List Decoding of q-ary Reed–Muller Codes

Ruud Pellikaan and Xin-Wen Wu, *Member, IEEE*

***Abstract*—The q-ary Reed–Muller (RM) codes $\mathcal{RM}_q(u,m)$ of length $n=q^m$ are a generalization of Reed–Solomon (RS) codes, which use polynomials in m variables to encode messages through functional encoding. Using an idea of reducing the multivariate case to the univariate case, randomized list-decoding algorithms for RM codes were given in [1] and [15]. The algorithm in [15] is an improvement of the algorithm in [1], it is applicable to codes $\mathcal{RM}_q(u,m)$ with $u<q/2$ and works for up to $E<n(1-\sqrt{2u/q})$ errors. In this correspondence, following [6], we show that q-ary RM codes are subfield subcodes of RS codes over $\mathbb{F}_{q^m}$. Then, using the list-decoding algorithm in [5] for RS codes over $\mathbb{F}_{q^m}$, we present a list-decoding algorithm for q-ary RM codes. This algorithm is applicable to codes of any rates, and achieves an error-correction bound $n(1-\sqrt{(n-d)/n})$. The algorithm achieves a better error-correction bound than the algorithm in [15], since when u is small**

$$n\left(1-\sqrt{(n-d)/n}\right)=n\left(1-\sqrt{u/q}\right).$$

The implementation of the algorithm requires $O(n)$ field operations in $\mathbb{F}_q$ and $O(n^3)$ field operations in $\mathbb{F}_{q^m}$ under some assumption.

***Index Terms*—Guruswami–Sudan algorithm, list decoding, order domain, q-ary Reed–Muller (RM) codes, subfield subcodes.**

I. Introduction

Let C be an $[n,k,d]$ code over the finite field $\mathbb{F}_q$ with q elements. Let $E<n$ and b be positive integers, C is called (E,b)-decodable if every Hamming sphere of radius E in $\mathbb{F}_q^n$ contains at most b codewords. For any received word $\boldsymbol{y}=(y_1,\ldots,y_n)\in\mathbb{F}_q^n$, a codeword $\boldsymbol{c}$ contained in the Hamming sphere centered at $\boldsymbol{y}$ with radius E, i.e., $d(\boldsymbol{c},\boldsymbol{y})\le E$, is called a *$E$-consistent codeword*. A list-decoding algorithm is an algorithm which tries to construct a list which includes all the E-consistent codewords. The parameter E can be greater than the traditional error-correction bound $\lfloor\frac{d-1}{2}\rfloor$. Thus, a list-decoding algorithm makes it possible to recover the information from errors beyond the traditional error-correction bound.

List decoding was introduced by Elias [2] and Wozencraft [16]. In [14], Sudan proposed a list-decoding algorithm for Reed–Solomon (RS) codes. Algebraic-geometry (AG) codes are a generalization of RS codes. In 1999, Shokrollahi and Wasserman generalized Sudan's algorithm and derived a list-decoding algorithm for AG codes [10]. Both of the list-decoding algorithms in [14] and [10] work only for codes of low rates. Guruswami and Sudan [5] later proposed improved list-decoding algorithms for RS and AG codes. The algorithms of Guruswami and Sudan have better error-correction capabilities than algorithms in [14] and [10], and are applicable to codes of any rates. Apart from AG codes, RS codes can be generalized in another way, by allowing multivariate polynomials to encode the message. These generalized codes are known as Reed–Muller (RM) codes.

Manuscript received February 21, 2003; revised September 29, 2003. This work was supported in part by the National Natural Science Foundation of China.

R. Pellikaan is with the Department of Mathematics and Computing Science, Technical University of Eindhoven, 5600 MB Eindhoven, The Netherlands (e-mail: g.r.pellikaan@TUE.nl).

X.-W. Wu is with the Academy of Mathematics and System Sciences, Chinese Academy of Sciences, Beijing, 100080, China (e-mail: x.wu@ee.mu.oz.au).

Communicated by R. Koetter, Associate Editor for Coding Theory.

Digital Object Identifier 10.1109/TIT.2004.825043

Let $\mathbb{F}_q[X_1,\ldots,X_m]$ be the ring of polynomials in m variables with coefficients in $\mathbb{F}_q$. Let $P_1,\ldots,P_n$ be an enumeration of the points of $\mathbb{F}_q^m$, where $n=q^m$. The q-ary RM code $\mathcal{RM}_q(u,m)$ of order u in m variables is defined as

$$\mathcal{RM}_q(u,m)=\{(f(P_1),\ldots,f(P_n))\mid f\in\mathbb{F}_q[X_1,\ldots,X_m],\deg(f)\le u\}.$$

When $m=1$, we get a RS code $C_{\mathrm{RS}}(u)=\mathcal{RM}_q(u,1)$. The list-decoding algorithm for RS code $C_{\mathrm{RS}}(u)$ in [5] decodes up to $E<n(1-\sqrt{(n-d)/n})$ errors, where n and d are the length and minimum distance of the code, respectively.

In [1] and [15], using an idea of reducing the multivariate case to the univariate case, randomized list-decoding algorithms for RM codes $\mathcal{RM}_q(u,m)$ were given. The algorithm in [15] improves upon the algorithm in [1], and it works for up to $E<n(1-c\sqrt{u/q})$ errors, where c is a constant greater than $\sqrt{2}$. It is clear that this algorithm is only applicable to codes $\mathcal{RM}_q(u,m)$ with $u<q/2$.

