Algebraic List Decoding of Reed-Solomon product codes

Farzad Parvaresh[*], Mostafa El-Khamy[†], Michael Stepanov[‡]
Daniel Augot[§], Robert J. McEliece[†] and Alexander Vardy[*]

Abstract

The product code of two Reed-Solomon codes can be regarded as an evaluation codes of bivariate polynomials, whose degrees in each variable are bounded. We propose to decode these codes with a generalization of the Guruswami-Sudan interpolation-based list decoding algorithm. A relative decoding radius of $1 - \sqrt[6]{4R}$ is found, where is the rate of the product code. We also discuss a generalization to the M variables base, where we get a figure of $1 - \sqrt[M(M+1)]{R}$. Finally the Pellikaan and Wu decoding algorithm is used to improve the decdoing radius.

1 Introduction

The product code $C_1 \otimes C_2$ of two codes C_1 and C_2 is the set of matrices whose every row belongs to C_1 and every column belong to C_2. In the case when C_1 is a Reed-Solomon code of dimension k_1, minimum distance $d_1 = n - k_1 + 1$, defined as an evaluation code over the set $A = \{\alpha_1, \ldots, \alpha_{n_1}\} \subset \mathbb{F}_q$ and and C_2 a Reed-Solomon code of dimension k_2, minimum distance d_2, defined as an evaluation code over the set $B = \{\beta_1, \ldots, \beta_{n_2}\} \subset \mathbb{F}_q$, we get an evaluation code defined by the evaluation map:

$$\begin{array}{rccl} \mathrm{ev}^2: & \mathbb{F}_q[X,Y] & \rightarrow & (\mathbb{F}_q)^{n_1 n_2} \\ & f(X,Y) & \mapsto & (f(\alpha_i, \beta_j), (i,j) \in \{1 \ldots n_1\} \times \{1 \ldots n_2\}) \,. \end{array}$$

And the code is defined as

$$C_1 \otimes C_2 = \mathrm{ev}^2(L)$$

where

$$L = \{f \in \mathbb{F}_q[X,Y], \deg_X f < k_1 \text{ and } \deg_Y f < k_2\} \,.$$

[*]University of California San Diego, {fparvaresh,avardy}@ ucsd.edu
[†]California Institute of Technology, {mostafa,rjm}@ systems.caltech.edu
[‡]St Petersburg State University of Aerospace Instrumentation, mike@catalina.spb.ru
[§]INRIA, Project-Team CODES, Daniel.Augot@inria.fr

This code has dimension $k_1 k_2$ and minimum distance $d_1 d_2$. A polynomial in L has the form

$$f = \sum_{i=0}^{k_1'} \sum_{j=0}^{k_2'} f_{i,j} X^i Y^j,$$

where $k_1' = k_1 - 1$ and $k_2' = k_2 - 1$. We also defines the rates $R_1 = \frac{k_1}{n_1}$ and $R_2 = \frac{k_2}{n_2}$, and $R = R_1 R_2$ is the rate of the product code.

It is well known that the half the distance bound is not always attainable by iteratively decoding the component codes. For example, if the decoding algorithms for the row and column component codes are capable of correcting $(d_1 - 1)/2$ and $(d_2 - 1)/2$ errors respectively, and an error rectangular block of $((d_1 - 1)/2 + 1)((d_2 - 1)/2 + 1)$ occurs, iterative decoding fails although the number of errors is less than or equal to $(d_1 d_2 - 1)/2$. Thus it is natural to wonder wether the algebraic list-decoding algorithms [1] can be generalized to these codes. This is furthermore motivated by another multivariate generalization, which gives a very high decoding radius [3, 2]

2 The algorithm and its analysis

We need this preliminary Theorem, stated withour proof, before introducing the algorithm.

Theorem 1 *The number of zeros, counted with multiplicites, of a non zero polynomial $Q = Q(X, Y)$ over the set $\{(\alpha_i, \beta_j); (i, j) \in \{1 \dots n_1\} \times \{1 \dots n_2\}\}$ is bounded by $wdeg_{n_2, n_1} Q$.*

Let $y = (y_{i,j})_{(i,j) \in \{1 \dots n_1\} \times \{1 \dots n_2\}}$, be the word to be decoded. We want to recover codewords at distance t, or equivalently find those $f = f(X, Y) \in L$ such that

$$\mu = \#\{(i, j) | f(\alpha_i, \beta_j) = y_{i,j}\} \geq n_1 n_2 - t.$$

Similarly to the Guruswami-Sudan decoding algorithm, we will look for a polynomial with one more variable Y, $Q = Q(X, Y, X)$ such that

1. $Q \neq 0$
2. $\text{wdeg}_{n_1, n_2, n_1 k_2' + n_2 k_1'} Q < \Delta$, where d is auxiliary, to be determined
3. $\text{mult}(Q; (\alpha_i, \beta_j, y_{ij})) = m$, $(i, j) \in \{1 \dots n_1\} \times \{1 \dots n_2\}$, where m a parameter of the algorithm. Note at this is linear algebra problem, whose unknowns are the cofficients of Q.

We will show that if f is solution to the decoding problem, then $Q(X, Y, f) = 0$. We need three Lemmas to analyse the algorithm.

Lemma 1 *Let D be the (n_2, n_1)-weighted degree of $Q(X, Y, f)$. If $m\mu > D$, then $Q(X, Y, f) = 0$.*

Proof Direct consequence of Theorem 1.

