Three Tutorial Lectures

David Galvin
University of Notre Dame

Entropy and Counting

The *entropy* (or *Shannon entropy*) of a probability distribution is a measure of how random a draw from the distribution is; it can also be thought of as a measure of the expected amount of surprise evinced when the result of the draw is revealed. Introduced by Claude Shannon in 1948, it plays a central role in information theory and has been studied intensively in that field.

In recent years entropy has been applied very successfully to a variety of combinatorial enumeration problems. The key property here is the following: the entropy of a uniform distribution on n values is $\log n$. So if X is a random variable that encodes a uniform selection from a set $\mathcal{C}$, then any statement one can make about the entropy of X (using old results from information theory, or new results created with combinatorial applications in mind) translates directly into a statement about $|\mathcal{C}|$.

In this series of talks I'll introduce the entropy function, and derive its key properties. I'll then discuss some combinatorial applications, including:

- bounding the volume of a set in $\mathbb{R}^d$ in terms of its $(d-1)$-dimensional projections (the Loomis-Whitney inequality),
- Radhakrishnan's proof of Brégman's theorem (the Minc conjecture) on the maximum permanent of a 0-1 matrix with fixed row sums,
- Kahn's tight bound on the number of independent sets in a regular bipartite graph, and
- Cuckler and Kahn's determination of the number of Hamilton cycles in a Dirac graph.

Along the way there will be plenty of open questions.