Program

Tuesday November 26, 2019

8:30 - 9:00 *Gathering, Registration and Coffee*

9:00 - 9:15 **Opening Remarks**

9:15 - 9:55 **Nikhil Bansal -** *On a generalization of iterated and randomized rounding*

I will describe a new method for rounding linear programs that combines the commonly used iterated rounding and randomized rounding techniques. In particular, we show that whenever iterated rounding can be applied to a problem with some slack, there is a randomized procedure that returns an integral solution that satisfies the guarantees of iterated rounding and also has concentration properties. We use this to give new results for several classic problems such as makespan minimization on unrelated machines, degree-bounded spanning trees and rounding column-sparse LPs.

9:55 - 10:25 **Noam Touitou -** *General Framework for Metric Optimization Problems with Delay or with Deadlines*

We present a framework used to construct and analyze algorithms for online optimization problems with deadlines or with delay over a metric space. Using this framework, we present algorithms for several different problems. We present an $O(D^2)$-competitive deterministic algorithm for online multilevel aggregation with delay on a tree of depth D, an exponential improvement over the $O(D^4 2^D)$-competitive algorithm of Bienkowski et al. (ESA '16), where the only previously-known improvement was for the special case of deadlines by Buchbinder et al. (SODA '17). We also present an $O(\log^2 n)$-competitive randomized algorithm for online service with delay over any general metric space of n points, improving upon the $O(\log^4 n)$-competitive algorithm by Azar et al. (STOC '17). In addition, we present the problem of online facility location with deadlines. In this problem, requests arrive over time in a metric space, and need to be served until their deadlines by facilities that are opened momentarily for some cost. We also consider the problem of facility location with delay, in which the deadlines are replaced with arbitrary delay functions. For those problems, we present $O(\log^2 n)$-competitive algorithms, with n the number of points in the metric space. The algorithmic framework we present includes techniques for the design of algorithms as well as techniques for their analysis.

10:25 - 10:55 **Yaniv Sadeh -** *Optimal Representations of a Traffic Distribution in Switch Memories*

Traffic splitting is a required functionality in networks, for example for load balancing over multiple paths or among different servers. The capacity of each server or path implies the distribution by which traffic should be split. A recent approach implements traffic splitting within the ternary content addressable memory (TCAM), which is often available in switches. It is important to reduce the amount of memory allocated for this task since TCAMs are power hungry and are often also required for other tasks such as classification and routing. For splitting a universe of 2^W addresses into k pieces of particular sizes, we give a simple algorithm that computes an optimal representation in $\tilde{O}(Wk)$ time. Furthermore, we prove that a recently published load balancer, called Niagara, which also runs in $\tilde{O}(Wk)$ time is in fact optimal. That is, both our algorithm and Niagara produce the smallest possible TCAM that splits the traffic exactly to the required pieces, where the only previously known

algorithm for computing optimal exact representation has running time exponential in k. Finally, we rely on our optimal $\tilde{O}(Wk)$ runtime algorithm to investigate through extensive experiments the amount of TCAM memory required to represent traffic splitting in typical scenarios.

10:55 - 11:20 *Coffee break*

11:20 - 11:50 **Benny Applebaum -** *The Round Complexity of Perfectly-Secure Multiparty Computation*

We study the round complexity of general secure multiparty computation (MPC) in the classical information-thoretic model of Ben-Or, Goldwasser, and Wigderson [BGW88]. That is, we strive for perfect, information-theoretic and error-free, security against any coalition of at most t computationally-unbounded corrupted parties. Classical feasibility results show that this is possible for any t<n/2 in the passive setting, when the parties follow the protocol, and up to t<n/3 in the active (aka Byzantine) setting when the parties may deviate from the protocol.

I will survey a recent line of works that settles the round complexity of perfect-MPC with optimal security threshold for general functions. In particular, we show that 2 rounds are sufficient and necessary in the passive setting and 4 rounds are sufficient and necessary in the active setting.

Based on joint works with Zvika Brakerski, Eliran Kachlon, Arpita Ptra, and Rotem Tsabary.

11:50 - 12:20 **Geoffroy Couteau -** *Efficient Pseudorandom Correlation Generators: Silent OT Extension and More*

I will present recent developments in secure computation in the preprocessing model. In this model, a protocol is divided in two phases: a preprocessing phase, independent of the inputs, during which long correlated strings are generated and distributed among the parties; and a lightweight online phase, were the actual computation takes place. The generation of the preprocessing material forms the main efficiency bottleneck of all modern secure computation protocols, due to the very large communication, computation, and storage involved.

