Title: On Algebraic Decoding of q-ary Reed-Muller and Products Reed-Solomon Codes

Author(s): Nandakishore Santhi, 221302, T-13

Intended for: ISIT 2007 Conference
June 24-29, 2007
Nice, France

On Algebraic Decoding of 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 $\mathcal{RM}_q(\ell,\, m,\, n)$ of length $n \le q^m$ when $\ell \le q$. A simple and easily accessible correctness proof is given which shows that this algorithm achieves a relative error-correction radius of $\tau \le \left(1 - \sqrt{\ell q^{m-1}/n}\right)$. 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. This algorithm achieves a relative error correction radius of $\tau \le \prod_{i=1}^{m} \left(1 - \sqrt{k_i/q}\right)$. This algorithm is then proved to outperform the Pellikaan-Wu algorithm in both complexity and error correction radius over a wide range of code rates.

I. Introduction

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 decoding methods for other related q-ary codes such as the Reed-Muller [3], [4] and product Reed-Solomon [5] codes. However some of the existing correctness proofs for these algorithms use advanced algebraic geometric tools. In this paper 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 $\mathbb{F}_q[x_1, x_2, \ldots, x_m]$ to a univariate polynomial in $\mathbb{F}_{q^m}[X]$ 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 comparable rate Reed-Solomon list decoder based on the Guruswami-Sudan algorithm. In the following section we describe the mapping rule and the decoding algorithm in some detail.

In the final section we propose new algorithms for decoding product Reed-Solomon codes and Reed-Muller codes. We then show that this new algorithm performs better than the Pellikaan-Wu algorithm in both complexity as well as decoding capability.

II. Correctness of a List Decoding Algorithm

Let us begin by defining a q-ary Reed-Muller code.

Definition 1 *The q-ary Reed-Muller code $\mathcal{RM}_q(\ell,\, m,\, n)$ of length $n \le q^m$ is defined as the set of vectors given by:*

$$\mathcal{RM}_q(\ell,\, m,\, n) \overset{\text{def}}{=} \{\ [\varphi(\alpha_1)\ \varphi(\alpha_1)\ \cdots\ \varphi(\alpha_n)]\\ \mid\ \varphi \in \mathbb{F}_q[x_1, x_2, \ldots, x_m],\ \deg(\varphi) \le \ell\ \} \qquad (1)$$

where $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ are any set of n distinct points in $\mathbb{F}_q^m$. Here by $\deg(\varphi)$ we mean the total degree of the multivariate polynomial φ.

The following well known property will be useful:

Proposition 1 *Let $\{a_1, a_2, \ldots, a_m\}$ be a basis for $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ and let $[x_1 x_2 \ldots x_m] \in \mathbb{F}_q^m$. Then the map $\psi : \mathbb{F}_q^m \to \mathbb{F}_{q^m}$ defined as in (2) is an isomorphism.*

$$[x_1 x_2 \ldots x_m] \mapsto X \overset{\text{def}}{=} \sum_{j=1}^{m} a_j x_j \qquad (2)$$

For example one might as usual use a polynomial basis $\{1, \xi, \xi^2, \ldots, \xi^{m-1}\}$ where ξ is any primitive element in $\mathbb{F}_{q^m}$ or even a normal basis of the form $\{\zeta, \zeta^q, \zeta^{q^2}, \ldots, \zeta^{q^{m-1}}\}$, where ζ is a suitable primitive element in $\mathbb{F}_{q^m}$.

Therefore we arrive at this elementary conclusion:

Lemma 1 *Let $X \in \mathbb{F}_{q^m}$. The reverse isomorphism for (2) is:*

$$X \mapsto [x_1 x_2 \ldots x_m]^T \overset{\text{def}}{=} \boldsymbol{A}^{-1} \cdot [X\, X^q\, X^{q^2}\, \ldots\, X^{q^{m-1}}]^T \qquad (3)$$

where

$$\boldsymbol{A} \overset{\text{def}}{=} \begin{bmatrix} a_1 & a_2 & \ldots & a_m \\ a_1^q & a_2^q & \ldots & a_m^q \\ \vdots & \vdots & \ddots & \vdots \\ a_1^{q^{m-1}} & a_2^{q^{m-1}} & \ldots & a_m^{q^{m-1}} \end{bmatrix} \qquad (4)$$

is a non-singular (invertible) square matrix.

