ACAC 2012

7th Athens Colloquium on Algorithms and Complexity
August 27-28, University of Athens, Greece

– *Abstracts* –

- **Mihalis Yannakakis**, Columbia University
  Computation of Least Fixed Points
  Many problems from different areas can be formulated as problems of computing a fixed point of a suitable function. For many of these problems, the function in the fixed point formulation is monotone, and the objects we want to compute are given by a specific fixed point, namely the least fixed point of the function. Many models and problems from a broad variety of areas can be thus expressed as least fixed point computation problems, including in particular the analysis of various probabilistic models, problems in stochastic optimization, and games. It turns out that for some classes of functions we can compute the least fixed point in polynomial time and thus we can analyze efficiently several of these models, while for others there are strong indications that they cannot be solved in polynomial time, and for yet others the question remains open. In this talk we will discuss progress in this area. The talk is based on a series of works with Kousha Etessami and Alistair Stewart.

- **Spyros Kontogiannis**, University of Ioannina
  Computation of Nash Equilibria in Bimatrix Games
  In this talk we shall explore the computability of Nash equilibria in bimatrix games, i.e., non-cooperative normal-form games with two players whose payoff functions are described by their payoff matrices. We shall demonstrate fundamental properties of these games, as well as various formulations for the problem 2NASH of constructing at least one Nash equilibrium (NE) point of the game. We shall also demonstrate the algorithm of Lemke and Howson, one of the the most characteristic algorithms for solving 2NASH. Due to the apparent (PPAD) hardness of 2NASH, we shall then explore two distinct lines of attack: The first is the determination of broad subclasses of games for which 2NASH is polynomial-time tractable, and the second is the provision of polynomial-time approximation algorithms for 2NASH, for various notion of NE approximations.

- **Orestis Telelis**, University of Liverpool
  Uniform Price Auctions: Equilibria and Efficiency
  We present our results on Uniform Price Auctions, one of the standard sealed-bid multi-unit auction formats, for selling multiple identical units of a single good to multi-demand bidders. Contrary to the truthful and economically efficient multi-unit Vickrey auction, the Uniform Price Auction encourages strategic bidding and is socially inefficient in general, partly because of a D̈emand Reductionëffect; bidders tend to bid for fewer (identical) units, so as to receive them at a lower uniform price. Despite its inefficiency, the uniform pricing rule is widely popular by its appeal to the intuitive anticipation, that identical items should be identically priced. Application domains of its variants include sales of U.S. Treasury notes to investors, trade exchanges over the internet facilitated by popular online brokers, allocation of radio spectrum licenses etc. In this work we study equilibria of the Uniform Price Auction in undominated strategies. In particular, we provide results regarding efficient computation of undominated pure Nash equilibria, and quantify the social inefficiency of pure and (mixed) Bayes-Nash equilibria by means of bounds on the Price of Anarchy.

  This is a joint work with Evangelos Markakis.

- **Angelina Vidali**, University of Vienna
  Characterizations of truthful mechanisms

  TBA

- **Dimitris Paparas**, Columbia University
  The Complexity of finding an Arrow-Debreu Market equilibrium for CES and other types of Markets
  We show that the long-open problem of finding an Arrow-Debreu Market Equilibrium with CES utilities is PPAD-hard when the Constant Elasticity of Substitution parameter, ρ, is any constant less than -1. We then generalize our proof to show PPAD-hardness for all types of Markets with the property that there is an instance of them for which increasing the price of one good i and keeping the prices of the rest of the goods unchanged results in increased demand for good i.

  Joint work with Xi Chen and Mihalis Yannakakis.

- **George Christodoulou**, University of Liverpool
  Coordination Mechanisms for Selfish Routing
  We reconsider the well-studied Selfish Routing game with affine latency functions. The Price of Anarchy for this class of games takes maximum value 4/3; this maximum is attained already for a simple network of two parallel links, known as Pigou's network. We improve upon the value 4/3 by means of Coordination Mechanisms.

