

More Efficient Algebraic Decoder with Larger Error Correction Radii for q -ary Reed-Muller and Product-Reed-Solomon Codes

Nandakishore Santhi*

Abstract— We consider a list decoding algorithm recently proposed by Pellikaan-Wu [4] for q -ary Reed-Muller codes $\mathcal{R}_q(\ell, m, n)$ of length $n \leq q^m$ when $\ell \leq q$. A simple and easily accessible correctness proof is given which shows that this algorithm achieves a relative error-correction radius of $\tau \leq \left(1 - \sqrt{\ell q^{m-1}/n}\right)$. This is an improvement over the proof using one-point Algebraic-Geometric decoding method given in [4]. The described algorithm can be adapted to decode product Reed-Solomon codes.

We then propose a new low complexity recursive algebraic decoding algorithm for product Reed-Solomon codes and Reed-Muller codes. Our algorithm achieves a relative error correction radius of $\tau \leq \prod_{i=1}^m \left(1 - \sqrt{k_i/q}\right)$. This technique is then proved to outperform the Pellikaan-Wu method in both complexity and error correction radius over a wide range of code rates.

I. INTRODUCTION TO CODES

Error correction codes are ubiquitous - they find use in DVDs, CDROMs, computer hardware, communication systems, space etc. Codes provide protection to valuable data against errors introduced as a result of a natural degradation or adversarial action.

A q -ary linear error-correction code $\mathbb{C}[n, k, d]$ of length n and dimension k is just a k -dimensional subspace of the n -dimensional vector space \mathbb{F}_q^n over the finite field \mathbb{F}_q . So, $\mathbb{C}[n, k, d] \subset \mathbb{F}_q^n$. The *minimum Hamming distance* d of the code is the least number of positions in which any two of its vectors differ. In typical applications, the larger the minimum distance, the better the code. Also we represent information sequences with corresponding codewords and wish to recover those codewords corrupted by noise: $\mathbf{r} = \mathbf{c} + \mathbf{e}$, where $\mathbf{c} \in \mathbb{C}$. See Figure 1.

II. SIMPLIFIED PROOF FOR PELLIKAAN-WU ALGORITHM AND SCHWARTZ LEMMA

Reed-Solomon codes are a very important family of codes with $d = n - k + 1$. Reed-Muller codes and Product-Reed-Solomon codes can be thought of as related derivative codes. Let $\rho = k/n$ denote the code rate. Various algebraic Reed-Solomon decoders due to Berlekamp et al.[1960s] can decode any error pattern of weight less than $n \cdot (1 - \rho)/2$. Recent progress made by Sudan[1997] and Guruswami-Sudan[1999] resulted in an algebraic list decoder for RS codes which can correct any error pattern of weight less than $n \cdot (1 - \sqrt{\rho})$. All these decoders are instances of bounded distance algebraic decoders, with guaranteed error correction radius which is efficiently achievable. See Figure 2.

With the discovery of deterministic list-decoding algorithms for several Algebraic-Geometric codes, most notably the Guruswami-Sudan [2] algorithm, there has been renewed interest in algebraic

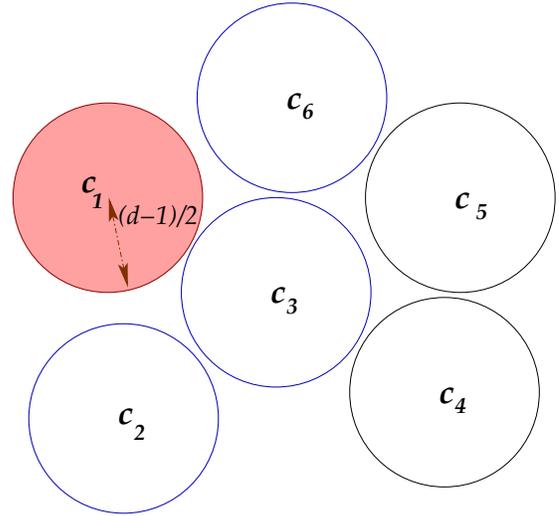


Figure 1: In principle any error of weight upto $\frac{d-1}{2}$ can be corrected.

