

1030-14-244

Philip R Busse* (pbusse@ms.uky.edu), Department of Mathematics, University of Kentucky,
Lexington, KY 40506-0027. *Groebner Bases & List Decoding BCH Codes*. Preliminary report.

Coding theory is one of the most relevant applied aspects of mathematics in industry today. List decoding Reed-Solomon codes via an interpolation and root-finding algorithm was pioneered by Madhu Sudan in the mid to late 1990's. In 2006, Kwankyu Lee and Michael O'Sullivan developed a Groebner basis based implementation of the interpolation algorithm, which they showed was an efficient generalization of the Berlekamp-Massey Algorithm. A change-of-basis technique that takes into account some reliability information given about the channel enhances the efficiency of their algorithm. We propose to apply these ideas to list decoding BCH codes by presenting BCH codes as subfield subcodes of generalized Reed-Solomon codes and to explore the resulting algorithm and apply a comparable change-of-basis transformation. In particular, we seek ways to optimize the new algorithm and to compare it with the Berlekamp-Massey algorithm. (Received August 04, 2007)