- **Euripides Markou**, University of Central Greece
  Online Graph Exploration with Advice
  We study the problem of exploring an unknown undirected graph with non-negative edge weights. Starting at a distinguished initial vertex s, an agent must visit every vertex of the graph and return to s. Upon visiting a node, the agent learns all incident edges, their weights and endpoints. The goal is to find a tour with minimal cost of traversed edges. This variant of the exploration problem has been introduced by Kalyanasundaram and Pruhs in 1994 and is known as a 'fixed graph scenario'. There have been recent advances by Megow, Mehlhorn, and Schweitzer in 2011, however the main question whether there exists a deterministic algorithm with constant competitive ratio (w.r.t. to offline algorithm knowing the graph) working on all graphs and with arbitrary edge weights remains open. In this paper we study this problem in the context of ádvice complexity; investigating the tradeoff between the amount of advice available to the deterministic agent, and the quality of the solution. We show that $\Omega(n \log n)$ bits of advice are necessary to achieve a competitive ratio of 1 (w.r.t. an optimal algorithm knowing the graph topology). Furthermore, we give a deterministic algorithm which uses $O(n)$ bits of advice and achieves a constant competitive ratio on any graph with arbitrary weights. Finally, going back to the original problem, we prove a lower bound of $5/2 - \epsilon$ for deterministic algorithms working with no advice, improving the best previous lower bound of $2 - \epsilon$ of Miyazaki, Morimoto, and Okabe from 2009. In this case, significantly more elaborate technique was needed to achieve the result.

- **Panagiotis Cheilaris**, Università della Svizzera italiana
  Conflict-free coloring with respect to a subset of intervals
  Given a hypergraph $H = (V, E)$, a coloring of its vertices is said to be conflict-free if for every hyperedge $S \in E$ there is at least one vertex in S whose color is distinct from the colors of all other vertices in S. The discrete interval hypergraph Hn is the hypergraph with vertex set $1, ..., n$ and hyperedge set the family of all subsets of consecutive integers in $1, ..., n$. We provide a polynomial time algorithm for conflict-free coloring any subhypergraph of Hn, we show that the algorithm has approximation ratio 2, and we prove that our analysis is tight, i.e., there is a subhypergraph for which the algorithm computes a solution which uses twice the number of colors of the optimal solution. We also show that the problem of deciding whether a given subhypergraph of Hn can be colored with at most k colors has a quasipolynomial time algorithm.

- **Tobias Müller**, Utrecht University
  First order logic and random geometric graph
  We say that a graph property is first order expressible if it can be written as a logic sentence using universal and existential quantifiers with variables ranging over the nodes of the graph, the usual

connectives AND, OR, NOT, parentheses and the relations = and , where x y means that x and y share an edge. For example, the property that G contains a triangle can be written as

Exists x,y,z : (x y) AND (x z) AND (y z).

Starting from the sixties, first order expressible properties have been studied extensively on random graphs. For the most commonly studied model of random graphs, the Erdos-Renyi model, a number of very attractive and surprising results have been obtained, and by now we have a fairly full description of the behaviour of first order expressible properties on this model.

The Gilbert model of random graphs is obtained as follows. We take n points uniformly at random from the d-dimensional unit torus, and join two points by an edge if and only their distance is at most r.

In this talk I will discuss joint work with S. Haber which tells a nearly complete story on first order expressible properties of the Gilbert random graph model. In particular we settle conjectures of McColm and of Agarwal-Spencer.

(Joint with S. Haber.)

- **Ilias Kotsireas**, Wilfrid Laurier University
  Complementary Sequences: Theory, Search Methods and Applications
  Complementary sequences are defined via the periodic and aperiodic autocorrelation functions associated to a finite sequence. We will present some of the theory developed for such sequences, including some new theoretical advances. We will also present various search methods that have been employed to search for complementary sequences of various kinds. Such methods include cyclotomy-based algorithms, string sorting algorithms, and metaheuristic algorithms. We shall mention some applications of complementary sequences in Coding Theory, Telecommunications and other areas.

- **Aris Anagnostopoulos**, Sapienza University of Rome
  Models and Algorithms for Online Collaborative Systems
  In the last years we have observed the emergence of a variety of systems where users communicate and collaborate online and produce knowledge or provide new services. Success stories include Wikipedia, Linux and the open source community, games with a purpose, crowdsourcing services, online labor marketpalaces, and car-sharing services, to name a few. This new paradigm, where users collaborate using the Internet for coordination, requires the development of new models and algorithms to capture both the machine and the human elements, and the interactions between them.

  In this talk I will start with a high-level presentation of some of these systems and with some of the issues needed to be captured when trying to formally model them. I will then proceed with the presentation of algorithms for the problem of creating online teams of experts, and for the problem of assigning tasks to experts in some crowdsourcing systems. I will conclude with a discussion of challenges for future work.