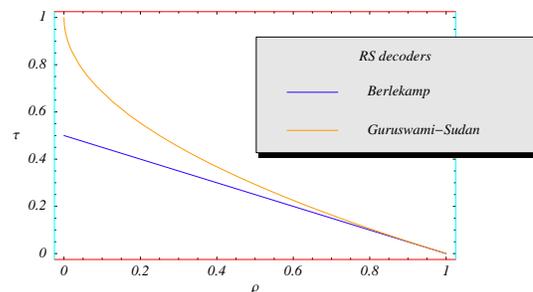


Figure 2: Comparison of bounded distance algebraic decoders for RS codes. τ is the relative error correction radius.

decoding methods for other related q -ary codes such as the Reed-Muller [3], [4] and product Reed-Solomon codes. However some of the existing correctness proofs for these algorithms use advanced algebraic geometric tools. In this research we derive a proof for a list decoding algorithm for a q -ary Reed-Muller code. Our proof is from first principles and require only the most basic notions from finite field theory.

The basic idea of our proof is to “lift” a multivariate polynomial in $\mathbb{F}_q[x_1, x_2, \dots, x_m]$ to a univariate polynomial in $\mathbb{F}_q[X]$ using a deterministic mapping rule. This in turn results in a higher total degree polynomial. The increase in degree will not be high enough to render our list decoding strategy for Reed-Muller codes useless at meaningful rates. A higher degree for the lifted polynomial means that this Reed-Muller code list decoding algorithm has a lower relative error-correction radius (as a function of the rate) than a

* The author is affiliated to the T-13 Complex Systems Group, the Center for Non-Linear Studies, and the CCS-3 division at the Los Alamos National Laboratory, Los Alamos, NM 87544, nsanthi@lanl.gov. Document #: LA-UR-07-0469. This document summarizes the work to be presented during the IEEE International Symposium on Information Theory (ISIT), Nice, France, June 2007.

comparable rate Reed-Solomon list decoder based on the Guruswami-Sudan algorithm.

A. Some Considerations on our results

The complexity of our proposed algorithm is of the same order as the complexity of Guruswami-Sudan algorithm for decoding Reed-Solomon codes over the extension field \mathbb{F}_{q^m} . This is $\mathcal{O}(n^3)$ field operations in \mathbb{F}_{q^m} .

Product-Reed-Solomon code $\mathcal{PRS}_{q,m}(q^m, k_1, \dots, k_m)$ is contained in $\mathcal{RM}_q(\sum_{i=1}^m (k_i - 1), m, q^m)$. When $\sum_{i=1}^m (k_i - 1) \leq q$ the list decoding we consider can be used to achieve a relative error correction radius of $(1 - \sqrt{\sum_{i=1}^m \rho_i})$, where $\rho_i \stackrel{\text{def}}{=} k_i/q$.

We also give a simple deterministic proof for the famous DeMillo-Lipton-Schwartz-Zippel lemma for polynomials over finite fields. Note that the statement above appears to be stronger than the classical lemma in that this counts multiplicities too. Moreover the proof also appears to differ from the traditional expositions which use probabilistic arguments.

III. A RECURSIVE DECODING ALGORITHM FOR PRODUCT REED-SOLOMON AND REED-MULLER CODES

Having given a simplified proof for the recently proposed, leading algebraic decoder for Reed-Muller and Product-Reed-Solomon codes, we then go ahead to propose two new algorithms for decoding product Reed-Solomon codes and Reed-Muller codes. We show that these new algorithms perform better than the Pellikaan-Wu algorithm in both complexity as well as decoding capability.

We have the following result concerning the decoding power of our new algorithms.

Theorem 1 *Our new PRS decoder has a relative error correction radius of $\tau_m \stackrel{\text{def}}{=} \prod_{i=1}^m (1 - \sqrt{\rho_i})$, where $\rho_i \stackrel{\text{def}}{=} k_i/q$. Moreover, there exist error patterns of weight above $n \prod_{i=1}^m (1 - \sqrt{\rho_i})$ which cannot be guaranteed to be efficiently decoded by the new algorithm.*

A. Considerations on our newly proposed decoders

The complexity of our new RM decoder is $\approx \mathcal{O}(n^2)$ field operations in \mathbb{F}_q . This is substantially better than the Pellikaan-Wu method. For PRS decoding our new algorithm achieves a nearly linear complexity.

