On Multivariate Interpolation Decoding of Folded Reed-Solomon codes [1]

Peter Trifonov petert@dcn.ftk.spbstu.ru
Saint-Petersburg State Polytechnic University

Abstract. The problem of list decoding of folded Reed-Solomon codes is considered. A generalization of the Wu list decoding algorithm to the case of multivariate interpolation decoding is proposed. The reformulated algorithm achieves higher error correction capability than the one of Guruswami-Rudra.

1 Introduction

Reed-Solomon codes are widely used in modern communication and storage systems. Recently, there was a great interest to list decoding of these codes. After the introduction of the Guruswami-Sudan algorithm [3], which was able to correct up to $t_{GS} = \lfloor n - \sqrt{n(k-1)} \rfloor$ errors in (n, k) RS code, numerous attempts were made to overcome this bound. In particular, it was shown by Guruswami and Rudra that one can recover up to a fraction $1 - R - \epsilon$ of errors in rate R folded RS code [2].

In this paper an alternative formulation of the multivariate decoding algorithm for folded RS codes is presented, which is based on Wu list decoding method [6] for conventional RS codes. The novel formulation enables one to achieve higher error correction capability in the case of high-rate codes compared to the case of Guruswami-Rudra algorithm.

The paper is organized as follows. The Guruswami-Rudra list decoding algorithm for folded RS codes is reviewed in Section 2. The generalization of the Wu algorithm to the case of folded RS codes is presented in Section 3. The numeric results are given in Section 4. Finally, some conclusions are drawn.

2 List decoding of folded Reed-Solomon codes

Let $\gamma \in \mathbb{F}$ be an element of order at least n. The m-folded RS code is a set of vectors $(c_0, \ldots, c_{N-1}), N = n/m$, where the symbols $c_j \in \mathbb{F}^m$ are m-tuples $c_j = (f(\gamma^{jm}), \ldots, f(\gamma^{jm+m-1})), \deg f(x) < k$. That is, m-folded RS code of length n/m is obtained from a conventional (n, k) RS code by considering m adjacent symbols in a codeword as a single one.

[1] This research is partially supported by the grant of the President of Russian Federation for young scientists MK-1195.2009.9.

List decoding of a folded RS code can be implemented using M-variate interpolation decoding. Let $(y_0, \ldots, y_{n-1})$ be an unfolded noisy vector to be decoded. The algorithm presented in [1] is based on construction of a polynomial $Q(X, Y_1, \ldots, Y_{M-1})$, such that the points

$$(\gamma^{jm+l}, y_{jm+l}, \ldots, y_{jm+l+M-1}), j = 0..n/m - 1, l = 0..m - M + 1 \tag{1}$$

are its roots of multiplicity r[2]. If $(1, k-1, \ldots, k-1)$-weighted degree of this polynomial is less than $D = \tau(m - M + 2)r$, then all polynomials $f(x)$ (i.e. codewords of the folded RS code), such that $\deg f(x) < k$, and $f(\gamma^{jm+l}) = y_{jm+l}, l = 0..m-1$, for at least τ distinct values of j satisfy $Q(x, f(x), f(\gamma x), \ldots, f(\gamma^{M-2}x)) = 0$.

The interpolation constraints for points given by (1) lead to $n\frac{m-(M-2)}{m}\binom{r+M-1}{M}$ linear equations. Obviously, the total degree of $Q(X, Y_1, \ldots, Y_{M-1})$ in Y_i cannot exceed $\rho = \lfloor (D-1)/(k-1) \rfloor$. Hence, the number of terms in the polynomial is given by

$$\tilde{N} = \sum_{j=0}^{\rho} \binom{j+M-2}{M-2}(D-(k-1)j) = \left(D - (k-1)\rho\frac{M-1}{M}\right)\binom{\rho+M-1}{M-1}.$$

If this value exceeds the number of interpolation constraints, then the coefficients of this polynomial can be recovered as a solution of the corresponding system of linear equations. That is, the parameters of the above described algorithm must satisfy

$$\left(D - (k-1)\rho\frac{M-1}{M}\right)\binom{\rho+M-1}{M-1} > n\frac{m-M+2}{m}\binom{r+M-1}{M} \tag{2}$$

It is possible to show that for sufficiently large r the Guruswami-Rudra algorithm can be used to correct a fraction of $\theta = \frac{n/m-\tau}{n/m}$ errors, provided that the code rate[3] satisfies

$$R < \frac{m-M+2}{m}\sqrt[M-1]{(1-\theta)^M}. \tag{3}$$

3 A multivariate generalization of the Wu algorithm

It was suggested in [6] to perform list decoding of RS codes by means of algebraic continuation of the classical Berlekamp-Massey algorithm. This method was reformulated in [4] using the language of Gröbner bases. We will adopt the latter approach, since it leads to simpler derivations.

