abstract

COMPUTER SCIENCE/DISCRETE MATH I
Topic:

Speaker:

Affiliation:

Date:

Time/Room:

Recently, algebraic codes which achieve the optimal trade-off between rate and (list) error-correction radius were constructed by a careful "folding" of the Reed-Solomon code. The "low-degree'' nature of this folding operation was crucial to the list decoding algorithm. We show how one can define such folding schemes based on the Artin-Frobenius automorphism at primes in Galois extensions. Using this approach, we construct new folded algebraic-geometric codes for list decoding based on cyclotomic function fields with a cyclic Galois group. Such function fields are obtained by adjoining torsion points of the Carlitz action of an irreducible M \in F_q[T] . The Reed-Solomon case corresponds to the simplest such extension (corresponding to the case M=T) . In the general case, we need to descend to the fixed field of a suitable Galois subgroup in order to ensure the existence of many degree one places that can be used for encoding.

In addition to shedding new light on algebraic codes and their list decoding, quantitatively our results lead to codes with list decoding guarantees similar to folded Reed-Solomon codes but whose alphabet size is at most polylogarithmic in the block length (rather than polynomial in the block length, as is the case for folded RS codes).