Algebraic Algorithms and Coding Theory

Madhu Sudan[1] *

MIT CSAIL, madhu@mit.edu

Abstract. The associated talk surveys some recent developments in algorithmic coding theory that answer some fundamental questions with algebraic techniques.

1 Introduction

The theory of error-correcting codes has long seen codes with remarkable combinatorial performance emerging from the study of algebraic functions over finite fields (e.g., Reed-Solomon code [9], BCH codes [2, 7], algebraic-geometry codes [4, 11]). They have also provided the inspiration for, and benefitted from, the development of algebraic algorithms (e.g., Berlekamp's algorithm for factoring univariate polynomials [1], Groebner basis based algorithms for decoding algebraic-geometry codes). This phenomenon has repeated itself in recent years with a resurgence of algorithms for problems in error-correction (list-decoding of Reed-Solomon codes [10, 6] and the recent results of Parvaresh-Vardy [8] and Guruswami-RudraGuRu), which have in turn inspired new (fast) algorithms for polynomial factorization (due to Chris Umans [12]).

In this survey we will introduce the basic algebraic codes and their decoding algorithms. The hope is to eventually describe the Guruswami-Rudra result which shows how to construct codes over a large alphabet of rate $1 - p - o(1)$ that correct (list-decode) p fraction of adversarially injected errors in polynomial time. Prior to this result no explicit construction of such codes (capable of correcting so many errors with even exponential time decoding algorithms) was known!

Tentative sequence of topics:

1. Codes, decoding, and list-decoding. basic parameters.
2. Reed-Solomon codes. combinatorial list-decodability.
3. Algorithmic list-decoding of Reed-Solomon Codes [10].
4. Improved list-decoding of Reed-Solomon codes [6].
5. Interleaved Reed-Solomon codes and decoding [8].
6. Folded Reed-Solomon codes and decoding [5].

References

1. Elwyn Berlekamp. Factoring polynomials over large finite fields. *Mathematics of Computations*, 24:713–735, 1970.
2. R. C. Bose and D. K. Ray-Chaudhuri. On a class of error correcting binary group codes. *Information and Control*, 3:68–79, 1960.

* Supported in part by NSF Award CCR 0514915.

3. Don Coppersmith and Madhu Sudan. Reconstructing curves in three (and higher) dimensional spaces from noisy data. In *Proceedings of the 35th Annual ACM Symposium on Theory of Computing*, pages 136–142, 2003.
4. V. D. Goppa. Codes associated with divisors. *Problems of Information Transmission*, 13(1):22–26, 1977.
5. Venkatesan Guruswami and Atri Rudra. Manuscript, 2004.
6. Venkatesan Guruswami and Madhu Sudan. Improved decoding of Reed-Solomon and algebraic-geometric codes. *IEEE Transactions on Information Theory*, 45:1757–1767, 1999.
7. A. Hocquenghem. Codes correcteurs d'erreurs. *Chiffres (Paris)*, 2:147–156, 1959.
8. Farzad Parvaresh and Alexander Vardy. Correcting errors beyond the Guruswami-Sudan radius in polynomial time. In *FOCS*, pages 285–294. IEEE Computer Society, 2005.
9. Irving S. Reed and Gustav Solomon. Polynomial codes over certain finite fields. *J. SIAM*, 8:300–304, 1960.
10. Madhu Sudan. Decoding of Reed-Solomon codes beyond the error-correction bound. *Journal of Complexity*, 13(1):180–193, 1997.
11. Michael A. Tsfasman, Serge G. Vlădut, and Thomas Zink. Modular curves, Shimura curves, and codes better than the Varshamov-Gilbert bound. *Math. Nachrichten*, 109:21–28, 1982.
12. Chris Umans. Fast polynomial factorization and modular composition in small characteristic. In *Proceedings of ACM STOC '08*, page to appear, 2008.