Proof: Since $X = \sum_{j=1}^{m} a_j x_j$, and $x_j \in \mathbb{F}_q$, we get $X^{q^i} = \sum_{j=1}^{m} a_j^{q^i} x_j$ using Fermat's little theorem. It only remains to show that $\boldsymbol{A}$ is non-singular. By construction, the set $\{a_1, a_2, \ldots, a_m\}$ is a basis for $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. It then follows from [1, Corollary 2.38, pp. 58] that $\boldsymbol{A}$ is non-singular. ■

It follows from Lemma 1 that there exist polynomials $\mu_j \in \mathbb{F}_{q^m}[X]$ of degree at most q^{m-1} such that $x_j = \mu_j(X), 1 \le j \le m$.

* The author is affiliated to the T-13 Complex Systems Group, the Center for Non-Linear Studies, and the CCS-5 division at the Los Alamos National Laboratory, Los Alamos, NM 87544, nsanthi@lanl.gov

Substituting for all x_j in this manner, we have proved the following:

Theorem 1 *Let $n \leq q^m$. If $\ell \leq q$ then*

$$\mathcal{RM}_q(\ell,\, m,\, n) \subseteq \mathcal{RS}_{q^m}(n,\, \ell q^{m-1}) \cap \mathbb{F}_q^n \tag{5}$$

where $\mathcal{RS}_{q^m}(n,\, \ell q^{m-1})$ is the Reed-Solomon code given by

$$\begin{aligned}\mathcal{RS}_{q^m}(n,\, \ell q^{m-1}) \overset{\text{def}}{=} \{\ &[f(\beta_1)\, f(\beta_2)\, \dots\, f(\beta_n)] \\ &\mid\ f \in \mathbb{F}_{q^m}[X],\, \deg(f) \leq \ell q^{m-1}\ \}\end{aligned} \tag{6}$$

where $\beta_i \overset{\text{def}}{=} \sum_{j=1}^{m} a_j \alpha_{ij}$, and $\boldsymbol{\alpha}_i \overset{\text{def}}{=} [\alpha_{i1}\, \alpha_{i2}\, \dots\, \alpha_{im}]$, $1 \leq i \leq n$ are the points of evaluation for the Reed-Muller code. Moreover if the information polynomial associated with the Reed-Muller code is given by

$$\varphi(x_1, x_2, \dots, x_m) \overset{\text{def}}{=} \sum_{\substack{i_1, i_2, \dots, i_m: \\ \sum_j i_j \leq \ell}} \varphi_{i_1, i_2, \dots, i_m} \prod_{j=1}^{m} x_j^{i_j} \tag{7}$$

then the information polynomial f of degree at most ℓq^{m-1} associated with the Reed-Solomon code is:

$$f(X) = \sum_{\substack{i_1, i_2, \dots, i_m: \\ \sum_j i_j \leq \ell}} \varphi_{i_1, i_2, \dots, i_m} \prod_{j=1}^{m} (\mu_j(X))^{i_j} \tag{8}$$