In this talk, I will discuss how a new cryptographic primitive, a pseudorandom correlation generator (PCG), can be used to considerably improve this state of affair. Informally, a PCG allows to stretch short, correlated keys into long correlated pseudorandom string of near-arbitrary length. This allows the preprocessing phase of all secure computation protocols to be executed with a tiny amound of communication (to generate the short correlated keys) followed only by local operations (to stretch correlated strings from these keys). I will discuss how to formalize this primitive, and describe a way to construct PCGs for an important class of correlations from the hardness of syndrome decoding. In turns, this results in considerable improvements for state-of-the-art secure computation, both from an asymptotic point of view and in practice.

12:20 - 12:50 **Noam Mazor -** *Channels of Small Log-Ratio Leakage and Characterization of Two-Party Differentially Private Computation.*

Consider a PPT two-party protocol $\Pi = (A, B)$ in which the parties get no private inputs and obtain outputs $O_A, O_B \in \{0, 1\}$, and let V_A and V_B denote the parties' individual views. Protocol π has α-*agreement* if $\Pr[O_A = O_B] = 1/2 + \alpha$. The *leakage* of π is the amount of information a party obtains about the event $\{O_A = O_B\}$; that is, the *leakage* ϵ is the maximum, over $P \in \{A, B\}$, of the distance between $V^P|_{O_A=O_B}$ and $V^P|_{O_A\neq O_B}$. Typically, this distance is measured in *statistical distance*, or, in the computational setting, in *computational indistinguishability*. For this choice, Wullschleger [TCC '09] showed that if $\epsilon \ll \alpha$ then the protocol can be transformed into an OT protocol.

We consider measuring the protocol leakage by the *log-ratio distance* (which was popularized by its use in the differential privacy framework). The log-ratio distance between X, Y over domain Ω is the minimal $\epsilon \geq 0$ for which, for every $v \in \Omega$, $\log \frac{\Pr[X=v]}{\Pr[Y=v]} \in [-\epsilon, \epsilon]$. In the computational setting, we use computational indistinguishability from having log-ratio distance ϵ. We show that a protocol with (noticeable) accuracy $\alpha \in \Omega(\epsilon^2)$ can be transformed into an OT protocol (note that this allows $\epsilon \gg \alpha$). We complete the picture, in this respect, showing that a protocol with $\alpha \in o(\epsilon^2)$ does not necessarily imply OT. Our results hold for both the information theoretic and the computational settings, and can be viewed as a "fine grained" approach to "weak OT amplification".

We then use the above result to *fully* characterize the complexity of differentially private two-party computation for the XOR function, answering the open question put by Goyal, Khurana, Mironov, Pandey and Sahai [ICALP '16] and Haitner, Omri, Shaltiel and Silbak [FOCS '18]. Specifically, we show that for any (noticeable) $\alpha \in \Omega(\epsilon^2)$, a two-party protocol that computes the XOR function with α-accuracy and ϵ-differential privacy can be transformed into an OT protocol. This improves upon Goyal et al. that only handle $\alpha \in \Omega(\epsilon)$, and upon Haitner et al. who showed that such a protocol implies (infinitely-often) key agreement (and not OT). Our characterization is tight since OT does not follow from protocols in which $\alpha \in o(\epsilon^2)$, and extends to functions (over many bits) that "contain" an "embedded copy" of the XOR function.

Joint work with Iftach Haitner, Ronen Shaltiel and Jad Silbak.

12:50 - 14:20 *Lunch* (Please see our list for a selection of restaurants.)

14:20 - 14:50 **Liran Carmel -** *Using ancient DNA methylation to understand human evolution*

Whereas genome sequences are available for many archaic humans and ancient H. sapiens, they provide limited information on gene expression and regulation. I will show how pre-mortem patterns of DNA methylation in ancient genomes can be reconstructed. These DNA methylation patterns provide ample information on gene activity patterns, which allows the detection of differentially expressed genes across human lineages. I will show how we use this information to infer about the anatomy of archaic humans and anatomical adaptations in modern humans.

