

Title: Coding, Cryptography, and Conics: using what they know to introduce research

Abstract: I have had some success in recent years bringing my research in finite geometry to the undergraduate level. My technique has been to use topics that students are already familiar with in order to introduce research level topics. In this talk I will address my use of quadratic curves, but applied to finite projective geometry – not Euclidean geometry, to study problems in coding theory and cryptography. Specifically, we look at applications to LDPC codes, secret-sharing schemes, and a certain cryptographic protocol. My expectations as well as student results will all be discussed. These range from in-house technical reports, to poster presentations, to refereed research publications.