[2] A polynomial $Q(X, Y_1, \ldots, Y_{M-1})$ has a root of multiplicity r at point $(x_0, y_0, \ldots, y_{M-1})$ if all its partial Hasse derivatives of total order $j_0 + \ldots + j_{M-1} < r$ are equal to zero.

[3] Here code rate is defined as $R = \frac{k-1}{n}$ in order to keep the notation consistent with [2].

The problem of decoding of RS codes (including folded ones) reduces to finding all pairs of polynomials $[\sigma(x), f(x)]$, such that

$$\sigma(\gamma^i)f(\gamma^i) = y_i f(\gamma^i), i = 0..n-1,$$

where $\deg f(x) < k$, and $\sigma(\gamma^i) = 0$ iff y_i is corrupted. This is equivalent to finding a bivariate polynomial $Q(x, y) = \sigma(x)y - p(x)$, such that $Q(\gamma^i, y_i) = 0$, and $\operatorname{LT} Q(x, y) = x^T y$, where $\operatorname{LT} Q(x, y)$ denotes the leading term of the polynomial with respect to $(1, k-1)$-weighted degree lexicographic ordering with $y \prec x$, T is the total number of errors in the vector $(y_0, \ldots, y_{n-1})$, and $\deg p(x) \leq T+k-1$. Decoding of folded codes requires one also to demand that the set of roots of $\sigma(x)$ should be covered by at most t sets $\{\gamma^{im}, \ldots, \gamma^{im+m-1}\}, i = 0..n/m-1$, i.e. there should be at most t groups of consecutive errors of length m. This implies $T = tm$.

All such bivariate polynomials can be found in the module $\mathcal{M} = \{Q(x, y) = q_0(x) + q_1(x)y | Q(\gamma^i, y_i) = 0, i = 0..n-1\}$, which can be considered as a two-dimensional vector space over $\mathbb{F}[x]$. Let $q_{00}(x) + yq_{01}(x)$ and $q_{10}(x) + yq_{11}(x)$ be a Gröbner basis of this module with respect to $(1, k-1)$-weighted degree lexicographic ordering. Then any polynomial $Q(x, y)$ corresponding to a solution of the decoding problem satisfies $Q(x, y) = a(x)(q_{00}(x) + yq_{01}(x)) + b(x)(q_{10}(x) + yq_{11}(x))$, where $\deg a(x) \leq w_1 = T + k - 1 - \deg q_{00}(x)$, and $\deg b(x) \leq w_2 = T - \deg q_{11}(x)$. In particular,

$$\sigma(x) = a(x)q_{01}(x) + b(x)q_{11}(x).$$

In the case of folded RS codes this implies that one should find $a(x), b(x)$: $a(\gamma^{im+j})q_{01}(\gamma^{im+j}) + b(\gamma^{im+j})q_{11}(\gamma^{im+j}) = 0, j = 0..m-1$ for at most t distinct values of i.

Following [4], we introduce a partially homogenized polynomial (PHP)

$$Q(x, y_1, z_1, \ldots, y_{M-1}, z_{M-1}) = \sum_{j_1=0}^{\rho} \cdots \sum_{j_{M-1}=0}^{\rho} q_{j_1,\ldots,j_{M-1}}(x) y_1^{j_1} z_1^{\rho-j_1} \cdots y_{M-1}^{j_{M-1}} z_{M-1}^{\rho-j_{M-1}}, \tag{4}$$

which will be used to identify all suitable polynomial pairs $[a(x), b(x)]$.

Lemma 1. *Let $Q(x, y_1, z_1, \ldots, y_{M-1}, z_{M-1})$ be a PHP such that for all α_j the points $(x_0, \alpha_1 u_1, \alpha_1 v_1, \ldots, \alpha_{M-1} u_{M-1}, \alpha_{M-1} v_{M-1})$ are its roots of multiplicity r. Then for all $a_i(x), b_i(x)$:*

$$v_i a_i(x_0) - u_i b_i(x_0) = 0, i = 1..M-1,$$

the polynomial $Q(x, a_1(x), b_1(x), \ldots, a_{M-1}(x), b_{M-1}(x))$ is divisible by $(x-x_0)^r$.