14:50 - 15:20 **Elhanan Borenstein -** *Systems biology of the human microbiome: From big data to models*

The human microbiome – the diverse ensemble of microorganisms that populate the human body – represents a vastly complex ecosystem that is tightly linked to our health. Multiple molecular assays now enable high-throughput profiling of this system, providing large-scale and comprehensive characterization of its ecology, functional capacity, and metabolic activity. To date, however, analyses of such multi-omic data typically focus on statistical associations, often ignoring extensive prior knowledge of the mechanisms, dependencies, and regularities linking these various facets of the microbiome. In this talk, I will highlight the pressing need for the development of predictive systems-level models of the microbiome and of model-based computational methods for integrating and analyzing microbiome multi-omic data. I will further introduce several novel computational frameworks for linking taxonomic, genomic, metagenomic, and metabolomic information about the microbiome. Combined, such frameworks lead to an improved comprehensive, multi-scale, and mechanistic understanding of the microbiome in health and disease, informing efforts for personalized microbiome-based therapy.

15:20 - 15:50 **Russ Harmer -** *Graph-based knowledge representation for cellular signalling*

A mathematical theory is presented for the representation of knowledge in the form of a directed acyclic hierarchy of objects in a category. The conditions under which knowledge update, in the form of the sesqui-pushout rewriting of an object, can be propagated to the rest of the hierarchy are analysed: some rewrites must be propagated in the direction of the arrows, while others must be propagated against the direction of the arrows.

This framework is instantiated into the concrete setting of directed graphs with attributes to build a knowledge representation system for protein-protein interactions in cellular signalling from which executable models, in the Kappa language, can be extracted automatically. The current state of the ongoing development of the KAMI bio-curation tool, based on this approach, is outlined along with our plans for future development.

16:00 - 16:30 *Coffee break*

16:30 - 17:00 **Amos Korman -** *Ant Navigation in Percolated Environments: A Locality Perspective*

Locality is a fundamental notion in the study of algorithms. Whereas locality has been studied extensively in computer science, it has been treated mostly implicitly in biological contexts. Here we study how crazy ants manage to effectively navigate as a group in percolated mazes, by collectively extending their sensing range. Interestingly, while the locality of the ants' algorithm is rather small, this nevertheless leads to a considerable improvement in the traversal length. To theoretically explain this phenomenon, we use percolation theory to show that below the percolation threshold, a sensing range that is logarithmic in system size suffices for extremely fast traversal, while above the threshold, large locality will not help, since there is no solution anyways.

17:00 - 17:30 **Shiri Chechik -** *TBA*

17:30 - 18:00 **Pierre Fraigniaud -** *Present-Biased Optimization*

This work explores the behavior of present-biased agents, that is, agents who erroneously anticipate the costs of future actions compared to their real costs. Specifically, the paper extends the original framework proposed by Akerlof (1991) for studying various aspects of human behavior related to time-inconsistent planning, including procrastination, and abandonment, as well as the elegant graph-theoretic model encapsulating this framework recently proposed by Kleinberg and Oren (2014). The benefit of this extension is twofold. First, it enables to perform fine grained analysis of the behavior of present-biased agents depending on the optimisation task they have to perform. We study covering tasks vs. hitting tasks, and show that the maximum ratio between the cost of the solutions computed by present-biased agents and the cost of the optimal solutions differ significantly for the two tasks. Second, our extension enables to study not only underestimation of future costs, coupled with minimisation problems, but also all combinations of minimization/maximization, and underestimation/overestimation. We study the four scenarios, and we establish upper bounds on the cost ratio for three of them (the cost ratio for the original scenario was known to be unbounded), providing a complete global picture of the behavior of present-biased agents, as far as optimisation tasks are concerned.

Joint work with Fedor V. Fomin (University of Bergen) and Petr Golovach (University of Bergen).

Wednesday November 27, 2019

8:30 - 9:00 *Gathering and Coffee*

9:00 - 9:40 **Stefano Leonardi -** *Envy, Regret, and Social Welfare Loss*

Incentive compatibility (IC) is a desirable property for any auction mechanism, including those used in online advertising. However, in real world applications practical constraints and complex environments often result in mechanisms that lack incentive compatibility. Recently, several papers investigated the problem of deploying black-box statistical tests to determine if an auction mechanism is incentive compatible. Unfortunately, most of those methods are costly, since they require the execution of many counterfactual experiments. In this work, we show that similar results can be obtained using the notion of IC-Envy. The advantage of IC-Envy is its efficiency: it can be computed using only the auction's outcome.