Lemma 2 *The (n_2, n_1)-weighted degree of $Q(X, Y, f)$ is less than or equal to the $(n_1, n_2, k'_1 n_2 + k'_2 n_1)$-weighted degree of $Q(X, Y, Z)$.*

Lemma 3 *Let $Q = Q(X, Y, Z)$ be of $(n_1, n_2, n_1 k'_2 + n_2 k'_1)$-weighted degree less than Δ, than the number $N(\Delta)$ of monomials of Q satisfies*

$$N(\Delta) < \frac{1}{6} \frac{\Delta^3}{n_1 n_2 (n_1 k'_2 + n_2 k'_1)} \tag{1}$$

Theorem 2 *Assume that the distance between $y = y_{i,j}$ and evf is less than or equal to t. Then one construct a polynomial $Q(X, Y, Z)$ such that $Q(X, Y, f) = 0$, provided that*

$$t \leq \left\lfloor n_1 n_2 \left(1 - \sqrt[3]{(R_1 + R_2)(1 + \frac{1}{m})(1 + \frac{2}{m})} \right) - \frac{1}{m} \right\rfloor \tag{2}$$

Proof On one hand, to ensure that a non zero $Q(X, Y, Z)$, of $(n_1, n_2, n_1 k'_2 + n_2 k'_1)$-weighted degree Δ, can be found we must have (more unknowns than equations)

$$\frac{1}{6} \frac{\Delta^3}{n_1 n_2 (n_1 k'_2 + n_2 k'_1)} > n_1 n_2 \frac{m(m+1)(m+2)}{6} \tag{3}$$

On the other, to ensure that $Q(X, Y, f)$ is identically zero, one must have

$$m\mu = m(n_1 n_2 - t) > \Delta. \tag{4}$$

Combining these two inequalities gives (2).

3 The M variables case

One can work out the case of M variables. For simplicity, we assume that all the codes are the same, that is to say, we take C to be the Reed-Solomon code with support $S = \{\alpha_1, \ldots, \alpha_n\} \subset \mathbb{F}_q$, and dimension k, and we get

$$C^M = C \otimes C \otimes \ldots C = \bigotimes_{i=1}^{M} C.$$

The corresponding evaluation map is

$$\begin{array}{rccl} \mathrm{ev}^M : & \mathbb{F}_q[X_1, \ldots, X_M] & \rightarrow & (\mathbb{F}_q)^{n^M} \\ & f(X_1, \ldots, X_M) & \mapsto & (f(x_{i_1}, \ldots, x_{i_M}))_{(x_{i_1} \ldots, x_{i_M}) \in S^m} \end{array}$$

and the space L of polynomials to evaluate is:

$$L = \left\{ f \in \mathbb{F}_q[X_1, \ldots, X_M], \deg_{X_i} f < k;\ i \in \{1 \ldots m\} \right\}.$$

We get

Theorem 3 *Let the received word be* $y = y_{i_1,\ldots,i_M} \in \mathbb{F}_q^{n^M}$, *and let* $f = f(X_1, \ldots, X_M)$ *be such that* $d(ev^M f, y) \leq t$, *then, provided that*

$$\frac{t}{n^M} \leq 1 - \sqrt[M+1]{\frac{M^{M+1}}{M!} \cdot R \cdot (1 + \frac{1}{m}) \cdots (1 + \frac{M}{m})}$$

then one can construct a polynomial $Q(X_1, \ldots, X_M, Y)$ *such that* $Q(X_1, \ldots, X_m, f) = 0$.

4 Decoding with Pellikaan-Wu interpretation

Let us consider the q-ary Reed-Muller code, with m variables, of order r, with $r < q$, denoted $\mathrm{RM}_q(r, m)$. It is defined by the same evaluation map ev^M, but the space L of polynomials to evaluate

$$L = \{f \in \mathbb{F}_q[X_1, \ldots, X_M];\ \deg f \leq r\},$$

where deg denotes the total degree.

We consider the decoding algorithm of Pellikaan and Wu [4], based on the interpretation of (shortened) Reed-Muller as cyclic codes. They show that it is possible to decode up to $q^n \left(1 - \sqrt{\frac{r}{q}}\right)$

One can see that, when $\{\alpha_1 \ldots, \alpha_{n_1}\} = \{\beta_1, \ldots, \beta_{n_1}\} = \mathbb{F}_q$, the code $C_1 \otimes C_2$ is a subcode of $\mathrm{RM}(k_1 + k_2, 2)$. Applying the Pellikaan-Wu algorithm, we get a decoding radius of

$$t < q^2 \left(1 - \sqrt{R_1 + R_2}\right).$$

For the M-variable case, the code C^m is a subcode of $\mathrm{RM}_q(R_1 M, m)$, and we get a decoding radius of $t < q^M \left(1 - \sqrt{M R_1}\right)$.

References

[1] Venkatesan Guruswami and Madhu Sudan. Improved decoding of Reed-Solomon and algebraic-geometry codes. *IEEE Transactions on Information Theory*, 45(6):1757–1767, 1999.

[2] Farzad Parvaresh and Alexander Vardy. Correcting errors beyond the Guruswami-Sudan radius in polynomial time. In *Proceeddings of the 46th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2005)*, pages 285–294, 2005.

[3] Farzad Parvaresh and Alexander Vardy. Multivariate interpolation decoding beyond the Guruswami-Sudan radius. In *Allerton Conference on Communication, Control and Computing*. CDROM only, 2005. available from authors.

[4] Ruud Pellikaan and Xin-Wen Wu. List decoding of q-ary Reed-Muller codes. *IEEE Transactions on Information Theory*, 50(4):679–682, 2004.