Proof. The polynomial has roots $(x_0, \alpha_1 u_1, \alpha_1 v_1, \ldots, \alpha_{M-1} u_{M-1}, \alpha_{M-1} v_{M-1})$ of multiplicity r iff all its Hasse derivatives of total order less than r are equal to zero at these points. In the case of PHP this can be written as

$$Q(x, y_1, z_1, \ldots, y_{M-1}, z_{M-1}) = \sum_{j_0+j_1+\ldots+j_{M-1}\geq r} q_{j_0,\ldots,j_{M-1}}(x-x_0)^{j_0}\prod_{i=1}^{M-1}(y_iv_i-z_iu_i)^{j_i}$$

Clearly, $(x - x_0)|(v_ia_i(x) - u_ib_i(x))$. Hence, $(x - x_0)^r$ divides $Q(x, a_1(x), b_1(x), \ldots, a_{M-1}(x), b_{M-1}(x))$. □

For the sake of simplicity, the arbitrary constants α_i will be omitted in the subsequent derivations. The following is a reformulation of [2, Lemma 4.1].

Lemma 2. *Let* $Q(x, y_1, z_1, \ldots, y_{M-1}, z_{M-1})$ *be a PHP having roots* $(\gamma^{im+j}, q_{11}(\gamma^{im+j}), -q_{10}(\gamma^{im+j}), \ldots, q_{11}(\gamma^{im+j+M-2}), -q_{10}(\gamma^{im+j+M-2})), j = 0..m - M + 1, i = 0..n/m - 1$, *of multiplicity* r. *If* $(1, w_1, w_2, \ldots, w_1, w_2)$*-weighted degree of this polynomial is less than* $D = r(m - M + 2)t$, *then* $Q(x, a(x), b(x), a(\gamma x), b(\gamma x), \ldots, a(\gamma^{M-2}x), b(\gamma^{M-2}x)) = 0$ *for all* $a(x), b(x)$, *such that* $\deg a(x) \leq w_1, \deg b(x) \leq w_2$, *and*

$$a(\gamma^{im+j})q_{10}(\gamma^{im+j}) + b(\gamma^{im+j})q_{10}(\gamma^{im+j}) = 0, j = 0..m - 1,$$

for at least t *distinct values of* i.

Proof. By lemma 1, $g(x) = Q(x, a(x), b(x), \ldots, a(\gamma^{M-2}x), b(\gamma^{M-2}x))$ is divisible by $(x - \gamma^{im+j})^r, j = 0..m - M + 1$ for all $i : a(\gamma^{im+j'})q_{10}(\gamma^{im+j'}) + b(\gamma^{im+j'})q_{10}(\gamma^{im+j'}) = 0, j' = 0..m - 1$. However, $\deg g(x)$ is less than $r(m - M + 2)t$. Hence, $g(x) = 0$. □

This lemma implies that one can correct up to t errors in a folded RS code by constructing a $(2M - 1)$-variate PHP with sufficiently small $(1, w_1, w_2, \ldots, w_1, w_2)$-weighted degree having $n\frac{m-M+2}{m}$ roots of multiplicity r. This can be done as long as the number of terms in it exceeds the number of equations. The number of terms of total degree less than D in (4) is given by $\overline{N} = \sum_{j_1=0}^{\rho}\cdots\sum_{j_{M-1}=0}^{\rho}\left(D - \sum_{l=1}^{M-1}(w_1j_i + w_2(\rho - j_i))\right) = (D - w_2\rho(M - 1))(\rho + 1)^{M-1} - (w_1 - w_2)(M - 1)\frac{\rho(\rho+1)^{M-1}}{2} = (D - \frac{w}{2}\rho(M - 1))(\rho + 1)^{M-1}$, where $w = w_1+w_2 = 2tm+k-1-\deg q_{11}(x)-\deg q_{00}(x) = 2tm+k-1-n$, and the latter equality follows from the properties of the Gröbner basis of $\mathcal{M}$ [4,5]. Hence, the parameters of the algorithm must satisfy

$$\left(r(m - M + 2)t - \frac{2tm + k - 1 - n}{2}\rho(M - 1)\right)(\rho+1)^{M-1} > \frac{n(m - M + 2)}{mM!}\prod_{j=0}^{M-1}(r+j). \tag{5}$$

Relaxing ρ to be a continuous variable and optimizing over it, one obtains that the left-hand side of this maximized by setting $\rho = \frac{D-w/2}{Mw/2}$. The optimal value