In particular, we focus on two relevant environments: position auctions and Ad Types auctions. For position auctions, we show that for a large class of pricing schemes (which includes e.g. VCG and GSP), IC-Envy $\geq$ IC-Regret (and IC-Envy = IC-Regret under mild supplementary conditions). Next, we consider non-separable CTRs in the Ad Types environment. In this setting, we show that for a generalization of the GSP mechanism IC-Envy $\geq$ IC-Regret holds as well. Our theoretical results are completed showing that, in the position auction environment, IC-Envy can be used to bound the loss in social welfare due to the advertiser untruthful behavior.

Joint work with Riccardo Colini-Baldeschi, Okke Schrijvers, and Eric Sodomka (Facebook Core Data Science).

9:40 - 10:10 **Daniel Lehmann -** *Many-to-many matching and bilateral markets*

A bilateral market can be described as a many-to-many matching problem with contracts where agents' preferences are expressed by choice functions. A natural solution concept is then that of a stable matching. Such stable matchings enjoy the one price property: identical items are traded at the same price. If all choice functions satisfy the path-independence property of C. Plott, then the existence of stable matchings is guaranteed and stable matchings have a lattice structure.

10:10 - 10:40 **Michal Feldman -** *A General Framework for Endowment Effects in Combinatorial Markets*

The endowment effect, coined by Nobel Laureate Richard Thaler, posits that people tend to inflate the value of items they own. This bias has been studied mainly using experimental methodology. Recently, Babaioff et al. proposed a specific formulation of the endowment effect in combinatorial markets, and showed that the existence of Walrasian equilibrium with respect to the endowed valuations extends from gross substitutes to submodular valuations, but provably fails to extend to XOS valuations.

We propose to harness the endowment effect further. We introduce a principle-based framework that captures a wide range of different formulations of the endowment effect (including that of Babaioff et al.). We equip our framework with a partial order over the different formulations, which ranks them from weak to strong, and provide algorithms for computing endowment equilibria with high welfare for sufficiently strong endowment effects, as well as non-existence results for weaker ones.

Our main results are the following: (1) For markets with XOS valuations, we provide an algorithm that, for any sufficiently strong endowment effect, given an arbitrary initial allocation S, returns an endowment equilibrium with at least as much welfare as in S. Moreover, every such endowment equilibrium gives at least half of the optimal social welfare. Evidently, the

negative result of Babaioff et al. for XOS markets is an artifact of their specific formulation. (2) For markets with arbitrary valuations, we show that bundling leads to a sweeping positive result. In particular, if items can be prepacked into indivisible bundles, we provide an algorithm that, for a wide range of endowment effects, given an initial allocation S, computes an endowment equilibrium with at least as much welfare as in S. The algorithm runs in poly time with poly many value (resp., demand) queries for submodular (resp., general) valuations.

Joint work with Tomer Ezra and Ophir Friedler.

10:40 - 11:00 *Coffee break*

11:00 - 11:40 **Gil Kalai -** *Report on Some Breakthroughs in Combinatorics*

I will discuss several breakthrough results (by other people) in Combinatorics of interest in the theory of computing. These results are related to Analysis of Boolean Functions (ABF): For some ABF played a role and for others ABF was expected to play a role but did not.

11:40 - 12:10 **Miklos Santha -** *Discrete logarithm and Diffie-Hellman problems in identity black-box groups*

We investigate the computational complexity of the discrete logarithm, the computational Diffie-Hellman and the decisional Diffie-Hellman problems in some identity black-box groups $G_{p,t}$, where p is a prime number and t is a positive integer. These are defined as quotient groups of vector space $\mathbb{Z}_p^{t+1}$ by a hyperplane H given through an identity oracle. While in general black-box groups with unique encoding these computational problems are classically all hard and quantumly all easy, we find that in the groups $G_{p,t}$ the situation is more contrasted. We prove that while there is a polynomial time probabilistic algorithm to solve the decisional Diffie-Hellman problem in $G_{p,1}$, the probabilistic query complexity of all the other problems is $\Omega(p)$, and their quantum query complexity is $\Omega(\sqrt{p})$. Our results therefore provide a new example of a group where the computational and the decisional Diffie-Hellman problems have widely different complexity.

This is joint work with Gábor Ivanyos and Antoine Joux.