Let $d_H(\boldsymbol{x},\, \boldsymbol{y})$ represent the Hamming distance between the two vectors. Using Theorem 1 and the Guruswami-Sudan algorithm [2] for list decoding a Reed-Solomon code, we have proved the correctness of the following deterministic list-decoding algorithm for Reed-Muller codes:

```
Algorithm 1 (RM-List-1)
INPUT: $q, \ell \leq q, m, n \leq q^m$; $\boldsymbol{r} = [r_1\ r_2\ \dots\ r_n] \in \mathbb{F}_q^n$.
STEPS:
1. Compute the parameter $t = \left\lceil n\left(1 - \sqrt{\ell q^{m-1}/n}\right)\right\rceil$.
2. Using Guruswami-Sudan algorithm find a list $\mathcal{L}$ of code-
   words $\boldsymbol{c} \in \mathcal{RS}_{q^m}(n,\, \ell q^{m-1})$ such that $d_H(\boldsymbol{c}, \boldsymbol{r}) < t$.
3. For every $\boldsymbol{c} \in \mathcal{L}$ check if $\boldsymbol{c} \in \mathbb{F}_q^n$ :
     i. If NO then discard $\boldsymbol{c}$ from $\mathcal{L}$.
     ii. If YES then check if $\boldsymbol{c} \in \mathcal{RM}_q(\ell,\, m,\, n)$ :
         a. If NO then discard $\boldsymbol{c}$ from $\mathcal{L}$.
         b. If YES then keep $\boldsymbol{c}$ in the list $\mathcal{L}$.
4. return
OUTPUT: $\mathcal{L}$
```

This algorithm was originally proposed by Pellikaan-Wu in [4], though their proofs were different.

A. Complexity of Algorithm 1

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 $O(n^3)$ field operations in $\mathbb{F}_{q^m}$.

B. Comparison to previous results

The Pellikaan-Wu algorithm for decoding Reed-Muller codes by means of embedding into one-point Algebraic-Geometric codes was shown [4] to achieve an error correction radius of $\left\lceil n\left(1 - \sqrt{\ell(q+1)^{m-1}/n}\right)\right\rceil$. It is interesting to note that the error-correction radius demonstrated herein is always larger than that suggested by the Pellikaan-Wu formalism employing Algebraic-Geometric codes. However we believe that the more important contribution of this paper is the readily accessible correctness proof which relies on just a few basic notions from Galois theory.

C. Product Reed-Solomon codes

Product Reed-Solomon codes $\mathcal{PRS}_{q,m}(q^m,\, k_1, \dots, k_m) \overset{\text{def}}{=} \otimes_{i=1}^{m} \mathcal{RS}_q(q,\, k_i)$ over $\mathbb{F}_q^m$ can be thought of as the set of vectors whose q^m coordinates consist of the q^m evaluations of m-variate information polynomials with coefficients in $\mathbb{F}_q$ and degree in the i^{th}-variable x_i at most $(k_i - 1)$. m is usually called the dimension of the product code. Thus $\mathcal{PRS}_{q,m}(q^m,\, k_1, \dots, k_m)$ 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 algorithm given in Algorithm 1 may be used essentially without any modifications. Several product Reed-Solomon algebraic list decoders, including a similar method as sketched above are described in [5]. Using Algorithm 1 it is possible to achieve a relative error correction radius of $(1 - \sqrt{\sum_{i=1}^{m} \rho_i})$, where $\rho_i \overset{\text{def}}{=} k_i/q$.

D. Zeros of Multivariate Polynomials

From Theorem 1, it is clear that $f(X)$ being of degree at most ℓq^{m-1}, has at most ℓq^{m-1} zeros in $\mathbb{F}_{q^m}$, including multiplicities. Therefore a non-zero multivariate polynomial $\varphi(x_1, x_2, \dots, x_m)$ of total degree ℓ has at most ℓq^{m-1} zeros in $\mathbb{F}_q^m$. This gives 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.

Next we propose a lower complexity recursive algebraic decoder which outperforms the Reed-Muller decoder considered in this section.