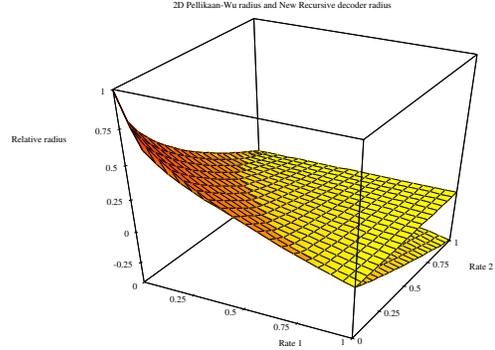
Our new algorithms not only have a lower complexity, but also perform better over a wide range of rates. For example when $\sum_i \rho_i > 1$, the Pellikaan-Wu algorithm is not effective, whereas our new algorithm is still very useful. Furthermore $\prod_{i=1}^m (1 - \sqrt{\rho_i})$ is larger than $(1 - \sqrt{\sum_{i=1}^m \rho_i})$ for most code rates and the advantage is more pronounced at higher code rates. See Figure 3.

The performance of several popular empirical iterative hard decision decoders for product Reed-Solomon codes available in literature can be characterized using Theorem 1. Essentially similar conclusions are also obvious for the case of other product codes which have algebraic bounded distance decoders available for their component codes.

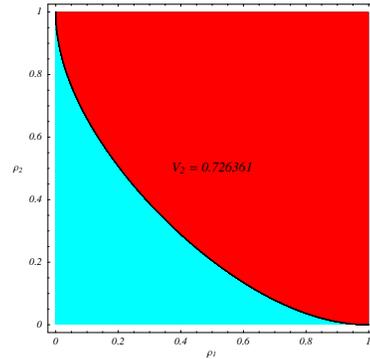
IV. CONCLUSIONS

In this work, we presented a simple and easily accessible proof for the Pellikaan-Wu algebraic decoding algorithm for Reed-Muller codes. Our proof uses only the fundamental properties of finite field arithmetic.

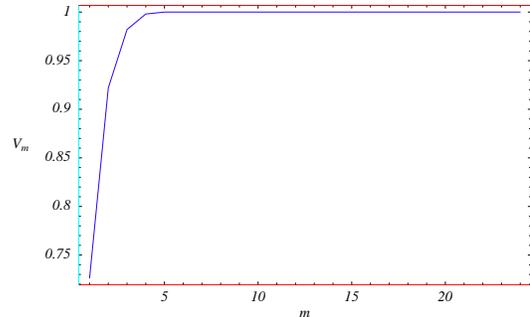
We also proposed a low complexity recursive algorithm for Reed-Muller and Product-Reed-Solomon codes. We further showed that the new algebraic algorithm has a significantly better error correction radius than the Pellikaan-Wu algorithm over a wide range of code rates.



(a) 2D radii of the two algorithms.



(b) 2D rate region where our algorithm performs better is shown in red.



(c) Relative rate region volume where our algorithm performs better is computed. The new algorithm is seen to out-perform the Pellikaan-Wu algorithm over most of the rate region.

Figure 3: Comparison of Pellikaan-Wu versus our new recursive RM/PRS decoder.

REFERENCES

- [1] R. Lidl and H. Niederreiter, *Introduction to finite fields and their applications*, University of Cambridge Press, Cambridge, 1986.
- [2] V. Guruswami and M. Sudan, "Improved Decoding of Reed-Solomon and Algebraic-Geometry Codes," *IEEE Trans. Inform. Theory*, **45**, No. 6, pp. 1757-1767, Sep. 1999.
- [3] R. Pellikaan and X.-W. Wu, "List Decoding of q -ary Reed-Muller Codes," *IEEE Trans. Inform. Theory*, **50**, No. 4, pp. 679-682, Apr. 2004.
- [4] R. Pellikaan and X.-W. Wu, "List Decoding of q -ary Reed-Muller Codes," Expanded version of [3], manuscript available at <http://www.win.tue.nl/~ruudp/paper/43-exp.pdf>, Nov. 2005.