12:10 - 12:40 **Itai Arad -** *Learning a local Hamiltonian from local measurements*

Recovering an unknown Hamiltonian from measurements is an increasingly important task for certification of noisy quantum devices and simulators. Recent works have succeeded in recovering the Hamiltonian of an isolated quantum system with local interactions from long-ranged correlators of a single eigenstate. Here we generalize these works to allow for the recovery of the Hamlitonian from any state that commutes with it, including, for example, the Gibbs state at a finite temperature. Our approach takes advantage of the non-commuteness of the underlying Hamiltonian to derive non-trivial local constraints between the local reduced density matrices and the local Hamiltonian terms. This enables us to learn a local patch of the Hamiltonian from local observations only on that patch, even though the overall state might be globally entangled. Surprisingly, there are interesting cases in which our algorithm is exponentially faster than the classical problem of learning a Boltzmann machine, or, more generally, a graphical model.

12:40 - 14:20 *Lunch* (Please see our list for a selection of restaurants.)

14:20 - 15:00 **Jean-Bernard Lasserre -** *Connecting optimization with spectral analysis of tri-diagonal (univariate) moment matrices*

We show that the global minimum (resp. maximum) of a continuous function on a compact set can be approximated from above (resp. from below) by computing the smallest (rest. largest) eigenvalue of a hierarchy of (r x r) tri-diagonal univariate moment matrices of increasing

size. Equivalently it reduces to computing the smallest (resp. largest) root of a certain univariate degree-r orthonormal polynomial. This provides a strong connection between the fields of optimization, orthogonal poly-nomials, numerical analysis and linear algebra, via asymptotic spectral analysis of tri-diagonal symmetric matrices. If time permits we will also show how the underlying technique allows to approximate the Lebsgue volume of sublevel sets of polynomials.

15:00 - 15:30 **Uri Feige -** *Finding cliques using few probes*

Consider algorithms with unbounded computation time that probe the entries of the adjacency matrix of an n vertex graph, and need to output a clique. We show that if the input graph is drawn at random from $G_{n,\frac{1}{2}}$ (and hence is likely to have a clique of size roughly $2\log n$), then for every $\delta < 2$ and constant ℓ, there is an $\alpha < 2$ (that may depend on δ and ℓ) such that no algorithm that makes n^δ probes in ℓ rounds is likely (over the choice of the random graph) to output a clique of size larger than $\alpha \log n$.

Joint work with David Gamarnik, Joe Neeman, Miklós Z. Rácz and Prasad Tetali.

15:30 - 16:00 **Amnon Ta-Shma -** *Parity samplers, double samplers and the quest for explicit, efficient binary error correcting codes*

The Gilbert-Varshamov bound tells us there are binary error correcting codes with distance $1/2 - \epsilon$ and relative rate $O(\epsilon^2)$. It has been long open to match these codes with explicit constructions. Recently, a construction with rate close to $O(\epsilon^2)$ and explicit encoding was found, but no explicit decoding is known to the code. One common technique for constructing such codes is using approximate error correction. In the talk I will explain what approximate error correction is, and survey several attempts at encoding and decoding such codes. As it turns out, many constructions use "double samplers" or variants of this object, and I will explain what double-samplers are, how they are related to the problem and what is known (and not known) about them.

The talk surveys many papers in the area and is also based on a recent paper with Dinur, Harsha, Kaufmann and Livni.

16:00 - 16:30 *Coffee break*

16:30 - 17:00 **Merav Parter -** *Nearly optimal secure distributed algorithms*

We study secure distributed algorithms that are nearly *optimal*, with respect to running time, for the given input graph G. Roughly speaking, an algorithm is *secure* if the nodes learn only their final output while gaining no information on the input (or output) of other nodes.