- **Paul Spirakis**, University of Patras
  Dynamic Networks Foundations
  We study the propagation of influence and distributed computation in the novel area of worst-case dynamic networks. We focus on a synchronous message passing communication model with bidirectional links. Message transmission is usually broadcast but in one case we also allow nodes to transmit a different message to each one of their neighbors. We consider both the cases of availability of unique identities and of anonymous nodes. In these networks, communication links are allowed to change arbitrarily from round to round. The main difficulties arise from the fact that the network modifications are not controlled by the computational nodes themselves but rather are dictated by an adversary scheduler. We first discuss the most common assumption that requires the network to be connected at every instant. This is a natural restriction on the adversarial schedule that can be implemented by distributed connectivity services. We then show how to drop this restriction. In particular, we present some useful metrics for capturing the propagation of influence in networks that are possibly disconnected at every instant and we also give several results that correlate these metrics. We also exhibit a nontrivial case of dynamic networks with always disconnected instances in which information spreads as fast as in those with always connected instances. Further, we investigate termination criteria by providing to the nodes some minimal knowledge on the influence

propagation time. Such knowledge is most of the time some explicit or implicit upper bound on the time it takes for the state of a node to influence another node. We exploit our termination criteria to provide efficient protocols (provably optimal in several cases) that solve the fundamental counting, naming, and all-to-all token dissemination (a.k.a. gossip) problems.

This work is joint with O. Michail and I. Chatzigiannakis.

- **Iordanis Kerenidis**, CNRS-Univ Paris Diderot
  Lower bounds on Information Complexity via zero-communication protocols
  We show that almost all known lower bound methods for communication complexity are also lower bounds for the information complexity. In particular, we define a relaxed version of the partition bound of Jain and Klauck and prove that it lower bounds the information complexity of any function. Our relaxed partition bound subsumes all norm based methods (e.g. the $\gamma 2$ method) and rectangle-based methods (e.g. the rectangle/corruption bound, the smooth rectangle bound, and the discrepancy bound), except the partition bound.

  Our result uses a new connection between rectangles and zero-communication protocols where the players can either output a value or abort. We prove the following compression lemma: given a protocol for a function f with information complexity I, one can construct a zero-communication protocol that has non-abort probability at least $2^{-O(I)}$ and that computes f correctly with high probability conditioned on not aborting. Then, we show how such a zero-communication protocol relates to the relaxed partition bound. We use our main theorem to resolve three of the open questions raised by Braverman. First, we show that the information complexity of the Vector in Subspace Problem is $\Omega(n^{1/3})$, which, in turn, implies that there exists an exponential separation between quantum communication complexity and classical information complexity. Moreover, we provide an $\Omega(n)$ lower bound on the information complexity of the Gap Hamming Distance Problem.

  To appear at FOCS 2012.

- **Vissarion Fisikopoulos**, University of Athens
  Computing the volume of the discriminant polytope
  The discriminant polynomial is a fundamental object in mathematics and engineering. The Newton polytope of a polynomial generalizes the notion of its degree. In this work in progress, we study algorithms for the volume of the Newton polytope of the discriminant, called discriminant polytope. The problem of computing the volume of a polytope is know to be ♯P-hard. Thus, our goal is a polynomial time randomized algorithm that approximates the volume of the discriminant polytope. To this end, we utilize results from randomized algorithms and combinatorial optimization.

- **George Tzoumas**, LE2I - Université de Bourgogne
  A New Representation for Geometric Sets
  We present a new representation for geometric sets and an application of this representation. Consider a geometric set described by a system of inequalities. By introducing auxiliary variables within appropriate intervals, one is able to describe the set as the zeros of an underconstrained system, corresponding to an equivalent optimization problem. This way we can represent not only boolean operations of CSG primitives (union, intersection, complement) but also more complicated sets such as Minkowski sums, projections and sweeps or extrusions. The algebraic system is solved by interval arithmetic. We show how the interval solver can be tuned for this particular application and how existing algorithms for topology computation can benefit from the new representation, allowing them to deal with more types of sets.

- **Loukas Georgiadis**, University of Ioannina
  Finding Dominators in Interprocedural Flowgraphs
  The computation of dominators in a flowgraph has applications in diverse areas including program optimization and code generation, constraint programming, circuit testing, and theoretical biology. Efficient algorithms for this problem operate in the intraprocedural case where all flowgraph paths are valid. In the interprocedural case, which appears in the setting of whole-program analysis and optimization, however, there are path constraints that have to be taken into account. As a result, the most efficient algorithms for computing dominators cannot handle the interprocedural case. Unlike the intraprocedural dominators problem, the transitive reduction of the interprocedural dominance relation is not a tree but a directed acyclic graph. Previously known algorithms compute the

complete interprocedural dominance relation in $O(mn)$ time and $O(n^2)$ space for a flowgraph with n vertices and m edges. Here we present an algorithm that computes an implicit representation of interprocedural dominance in $O(m\lambda + \lambda^{\omega})$ time and $O(n\lambda)$ space, where λ is the number of procedures, and ω is the matrix multiplication exponent. Using this representation we can list the set of dominators $Dom(v)$ of any vertex v in $O(|Dom(v)|)$ time and test if u dominates v in constant time, for any pair of query vertices u and v.

