

RS&A 2007 Plenary Talks

Local consistency in direct products

Irit Dinur

Hebrew University

Given a function $f : [n] \rightarrow \{0, 1\}$, its k -wise direct product encoding is the function $F : [n]^k \rightarrow \{0, 1\}^k$ defined by $F(x_1, \dots, x_k) = (f(x_1), \dots, f(x_k))$. This simple “encoding” is useful in PCP-like settings, when we want to simulate reading k arbitrary values of f by accessing only a constant number of inputs of the encoding F .

The main challenge is to test that a given F is indeed a “correct” encoding of some f by reading only few (ultimately 2) random values in F . This is called a local consistency test.

In the talk I will survey some variants of the problem and discuss the context in which this problem arises, with particular focus on gap amplification.

Pseudo-randomness

Tomasz Łuczak

Adam Mickiewicz University, Poznań, Poland

In the talk we survey some results and conjectures on pseudo-randomness and the structural theorems (as the Regularity Lemma) for sets, graphs, and hypergraphs.

Random Graphs, Spin Glasses and Percolation

Charles Newman

Courant Institute, NYU

We will survey some percolation methods based on the Fortuin-Kasteleyn random cluster model, that have been important in the analysis of ferromagnetic Ising models, when the underlying graph

is d -dimensional ($d > 2$). When the underlying graph is the complete graph, the random cluster model relates the ferromagnet phase transition to the occurrence of giant clusters in Erdős-Rényi random graphs.

There also is a random cluster model for non-ferromagnets, including spin glasses such as those on the complete graph, studied in recent years by Talagrand. In joint work with Jon Machta and Dan Stein, motivated by d -dimensional spin glasses, we have studied the nature of the giant cluster transition in a “two-replica” random cluster model on the complete graph and shown that beyond the transition point there are exactly **two** giant clusters and they have *unequal* densities (i.e., fractions of sites). There is also numerical evidence that this phenomenon occurs in 3-dimensional spin glasses.

Decomposition Of Multiple Coverings

János Pach

City College, New York and Rényi Institute, Budapest

A family \mathcal{C} of convex bodies form a k -fold covering of a region R if every point of R is contained in at least k members of \mathcal{C} . Twenty ears ago I proved that for each centrally symmetric convex polygon P , there is a constant $k = k(P)$ such that any k -fold covering of the plane with translates of P can be decomposed into *two* coverings. Does the same theorem remain true for (a) unit circles in the place of polygons, (b) circles of arbitrary radii, (c) unit balls in higher dimensions? We survey some old and new results of this type.

The case when \mathcal{C} consists of axis-parallel rectangles will be discussed in more detail. We construct, for every k , a k -fold covering \mathcal{C}_k of the plane (or of a large square) with rectangles whose sides are parallel to the coordinate-axes, such that \mathcal{C}_k cannot be split into two coverings (P.-Tardos-Tóth). We also present, for every k and c , a probabilistic construction of a k -fold covering $\mathcal{C}_{k,c}$ of the plane with axis-parallel rectangles such that no matter how we color these rectangles with c colors, we find a point that is covered only by rectangles of the same color (P.-Tardos). The “dual” statement is also true: With probability tending to one, a sufficiently large point set, randomly and uniformly selected from the unit square, has the property that no

matter how we color its elements by c colors, there is an axis-parallel rectangle containing precisely k points, all of which have the same color (Chen-P.-Szegedy-Tardos).

Critical random graphs: diameter and mixing time

Yuval Peres

Microsoft Research and UC Berkeley

Let C_1 denote the largest connected component of the Erdős-Rényi random graph $G(n, c/n)$. For c different from 1, the diameter of C_1 and the mixing time of lazy simple random walk on C_1 are known powers of $\log(n)$. For the critical case $c = 1$, it is well known that C_1 typically has volume of order $n^{2/3}$. We show that, for $c = 1$, the diameter of C_1 is typically of order $n^{1/3}$ and the mixing time of the lazy random walk on C_1 is of order n . The latter answers a question of Benjamini, Kozma and Wormald. These results extend to clusters of size $n^{2/3}$ of p -bond percolation on any d -regular n -vertex graph where such clusters typically exist, provided that $p(d - 1)$ is at most 1; they also extend to the “scaling window”. Finally, we propose a new definition for the critical percolation probability p_c in a transitive finite graph. (Joint work with Asaf Nachmias).