A graph theoretic framework for secure distributed computation was recently introduced by the authors (SODA 2019). This framework is quite general and it is based on a new combinatorial structure called *private neighborhood trees*: a collection of n trees $T(u_1), \ldots, T(u_n)$ such that each tree $T(u_i)$ spans the neighbors of u_i without going through u_i. Intuitively, each tree $T(u_i)$ allows all neighbors of u_i to exchange a *secret* that is hidden from u_i. The efficiency of the framework depends on two key parameters of these trees: their depth and the amount of overlap. In a $(\mathtt{d}, \mathtt{c})$-private neighborhood trees each tree $T(u_i)$ has depth $O(\mathtt{d})$ and each edge $e \in G$ appears in at most $O(\mathtt{c})$ different trees. An *existentially* optimal construction of private neighborhood trees with $\mathtt{d} = O(\Delta \cdot D)$ and $\mathtt{c} = \widetilde{O}(D)$ was presented therein. We make two key contributions: *Universally Optimal Private Trees:* We show a combinatorial construction of nearly (universally) optimal $(\mathtt{d}, \mathtt{c})$-private neighborhood trees with $\mathtt{d} + \mathtt{c} = \widetilde{O}(\mathsf{OPT}(G))$ for any input graph G. Perhaps surprisingly, we show that $\mathsf{OPT}(G)$ is equal to the best depth possible for these trees even without the congestion constraint. We also present efficient distributed constructions of these private trees. *Optimal Secure Computation:* Using the

optimal constructions above, we get a secure compiler for distributed algorithms where the overhead for each round is $\widetilde{O}(\mathsf{poly}(\Delta) \cdot \mathsf{OPT}(G))$. As our second key contribution, we design an optimal compiler with an overhead of merely $\widetilde{O}(\mathsf{OPT}(G))$ per round for a class of "simple" algorithms. This class includes many standard distributed algorithms such as Luby-MIS, the standard logarithmic-round algorithms for matching and $\Delta + 1$-coloring, as well as the computation of aggregate functions.

Joint with Eylon Yogev.

17:00 - 17:30 **Guy Even -** *Fully-Dynamic Space-Efficient Dictionaries and Filters with Constant Number of Memory Accesses*

A fully-dynamic dictionary is a data structure for maintaining sets that supports insertions, deletions and membership queries. A filter approximates membership queries with a one-sided error. We present two designs: (1) The first space-efficient fully-dynamic dictionary that maintains both sets and random multisets and supports queries, insertions, and deletions with a constant number of memory accesses in the worst case with high probability. The comparable dictionary of Arbitman, Naor, and Segev [FOCS 2010] works only for sets. (2) By a reduction from our dictionary for random multisets, we obtain a space-efficient fully-dynamic filter that supports queries, insertions, and deletions with a constant number of memory accesses in the worst case with high probability (as long as the false positive probability is $2^{-O(w)}$, where w denotes the word length). This is the first in-memory space-efficient fully-dynamic filter design that provably achieves these properties. We also present an application of the techniques used to design our dictionary to the static Retrieval Problem.

Joint work with Ioana O. Bercea.

19:00 - *Reception* (see more details in "local information for participants")

Thursday November 28, 2019

8:30 - 9:00 *Gathering and Coffee*

9:00 - 9:40 **Allan Borodin -** *Two studies concerning voting systems*

There is a current interest in social choice theory (e.g. voting systems) motivated at least in part by the divisiveness apparent in many countries. Can theoretical computer science bring any insight into some of the more prominent issues? More specifically, recent elections in the US and Canada (and elsewhere) have brought to prominence a couple of issues, Gerrymamdering and the role of primaries in voting. . (Voting goes beyond political elections but political elections are the most newsworthy.) As one can imagine, there are complex modeling and computational issues when dealing with large social systems.

We have some preliminary but we think interesting insights into gerrymandering and primary systems. I will only briefly talk about gerrymandering and how the "power of gerrymadering" relates to the degree of urbanization. I will mainly talk about the issue of primaries vs direct elections as our work here is a blend of both theory and experimental work. Here is (are) the question(s): What is the impact on the "quality" of our chosen leaders by having primaries where each party has its own election to choose their candidate for the general election? Does this tend to result in more extreme candidates? In our AAAI 2019 paper on primaries, we conduct the first quantitative study of primary vs direct elections.

Joint work with Omer Lev, Nisarg Shah and Tyrone Strangway.

9:40 - 10:10 **Keerti Choudhary -** *Extremal Distance Spanners*

In the area of graph sparsification, the distance spanners are sparse subgraphs preserving pairwise distances up to a small stretch. These structures have been well studied for undirected graphs for the past three decades. However, for directed graphs, sparse (subquadratic-sized) distance approximating spanners are not possible in general. We thus focus on the notion of extremal distance spanners in directed graphs.