III. A Recursive Decoding Algorithm for Product Reed-Solomon and Reed-Muller Codes

For simplicity, let $n \overset{\text{def}}{=} q^m$. A codeword in the code $\mathcal{PRS}_{q,m}(q^m,\, k_1, \dots, k_m)$ can be described within an m-dimensional cube of side length q. Let a codeword $\boldsymbol{c}$ (correspondingly a received word, $\boldsymbol{r}$) be so described. We will find it convenient to write this vector as $[\boldsymbol{c}_{i_1, i_2, \dots, i_m}]$, where each of the indices i_j take values in the range $\{1, \dots, q\}$. We further use the notation $[\boldsymbol{c}_{i_1, i_2, \dots, i_{j-1}}^{a_j, a_{j+1}, \dots, a_m}]$ to denote the $(j-1)$-dimensional vector formed out of $[\boldsymbol{c}_{i_1, i_2, \dots, i_m}]$ when the coordinates indexed by $(i_j, i_{j+1}, \dots, i_m)$ are fixed at $(a_j, a_{j+1}, \dots, a_m)$ and the rest of the indices are free. By the nature of the product code, $[\boldsymbol{c}_{i_1, i_2, \dots, i_{j-1}}^{a_j, a_{j+1}, \dots, a_m}]$ belongs to $\mathcal{PRS}_{q,j-1}(q^{j-1},\, k_1, \dots, k_{j-1})$.

Now consider the following decoding algorithm for the code $\mathcal{PRS}_{q,m}(q^m, k_1, \ldots, k_m)$:

Algorithm 2 (PRS-Decoder)

```
INPUT: $q, (k_1, k_2, \ldots, k_m) : k_i < q, m;\ \boldsymbol{r} \in \mathbb{F}_q^n$, where $\boldsymbol{r} \overset{\text{def}}{=} [r_{i_1,i_2,\ldots,i_m}]; 1 \le i_j \le q$.
STEPS:
1. If $m = 1$ do:
    i. Compute the parameter $t_1 = \left\lceil q\left(1 - \sqrt{k_1/q}\right)\right\rceil$.
    ii. Using Guruswami-Sudan algorithm find a list $\mathcal{L}_1$ of codewords $\boldsymbol{c}_1 \in \mathcal{RS}_q(q, k_1)$ such that $d_H(\boldsymbol{c}_1, \boldsymbol{r}_{i_1}) < t_1$.
    iii. Search $\mathcal{L}_1$ for $\boldsymbol{c}_1$ such that $d_H(\boldsymbol{c}_1, \boldsymbol{r}_{i_1})$ is least. Substitute in-place the positions corresponding to $\boldsymbol{r}_{i_1}$ in $\boldsymbol{r}$ with $\boldsymbol{c}_1$ and return .
2. For $a_m = 1, 2, \ldots, q$ do:
    i. Set $\boldsymbol{r}' \leftarrow [\boldsymbol{r}^{a_m}_{i_1,i_2,\ldots,i_{m-1}}]$
    ii. Set $m' \leftarrow m - 1$ and $n' \leftarrow q^{m'}$
    iii. Recursively decode $\boldsymbol{r}'$ using PRS-Decoder with input parameters $q, (k_1, k_2, \ldots, k_{m'}), m';\ \boldsymbol{r}' \in \mathbb{F}_q^{n'}$.
3. Compute the parameter $t_m = \left\lceil q\left(1 - \sqrt{k_m/q}\right)\right\rceil$.
4. For each $m - 1$ tuple $(a_1, a_2, \ldots, a_{m-1})$ do:
    i. Using Guruswami-Sudan algorithm find a list $\mathcal{L}_m$ of codewords $\boldsymbol{c}_m \in \mathcal{RS}_q(q, k_m)$ such that $d_H(\boldsymbol{c}_m, \boldsymbol{r}^{a_1,a_2,\ldots,a_{m-1}}_{i_m}) < t_m$.
    ii. Search $\mathcal{L}_m$ for $\boldsymbol{c}_m$ such that $d_H(\boldsymbol{c}_m, \boldsymbol{r}^{a_1,a_2,\ldots,a_{m-1}}_{i_m})$ is least. Substitute in-place the positions corresponding to $\boldsymbol{r}^{a_1,a_2,\ldots,a_{m-1}}_{i_m}$ with $\boldsymbol{c}_m$.
5. return
OUTPUT: Resulting vector $\boldsymbol{r}$
```

The following recursive algorithm uses **PRS-Decoder** to decode $\mathcal{RM}_q(\ell, m, n)$.