Table 1: Comparison of the decoding algorithms: $n = 255, M = 3$

θ	t	m	Guruswami-Rudra				Multivariate Wu			
			R_{opt}	k	r	ρ	R_{opt}	k	r	ρ
0.1	25	1	0.81	208	46	13	0.81	208	5	51
	8	3	0.57	147	19	20	0.82	212	7	18
	5	5	0.68	175	18	19	0.82	211	6	15
0.3	76	1	0.49	125	23	33	0.49	125	9	32
	25	3	0.39	100	12	14	0.50	131	33	43
	15	5	0.47	120	15	18	0.52	136	33	43
0.5	127	1	0.25	64	26	52	0.25	64	25	51
	42	3	0.24	61	22	31	0.22	59	42	42
	25	5	0.28	73	14	20	0.27	72	3421	3455
0.8	204	1	0.04	11	41	209	0.04	11	165	206
	68	3	0.059	16	61	138	-0.15	-	-	-
	40	5	0.071	19	6	14	-0.06	-	-	-

is given by $\overline{N}^* = \frac{(D+(M-1)w/2)^M}{M^M(w/2)^{M-1}} = \frac{(r(m-M+2)t+(M-1)(2tm+k-1-n)/2)^M}{M^M((2tm+k-1-n)/2)^{M-1}}$. Then (5) can be rewritten as

$$\frac{(\frac{m-M+2}{m}\theta + \frac{M-1}{r}(\theta + (R-1)/2))^M}{M^M(\theta + (R-1)/2)^{M-1}} > \frac{m-M+2}{mM!}\prod_{j=0}^{M-1}\left(1+\frac{j}{r}\right)$$

For sufficiently large r this inequality can be solved if $\left(\frac{m-M+2}{m}\right)^{M-1}\theta^M > \frac{M^M}{M!}\left(\theta + (R-1)/2\right)^{M-1}$, i.e.

$$R < 1 - 2\theta + 2\frac{m-M+2}{m}\left(\frac{M!}{M^M}\theta^M\right)^{\frac{1}{M-1}}. \tag{6}$$

This expression implies that the multivariate Wu algorithm always outperforms the classical decoding techniques, which require $R < 1 - 2\theta$.

4 Numeric results

This section presents comparison of the Guruswami-Rudra and Wu-based decoding algorithms. For each θ the maximal achievable rate was computed from (3) and (6). The exact values of parameters r, ρ, and k, such that (2) and (5) are satisfied, are reported for the case of m-folded RS code of length $255/m$.

It can be seen that the multivariate Wu algorithm outperforms the Guruswami-Rudra one in the case of small θ, i.e. high-rate codes. In the case of $m = 1$ (i.e. list decoding of conventional RS codes) the error correction capability of both algorithms is identical. For $m = 3$ and small θ the performance of the Guruswami-Rudra algorithm turns out to be worse than for $m = 1$, as it was observed in [2]. However, the achievable rate improves with m and θ. The multivariate Wu algorithm described in this paper outperforms the Guruswami-Rudra algorithm for small values of θ, but increasing θ causes its performance to degrade. For $\theta \geq 0.8$ it turns out to be impossible to find suitable parameters r and ρ. It can be also seen that the actual rate of the codes which can be decoded using the reformulated Wu algorithm exceeds slightly the value given by (6).

5 Conclusions

In this paper a multivariate generalization of the Wu list decoding algorithm to the case of folded RS codes was proposed. It was shown that for relatively small values of θ the proposed algorithm can be used to list decode rate R m-folded RS codes from a fraction θ of errors for larger values of R compared to the case of the Guruswami-Rudra algorithm. However, the proposed algorithm cannot be used for θ close to 1.

References

[1] V. Guruswami and A. Rudra. Achieving list decoding capacity using folded Reed-Solomon codes. In *Proceedings of 44th Allerton Conference on Communication, Control, and Computing*, 2006.

[2] V. Guruswami and A. Rudra. Explicit codes achieving list decoding capacity: Error-correction with optimal redundancy. *IEEE Transactions On Information Theory*, 54(1), January 2008.

[3] V. Guruswami and M. Sudan. Improved decoding of Reed-Solomon and algebraic-geometric codes. *IEEE Transactions on Information Theory*, 45(6):1757–1767, September 1999.

[4] P. Trifonov. Another derivation of Wu list decoding algorithm and interpolation in rational curve fitting. In *Proceedings of IEEE R8 International Conference on Computational Technologies in Electrical and Electronics Engineering*, 2010.

[5] P. Trifonov. Efficient interpolation in the Guruswami-Sudan algorithm. *IEEE Transactions on Information Theory, accepted for publication*, 2010.

[6] Y. Wu. New list decoding algorithms for Reed-Solomon and BCH codes. *IEEE Transactions On Information Theory*, 54(8), August 2008.