For a directed graph $G = (V, E)$, a subgraph $H = (V, E')$ is said to a t-diameter spanner if the diameter of H is at most t times the diameter of G. Similarly, a t-eccentricity spanner, is a subgraph that approximately preserves all vertex eccentricities of the original graph, up to a stretch factor t. In this talk, we will look at the existence of (and algorithms to compute) various t-diameter and t-eccentricity spanners with a sparse set of edges for t at most 2. These spanner constructions are tight for graphs of small diameter. As a byproduct of the eccentricity spanner construction, we obtain a near-linear time algorithm for computing a two approximation of vertex eccentricities in general directed graphs.

Joint work with Omer Gold.

10:10 - 10:40 *Coffee break*

10:40 - 11:10 **Roi Livni -** *Graph-Based Discrimination*

A basic question in learning theory is to identify if two distributions are identical when we have access only to examples sampled from the distributions. This basic task arises in the context of learning, but also in the context of Generative Adversarial Networks (GANs), where a discriminator is trained to distinguish between a real-life distribution and a synthetic distribution. Classically, we use a hypothesis class H and claim that the two distributions are distinct if for some hypothesis in H the expected value on the two distributions is (significantly) different. Our starting point is the following fundamental problem: "is having the hypothesis

dependent on more than a single random example beneficial". To address this challenge we introduce k-ary based discriminators which can be modeled by a family of (hyper)-graphs. Each hypergraph is used to test if the distributions are distinct by estimating the probability of an (hyper)-edge. We study the expressiveness of such graph-based discriminators and compare them to the classical setting of learning, which is $k = 1$. We show a separation in expressiveness of $k + 1$ vs k-ary graph based discriminators and introduce a combinatorial measure, called graph-VC dimension, and show that it controls the sample complexity.

11:10 - 11:40 **Ohad Shamir -** *Training Neural Networks: The Bigger the Better?*

Artificial neural networks are nowadays routinely trained to solve challenging learning tasks, but our theoretical understanding of this phenomenon remains quite limited. One increasingly popular approach, which is aligned with practice, is to study how making the network sufficiently large (a.k.a. "over-parameterized") makes the associated training problem easier. In this talk, I'll describe some of the possibilities and challenges in understanding neural networks using this approach.

Based on joint works with Itay Safran and Gilad Yehudai

11:40 - 12:10 **Vianney Perchet -** *Multiplayer Multi-Armed Bandits. Synchronisation Unlocks Communication !*

Motivated by cognitive radio networks, we consider the stochastic multiplayer multi-armed bandit problem, where several players pull arms simultaneously and collisions occur if one of them is pulled by several players at the same stage. We present a decentralized algorithm that achieves the same performance as a centralized one, contradicting the existing lower bounds for that problem. This is possible by "hacking" the standard model by constructing a communication protocol between players that deliberately enforces collisions, allowing them to share their information at a negligible cost. This motivates the introduction of a more appropriate dynamic setting without sensing, where similar communication protocols are no longer possible. However, we show that the logarithmic growth of the regret is still achievable for this model with a new algorithm.

12:10 - 12:40 **Shie Mannor -** *Batch-Size Independent Regret Bounds for the Combinatorial Multi-Armed Bandit Problem*

12:40 - 14:20 *Lunch* (Please see our list for a selection of restaurants.)

14:20 - 15:00 **Amit Chakrabarti -** *Verifiable Stream Computation and Arthur-Merlin Communication*

A space-limited client needs to process a massive stream of data and perform a computation that does not admit a sublinear-space algorithm. So it outsources the processing to a commercial cloud computing service, but is unwilling to blindly trust answers returned by this service. It turns out that for many important problems, one can design a suitable communication protocol between server (prover) and client (verifier) that allows the former to convince the latter of the correct answer.

This general question has been studied in a number of research works over the past decade, leading to protocols for statistical problems such as computing moments, norms, and heavy hitters; geometric problems such as nearest neighbor search and range counting; and graph problems such as shortest path, maximum matching, and triangle counting. I shall survey some of the highlights of this emergent area, with a particular focus on recent developments on graph computations in this setting. Lower bounds in the area are closely related to Arthur-Merlin communication, a fascinating and less-explored corner of communication complexity. I shall broadly outline these connections.

