Canada	6468 2001	Not needed
AF	Air France	400 880 8808	Not needed
AY	Finnair	6512 7180	Not needed
BA	British Airways	8511 5599	
BR	EVA Air	6563 5000	Not needed
CA	Air China	400 810 0999	
CI	China Airlines	6510 2671	
CO	Continental	8527 6686	
CX	Cathay Pacific	8486 8532	Not needed
CZ	China Southern	950333	
FM	Shanghai Airlines	6456 9018	Not needed
JL	Japan Airlines	6513 0888	
KA	Dragon Air	6518 2533	Not needed
KE	Korean Air	400 658 8888	
KL	KLM	6505 3505	
LH	Lufthansa	6468 8838	Not needed
LY	Israel Airline	6597 3388-2906	Not needed
MU	China Eastern	951081	
NH	All Nippon Airways	6590 9191	
NW	Northwest Airlines	6505 3505	Not needed
OS	Austrian Airlines	6462 2161	Not needed
OM	MIAT Mongolian Airlines	6507 7397	Not needed
OZ	Asiana Airlines	6468 4000	Not needed
PK	Pakistan International	6505 1681	
QF	Qantas	6467 4794-3337	
SK	SAS	8527 6100	Not needed
SQ	Singapore Airlines	6505 2233	Not needed
SU	Aeroflot-Russian	6500 2412	
TG	Thai International	8515 0088	Not needed
TK	Turkish Airlines	6465 1867	
UA	United Airlines	6463 1111	Not needed

## Principal Embassy

Country	Telephone	Country	Telephone
Australia	6532 1724	Oman	6532 3692
Belgium	6532 2104	Laos	6532 1224
Bengal	6532 2521	Japan	6532 2361
Bulgaria	6532 1916	Korea	6505 2608
Chile	6532 1591	Poland	6532 1235
Egypt	6532 1825	Pakistan	6532 2504
Finland	8529 8541	Portugal	6532 3497
France	6532 1331	Russian	6532 2051
Germany	6532 5560	Singapore	6532 3926
Holland	6532 1131	Sri Lanka	6532 1861
Hungary	6532 1431	Spain	6532 1986
India	6532 1856	Sweden	6532 3331
Indonesia	6532 5487	Switzerland	6532 2736
Iran	6532 2040	Syria	6532 1372
Israel	6505 2970	Thailand	6532 1903
Italy	6532 2131	Turkey	6532 2650
Malaysia	6532 2531	UK	6532 1961
Mongolia	6532 1203	USA	6532 3831
Myanmar	6532 1624	Vietnam	6532 1155
New Zealand	6532 2731		