DAVID THOMSON, Tutte Institute for Mathematics and Computing
Derivatives in Finite Fields

Derivative-like transformations over finite fields arise in numerous applications: they measure autocorrelations of permutation arrays and they are used in cryptanalysis of both symmetric and asymmetric cryptography. Interestingly, these finite derivatives are expressed in the same way as bilinear forms associated with a quadratic form. Quadratic maps are also of significant interest in applications.

In this talk, we make explicit a correspondence between uni- and multi-variate polynomials that translates q-degrees in univariate representations to algebraic degrees in the familiar sense. We view so-called Dembowski-Ostrom polynomials (with q-degree 2) as quadratic forms and continue to pull on this thread to find out where this correspondence leads.