Algorithm 3 (RM-List-2)

```
INPUT: $q, \ell \le q, m, n \le q^m;\ \boldsymbol{r} = [r_1\ r_2\ \ldots\ r_n] \in \mathbb{F}_q^n$.
STEPS:
1. For each possible m-tuple $(k_1, k_2, \ldots, k_m) : k_i < q, \sum_j k_j \le \ell$ do:
    i. Using PRS-Decoder with input parameters $q, (k_1, k_2, \ldots, k_m), m;\ \boldsymbol{r} \in \mathbb{F}_q^n$, decode $\boldsymbol{r}$ as $\boldsymbol{c}$.
    ii. Add $\boldsymbol{c}$ to a list $\mathcal{L}$ of codeword candidates.
2. return
OUTPUT: $\mathcal{L}$
```

We have the following result concerning the decoding power of Algorithm 2 and Algorithm 3.

Theorem 2 *Algorithm 2 has a relative error correction radius of* $\tau_m \overset{\text{def}}{=} \prod_{i=1}^m (1 - \sqrt{\rho_i})$, *where* $\rho_i \overset{\text{def}}{=} k_i/q$. *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 Algorithm 2.*

Proof: Our proof is by induction. When $m = 1$, the claim is trivially true. Let us assume the claim to be true for some $m = M$. We will now show it to be true for the case $m = M + 1$. Let there be a maximum of $t_{M+1} = q^{M+1}\prod_{i=1}^{M+1}(1 - \sqrt{\rho_i})$ errors. In Step 2 of Algorithm 2, let there be a maximum of x recursions which fail to decode correctly. Since by the induction hypothesis, this would mean that there are more than t_M errors in these x sub-recursions, we have that $x t_M \le t_{M+1}$. Substituting for t_{M+1} and t_M gives, $x \le q(1 - \sqrt{\rho_{M+1}})$. These errors will get corrected in Step 4 of the algorithm. This proves the first part of the claim.

To see the second part of the claim, we observe that an error pattern which is contiguously spread over an m dimensional sub-cube of volume more than $n\prod_{i=1}^m (1 - \sqrt{\rho_i})$ cannot be guaranteed to be efficiently decoded by the proposed algorithm. This shows that the error correction radius predicted by Theorem 2 is rather tight. ■

A. Complexity of Algorithm 2 and Algorithm 3

Let ϑ_m be the complexity of decoding an m-dimensional product Reed-Solomon Code using Algorithm 2. Then the complexity of decoding an $m+1$ dimensional code is $\vartheta_{m+1} = O(q\vartheta_m + q^m\vartheta_1)$. But $\vartheta_1 = O(q^3)$ field operations in $\mathbb{F}_q$. This gives, $\vartheta_m = O(q^{m+2})$ which is $\approx O(n)$ for large m. The complexity of Algorithm 3 is $\approx O(n^2)$ field operations in $\mathbb{F}_q$. This is substantially better than the Pellikaan-Wu method in Algorithm 1.

B. Comparison of Algorithm 1 and Algorithm 3

Algorithm 3 not only has a lower complexity, but also performs better over a wide range of rates. For example when $\sum_i \rho_i > 1$, the Pellikaan-Wu algorithm is not effective, whereas the new algorithm is still 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.

C. Other Related Product Code Decoders

Several iterative hard decision decoders for product Reed-Solomon codes available in literature use some form of Algorithm 2. The performance of such iterative decoders can also be characterized using Theorem 2. Similar conclusions are obvious for the case of other product codes which have algebraic bounded distance decoders available for their component codes.

IV. Conclusions

In this paper, we present 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 propose a low complexity recursive algorithm for product Reed-Solomon and Reed-Muller codes. This new algebraic algorithm is then shown to have a significantly better error correction radius than the Pellikaan-Wu algorithm over a wide range of code rates.

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.

[5] F. Parvaresh, M. El-Khamy, R. J. McEliece and A. Vardy, "Algebraic List-decoding of Reed-Solomon Product Codes," Unpublished note of Jan. 2006, private communication.