- **Konstantinos Draziotis**, Aristotle University of Thessaloniki
  Integer solutions of diophanine linear equation under constraints
  We use lattice based methods in order to get an integer solution of the linear equation $a_1x_1 + \cdots + a_nx_n = a_0$, which satisfies the bound constraints $|x_j| < X_j$ under certain conditions.

- **Elias Tsigaridas**, INRIA
  Univariate real root isolation in an extension field
  Computing the real roots of a univariate polynomial is probably the single most important problem in computational mathematics. We present algorithmic and complexity results for the problem of isolating the real roots of a univariate polynomial, the coefficients of which belong to a simple algebraic extension of the rational numbers.

- **Aggelos Kiayias**,University of Athens
  Cryptography research : directions and challenges
  Modern cryptography combines the best parts of a diverse set of areas in computer science and mathematics that include number theory, computational complexity, and probability theory with the objective to study, in a complete and sound basis, the security of computer systems. In the last 36 years, since the seminal paper of Diffie and Hellman, cryptography has matured and rapidly expanded from its traditional objectives of encryption and signatures to consider a variety of problems of trust in the two-party and multiparty setting. In this talk, I will give an overview of the area aimed at beginning graduate students, introduce some of the main current trends and point to directions for future research.

- **Dimitrios Poulakis**, Aristotle University of Thessaloniki
  A digital signature scheme for long-term security
  Many applications of the digital signatures, such as the signatures of health cards, contracts etc, need long-term cryptographic security. Todayś digital signatures guarantee only short-term security. To remedy this, the use of more than one independent signature schemes has been suggested. Thus, if one of them is broken, then it will be replaced by a new secure one and the document will be re-signed. Therefore, it is more efficient for applications requiring long-term security to use digital signatures whose their security is based on two intractable problems, so if any of the underlying problems is broken, the other will still be valid and hence the signature will be protected. In this talk we present a signature scheme based on the integer factorization problem and on the discrete logarithm problem on a supersingular elliptic curve. Note that these two problems have similar resistance to attack, thus they can coexist within the same protocol. The use of a super-singular elliptic curve allows us to easily build a pairing that we use to verify the signature. Furthermore, we explain how to implement in practice all the basic functions we need for the establishment and operation of this system.

- **Anna Pappa**, Telecom ParisTech
  Practical Aspects of Quantum Coin Flipping
  Coin Flipping is an important primitive in two-party computation, since it provides the involved parties with trusted shared randomness. In this work we investigate what happens in the quantum case, when an adversary is bounded by his resources (noisy or bounded storage) or by his computational power (inefficiency in inverting a 1-way function) and when he is unbounded. The importance of the proposed protocol is that it is significantly easier to implement that the previously available protocols and can be demonstrated using currently available commercial products.

- **Nikolaos Fytas**, Complutense University of Madrid
  Linking physics and algorithms in the three-dimensional random-field Ising
  For many years now, it is well-known that there exists a fundamental connection between the concepts of statistical physics and the algorithms used to simulate disordered magnetic systems:

the mathematics of graphs. In this talk I will describe an efficient implementation of the push-relabel algorithm to investigate the ground-state properties of a prototypical glassy model: the three-dimensional Ising model under the presence of a Gaussian-distributed random-field. Results concerning the zero-temperature phase transition of the model will be given together with a discussion on the connection of the auxiliary fields of the push-relabel algorithm and the characteristics of the transition.

- **Vangelis Paschos**, Université Paris-Dauphine, LAMSADE
  Beyond polynomial approximation. Moderately exponential, subexponential and parameterized approximability.
  The talk surveys main results and techniques for three recent research issues that aim at compensating polynomial inapproximability. The issues surveyed are the moderately exponential and subexponential approximation, whose goal is the design of approximation algorithms running in moderately exponential or subexponential time and achieving approximation ratios unachievable in polynomial time, and the parameterized approximation whose goal is the design of fixed parameter algorithms, also achieving approximation ratios impossible to achieve in polynomial time.