Entropy, partitions, groups and association schemes

Peter Cameron, Rosemary Bailey and Søren Riis

This short series is inspired by the talks by Terence Chan at our recent workshop on "Information flows and information bottlenecks". No familiarity with those talks will be assumed.

In the first talk, we define the entropy function of a family of random variables on a finite probability space. We prove Chan's theorem that it can be approximated (up to a scalar multiple) by the entropy function obtained when G is a finite group (carrying the uniform distribution) and the random variables are associated with a family of subgroups of G: the random variable associated with H takes a group element to the coset of H containing it.

These partitions are uniform (all parts have the same size). In the second talk, we define orthogonality of partitions, and interpret orthogonality in terms of the entropy of the associated random variables. We explain how a sublattice of the partition lattice consisting of mutually orthogonal uniform partitions gives rise to an association scheme.

The third talk concerns information inequalities. These are connected to multiplicative subgroup inequalities in group theory: for example, the linear information inequality $H(A,B) \leq H(A)+H(B)$ corresponds to Lagrange's inequality $|A| \cdot |B| \leq |G| \cdot |A \cap B|$.

In 1999 Zhang and Yeung showed – contradicting conventional wisdom – that there exist "laws of information theory" beyond those that follow from Shannon's classical information inequalities. The talk presents the key parts of Zhang's and Yeung's proof. To the extent that the time allows we will also present and prove a more recent result by Chan and Grant which shows that the entropy cone is "curved" and that there exist non-linear laws of information theory. Thus there exist "non-multiplicative" subgroup inequalities that are valid for the class of finite groups , but do not follow form any finite collection of multiplicative subgroup inequalities.

The talk also presents a list of natural open questions on the interface between Information Theory, Graph Theory and Group Theory.