15:00 - 15:30 **Rotem Oshman -** *Interactive Distributed Proofs*

Interactive proof systems allow a resource-bounded verifier to decide an intractable language (or compute a hard function) by communicating with a powerful but untrusted prover. Such systems guarantee that the prover can only convince the verifier of true statements. In the context of centralized computation, a celebrated result shows that interactive proofs are extremely powerful, allowing polynomial-time verifiers to decide any language in PSPACE. In this work we initiate the study of distributed interactive proofs: a network of nodes interacts with a single untrusted prover, who sees the entire network graph, to decide whether the graph satisfies some property. We focus on the communication cost of the protocol – the number of bits the nodes must exchange with the prover and each other. Our model can also be viewed as a generalization of the various models of "distributed NP" (proof labeling schemes, etc.) which received significant attention recently: while these models only allow the prover to present each network node with a string of advice, our model allows for back-and-forth interaction. We show that for some problems, interaction can exponentially decrease the communication cost compared to a non-interactive prover, but on the other hand, some problems retain non-trivial cost even with interaction.

15:30 - 16:00 **Alexandre Nolin -** *The communication complexity of functions with large outputs*

We study the two-party communication complexity of functions with large outputs, and show that the communication complexity can greatly vary depending on what output model is considered. The output models we consider are arranged in a hierarchy. The most communication-demanding model requires that the players' communication reveals the outcome of their computation to an external observer, while the most communication-efficient model – named the XOR model – requires that the two players' communication allows them to each locally compute a bit string such that the bitwise XOR of the two bit strings is the outcome of the computation. We extend the classical results of error reduction and randomness removal in all models, and prove separations between all models.

For functions of output size k, the naive approach to error reduction in some models would introduce an additional cost in k. Our main result is that no dependency in k is actually necessary, in all models. Optimizing the dependencies in the error parameters in the XOR model involves a random graph and using an amortized protocol for the Equality problem.

16:00 - 16:30 **Adi Rosén -** *A New Approach to Multi-Party Peer-to-Peer Communication Complexity*

We introduce new models and new information theoretic measures for the study of communication complexity in the natural peer-to-peer, multi-party, number-in-hand setting. We prove a number of properties of our new models and measures and then exemplify their effectiveness by proving two lower bounds. The more elaborate one is a tight lower bound of $\Omega(kn)$ on the multi-party peer-to-peer randomized communication complexity of the k-player, n-bit Disjointness function. The other one is a tight lower bound of $\Omega(kn)$ on the multi-party peer-to-peer randomized communication complexity of the k-player, n-bit bitwise parity function. The lower bound for Disjointness improves over the lower bound that can be inferred from the result of Braverman et al. (FOCS 2013), which was proved in the coordinator model and can yield a lower bound of $\Omega(kn/\log k)$ in the peer-to-peer model. To the best of our knowledge, our lower bounds are the first tight (non-trivial) lower bounds on communication complexity in the natural *peer-to-peer* multi-party setting.

Joint work with Florent Urrutia.

16:30 - 17:00 *Coffee break*

17:00 - 17:30 **Or Zamir -** *Faster k-SAT algorithms using biased-PPSZ*

The PPSZ algorithm, due to Paturi, Pudlak, Saks and Zane, is currently the fastest known algorithm for the k-SAT problem, for every $k > 3$. For 3-SAT, a tiny improvement over PPSZ was obtained by Hertli. We introduce a biased version of the PPSZ algorithm using which we obtain an improvement over PPSZ for every $k \geq 3$. For $k = 3$ we also improve on HerliÕs result and get a much more noticeable improvement over PPSZ, though still relatively small. In particular, for Unique 3-SAT, we improve the current bound from 1.308^n to 1.307^n.

Joint work with Thomas Dueholm Hansen, Haim Kaplan and Uri Zwick.

17:30 - 18:00 **Uri Zwick -** *A faster deterministic exponential time algorithm for Energy Games and Mean Payoff Games*

We present an improved exponential time algorithm for Energy Games, and hence also for Mean Payoff Games. The running time of the new algorithm is $O(\min\{mnW, mn2^{n/2}\}$, where n is the number of vertices, m is the number of edges, and when the edge weights are integers of absolute value at most W. For small values of W, the algorithm matches the performance of the pseudopolynomial time algorithm of Brim et al. on which it is based. For $W \geq 2^{n/2}$, the new algorithm is faster than the algorithm of Brim et al. and is currently the fastest *deterministic* algorithm for Energy Games and Mean Payoff Games. The new algorithm is obtained by introducing a technique of forecasting repetitive actions performed by the algorithm of Brim et al.

Joint work with Dani Dorfman and Haim Kaplan.