Testing Properties of Distributions

Ronitt Rubinfeld

MIT CSAIL

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 algorithms for many such testing problems whose sample complexities are sublinear in the size of the support.

Sumsets, arithmetical progressions, entropy

Imre Z. Ruzsa

Alfréd Rényi Institute of Mathematics, Budapest

Some problems of combinatorial number theory (or “additive combinatorics”, with a recent term) can be expressed in the language of entropy. One example is the *arithmetical progression conjecture*: if a set contains n arithmetical progressions of length k and distinct differences, then its size must be $\gg n^{1-\varepsilon_k}$, where $\varepsilon_k \rightarrow 0$ as $k \rightarrow \infty$. This is important, among others, because of its connection with the Kakeya conjecture. An affirmative answer to the arithmetical progression conjecture would imply the Kakeya conjecture, and a negative answer would be good reason to doubt it.

Now the arithmetical progression conjecture is equivalent to the following. For every $\varepsilon > 0$ there exist rational numbers a_1, \dots, a_k and positive numbers c_1, \dots, c_k such that $\sum c_i < 1 + \varepsilon$ and for every pair ξ, η of (not necessarily independent) discrete random variables the inequality $h(\eta) \leq c_1 h(\xi + a_1 \eta) + c_2 h(\xi + a_2 \eta) + \dots + c_k h(\xi + a_k \eta)$ holds. Here h denotes the (discrete) entropy, that is, if a random variable ξ assumes values x_1, x_2, \dots with probabilities p_1, p_2, \dots , then its entropy is $h(\xi) = -\sum p_i \log p_i$.

As an example, the entropy translation of an inequality of Katz and Tao reads as follows: $h(\eta) \leq \frac{2}{3}h(\xi + \eta) + \frac{2}{3}h(\xi - \eta) + \frac{1}{2}h(\xi)$. The important point here is that the sum of coefficients, though not very near to 1, is definitely less than 2; for 2 there are trivial such inequalities. Another example is the following simple inequality of mine: if X, Y, Z are finite sets, then $|X||Y - Z| \leq |X - Y||X - Z|$. The entropy analogue is now $h(\xi) + h(\eta - \zeta) \leq h(\xi - \eta) + h(\xi - \zeta)$, whenever ξ is independent of (η, ζ) .

At this moment I do not have a general “theory of entropy translation”, only a few isolated examples and a feeling how others should look. For instance, for sumsets we have the inequality (which differs from the previous one only in a sign): $|X||Y + Z| \leq |X + Y||X + Z|$. Is it true that (for independent variables) $h(\xi) + h(\eta + \zeta) \leq h(\xi + \eta) + h(\xi + \zeta)$? We know that $|X + Y + Z|^2 \leq |X + Y||X + Z||Y + Z|$. Is it true that (for independent variables) $2h(\xi + \eta + \zeta) \leq h(\xi + \eta) + h(\xi + \zeta) + h(\eta + \zeta)$?

List-Decoding: A Survey

Madhu Sudan

MIT CSAIL

The theory of error-correction has had two divergent schools of thought, going back to the works of Shannon and Hamming. In the Shannon school, error is presumed to have been effected probabilistically. In the Hamming school, the error is modeled as effected by an all-powerful adversary. The two schools lead to drastically different limits. In the Shannon model, a binary channel with error-rate close to, but less than, 50% is useable for effective communication. In the Hamming model, a binary channel with an error-rate of more than 25% prohibits unique recovery of the message.

In this talk, we describe the notion of list-decoding, as a bridge between the Hamming and Shannon models. This model relaxes the notion of recovery to allow for a "list of candidates". We describe some of the algorithmic results in this model, hopefully ending with the recent breakthroughs of Parvaresh and Vardy; and Guruswami and Rudra, that achieve optimal rate list-decodable codes over large alphabets.

On perfect factoring of random (hyper)-graphs

Van Vu

Rutgers University

Let H be a fixed (hyper)graph with v points and m edges. We say that a (hyper)graph G on n points (with $v \mid n$) has a perfect H -factoring if G contain n/v vertex disjoint copies of H . The problem of finding the threshold for having a perfect H -factor for the random (hyper)graph $G(n, p)$ is well known and has been open for some time.

I will give a brief survey on this problem and discuss a few recent results.