

# **abstract**

Computer Science/Discrete Mathematics Seminar II  
Topic:

Speaker:

Affiliation:

Date:

Time/Room:

---

We study the list-decodability of multiplicity codes.

These codes, which are based on evaluations of high-degree polynomials and their derivatives, have rate approaching 1 while simultaneously allowing for sublinear-time error-correction. In this paper, we show that multiplicity codes also admit powerful list-decoding and local list-decoding algorithms correcting a large fraction of errors.

Our first main result shows that univariate multiplicity codes over prime fields achieve “list decoding capacity”. This provides a new (and perhaps more natural) example of such a code after the original Folded Reed-Solomon Codes of Guruswami and Rudra. The list decoding algorithm is based on constructing a differential equation of which the desired codeword is a solution; this differential equation is then solved using a power-series approach (a variation of Hensel lifting) along with other algebraic ideas.

Our second main result is a list-decoding algorithm for decoding multivariate multiplicity codes up to the Johnson radius.

In particular, this is the first algorithm to decode multiplicity codes up to half their minimum distance. The key ingredient of this algorithm is the construction of a special family of “algebraically-repelling” curves passing through the points of  $F_q^m$ ; no moderate-degree multivariate polynomial over  $F_q^m$  can simultaneously vanish on all these curves.

As a corollary, we show that multivariate multiplicity codes of length  $n$  and rate nearly 1 can be locally list-decoded up to the Johnson radius in  $O(n^{\epsilon})$  time.