

# Performance Enhancements for Algebraic Soft Decision Decoding of Reed-Solomon Codes<sup>1</sup>

Mostafa El-Khamy, Robert J. McEliece, and Jonathan Harel  
 California Institute of Technology  
 Pasadena, CA 91125, USA  
 {mostafa, rjm, harel}@systems.caltech.edu

*Abstract* — In an attempt to determine the ultimate capabilities of the Sudan/Guruswami-Sudan/Kötter-Vardy algebraic soft decision decoding algorithm for Reed-Solomon codes, we present a new method, based on the Chernoff bound, for constructing multiplicity matrices. In many cases, this technique predicts that the potential performance of ASD decoding of RS codes is significantly better than previously thought.

## I. INTRODUCTION

Through the seminal work of Guruswami-Sudan (GS) [1], and Kötter-Vardy (KV) [2], we now have a polynomial-time algebraic soft decision (ASD) decoding algorithm for Reed-Solomon codes. In this paper we offer a methodology for assigning multiplicities used by the GS algorithm and thus an ASD algorithm with an improved performance over previously proposed algorithms [2, 3]. The idea is to choose the multiplicity matrix so as to maximize the probability that the causal codeword is on the decoder’s list, as suggested in [3], rather than to maximize the expected score of the causal codeword, as is done in [2]. However, whereas in [3], a Gaussian approximation is employed, we use a Chernoff bound instead. It was independently suggested in [4] to use the Chernoff bound in optimizing symbol based multiplicity matrices for the case of infinite costs and discrete memoryless channels.

Let an  $(n, k)$  RS codeword over  $GF(q)$  be represented by a binary  $(q \times n)$  matrix  $C$  determining which symbols were sent. The soft output of the channel is represented by an  $(q \times n)$  matrix  $\Pi$  of a-posteriori probabilities. The multiplicity assignment optimization problem is to generate a multiplicity matrix  $M$  of non-negative integers that will minimize the error probability  $P(\Pi, |M|) = P\{S_M(C) < \Delta(M)\}$  where  $\Delta(M)$  is a function of  $|M|$ , the interpolation cost of  $M$ , and  $k$ .  $S_M(C)$  is the dot product of  $M$  and  $C$  and is termed the *score* [2].

## II. OPTIMIZATION PROBLEM

Let  $G(\nu, M) = E\{e^{-\nu S_M(C)}\}$  be the moment generating function of the score, then the Chernoff bound says

$$P(\Pi, |M|) \leq \min_{\nu \geq 0} e^{\nu \Delta(M)} G(\nu, M).$$

Since integer optimization is hard we relax the constraint that the entries of  $M$  are integers and let the associated error probability be  $P^*(\Pi, |Q|)$ . In fact the following theorem shows that if cost is no object we loose nothing by this relaxation.

**Theorem 1** *Let  $P(\Pi) = \lim_{\gamma \rightarrow \infty} P(\Pi, \gamma)$  and  $P^*(\Pi) = \lim_{\gamma \rightarrow \infty} P^*(\Pi, \gamma)$ , then  $P^*(\Pi) = P(\Pi)$ .*

<sup>1</sup>This research was supported by NSF grant no. CCR-0118670 and grants from Sony, Qualcomm, and the Lee Center for Advanced Networking.

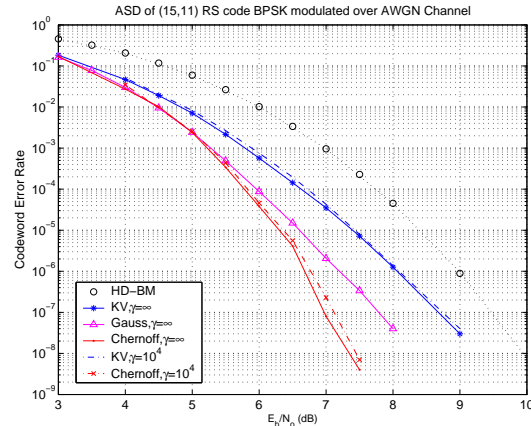


Fig. 1: (15,11) RS code BPSK modulated over an AWGN channel

Thus, for a finite cost  $\gamma$ , the relaxed optimum matrix,  $Q$ , is found by solving the constrained optimization problem,  $Q = \arg \min_{|Q|=\gamma} \min_{\nu \geq 0} (\nu \Delta(Q) + \log G(\nu, Q))$ , using the Lagrange multipliers technique. (The optimized Lagrangian is convex in both  $\nu$  and  $Q$ .) An algorithm is thus developed that will iteratively solve for the optimum  $\nu$  and  $Q$ . For the case of an infinite cost multiplicity matrix we make use of the following theorem in deriving the algorithm,

## Theorem 2

$$P(\Pi) \leq \min_{\|Q\|^2=1} \min_{\nu \geq 0} (\nu \sqrt{k-1} + \log G(\nu, Q)).$$

## III. RESULTS

In Fig. 1, we refer to our algorithm, the algorithms of [2] and [3] as Chernoff, KV and Gauss respectively. For the (15,11) RS code, infinite cost  $\gamma$ , and an error rate of  $4 \times 10^{-8}$ , our algorithm has about 0.85 dB, 1.75 dB and 2.5 dB coding gains over the Gauss, KV and Berlekamp-Massey algorithms respectively. Simulation results for a cost of  $10^4$  also show the potential of our algorithm over previously proposed ones.

## REFERENCES

- [1] V. Guruswami and M. Sudan, “Improved decoding of Reed-Solomon codes and algebraic geometry codes,” *IEEE Trans. Inform. Theory*, vol. 45, no. 6, pp. 1757–1767, Sept. 1999.
- [2] R. Kötter and A. Vardy, “Algebraic soft-decision decoding of Reed-Solomon codes,” *IEEE Trans. Inform. Theory*, vol. 49, no. 11, pp. 2809–2825, Nov. 2003.
- [3] F. Parvaresh and A. Vardy, “Multiplicity assignments for algebraic soft-decoding of Reed-Solomon codes,” in *Proc. ISIT*, 2003.
- [4] N. Ratnakar and R. Kötter, “Exponential error bounds for algebraic soft-decision decoding of Reed-Solomon codes,” submitted to *IEEE Trans. Inform. Theory*.