Following [6], we show that q-ary RM codes are subfield subcodes of RS codes over $\mathbb{F}_{q^m}$. Using the list-decoding algorithm in [5] for RS codes over $\mathbb{F}_{q^m}$, we present a list-decoding algorithm for q-ary RM codes. This algorithm is applicable to RM codes of any rates, and achieves an error-correction bound $n(1-\sqrt{(n-d)/n})$. It is known that when $u<q$, the minimum distance of $\mathcal{RM}_q(u,m)$ of length $n=q^m$ is $d=(q-u)q^{m-1}$, so we have

$$n\left(1-\sqrt{(n-d)/n}\right)=n\left(1-\sqrt{u/q}\right).$$

Thus, our algorithm works for up to $E<n(1-\sqrt{u/q})$ errors in low rate case, which is better than the error-correction bound $n(1-\sqrt{2u/q})$ of the algorithm in [15]. We show that in the case of fixed rate, the implementation of the algorithm requires $O(n)$ field operations in $\mathbb{F}_q$ and $O(n^3)$ field operations in $\mathbb{F}_{q^m}$.

In this work, we also give a list-decoding algorithm for q-ary RM codes, which is a straightforward generalization of the algorithm in [5]. The error-correction capability and complexity of this algorithm are given.

This work is organized as follows. In Section II, following [6], we show that q-ary RM codes are subfield subcodes of RS codes over $\mathbb{F}_{q^m}$. Then, in Section III, we propose a list-decoding algorithm for q-ary RM codes, using the list-decoding algorithm for RS codes over $\mathbb{F}_{q^m}$. In Section IV, we present a straightforward generalization of the list-decoding algorithm of RS codes [5], which is applicable to RM codes. Finally, in Section V, we give conclusions.

II. Subfield Subcodes of RS Codes

In this section, following [6] we will show that the q-ary RM code $\mathcal{RM}_q(u,m)$ is a subfield subcode of a generalized RS code over $\mathbb{F}_{q^m}$. We say that a q-ary code C of length n is a *subfield subcode* of a code $\tilde{C}$ over an extension $\mathbb{F}_{q^m}$ of $\mathbb{F}_q$ if $C\subseteq(\tilde{C}\cap\mathbb{F}_q^n)$.

Let ζ be a primitive element of $\mathbb{F}_{q^m}$, then

$$\mathbb{F}_{q^m}=\{0,1,\zeta,\zeta^2,\ldots,\zeta^{q^m-2}\}.$$

The field $\mathbb{F}_{q^m}$ can be viewed as an m-dimensional vector space over $\mathbb{F}_q$ with $1,\zeta,\ldots,\zeta^{m-1}$ as basis elements, so

$$\zeta^j=\sum_{i=0}^{m-1}a_{ij}\zeta^i,\qquad 0\le j\le q^m-2$$

where $a_{ij} \in \mathbb{F}_q$, $0 \le i \le m-1$, $0 \le j \le q^m - 2$. In other words, the elements of $\mathbb{F}_{q^m}$ can be written in the vector form as

$$\zeta^j = \begin{pmatrix} a_{0j} \\ a_{1j} \\ \vdots \\ a_{m-1,j} \end{pmatrix}, \qquad j = 0, 1, \ldots, q^m - 2.$$

Let $n = q^m$. The vector space $\mathbb{F}_q^m$ has n elements which are often called points. Let

$$P_0 := (0, 0, \ldots, 0)$$
$$P_j := (a_{0,j-1}, a_{1,j-1}, \ldots, a_{m-1,j-1}), \quad j = 1, \ldots, n-1. \quad (2.1)$$

Then $P_0, P_1, \ldots, P_{n-1}$ is an enumeration of the points of $\mathbb{F}_q^m$. Under this enumeration, a q-ary RM code $\mathcal{RM}_q(u, m)$ of order u is defined as shown at the bottom of the page.

For two vectors $U = (a_1, \ldots, a_n)$ and $V = (b_1, \ldots, b_n)$, define the vector product as

$$UV = (a_1 b_1, a_2 b_2, \ldots, a_n b_n).$$

Now let

$$V_I = (1, 1, \ldots, 1) \in \mathbb{F}_q^n$$
$$V_i = (0, a_{i0}, a_{i1}, \ldots, a_{i,n-2}), \qquad i = 0, 1, \ldots, m-1.$$

With these vectors in $\mathbb{F}_q^n$, we construct a matrix G_u as

$$G_u = \begin{pmatrix} V_I \\ V_0^{k_0} V_1^{k_1} \ldots V_{m-1}^{k_{m-1}} \end{pmatrix}$$

with V_I and $V_0^{k_0} V_1^{k_1} \cdots V_{m-1}^{k_{m-1}}$ as rows for all nonnegative integers $k_0, k_1, \ldots, k_{m-1}$ such that $\sum_{t=0}^{m-1} k_t \le u$.

It is clear that the code over $\mathbb{F}_q$ generated by G_u is exactly the RM code $\mathcal{RM}_q(u, m)$. From this representation of RM codes, we can easily find an RS code over $\mathbb{F}_{q^m}$ such that $\mathcal{RM}_q(u, m)$ can be embedded into the RS code as a subfield subcode.

Let

$$\boldsymbol{v}_I = (1, 1, \ldots, 1) \in \mathbb{F}_q^{n-1}$$
$$\boldsymbol{v}_i = (a_{i0}, a_{i1}, \ldots, a_{i,n-2}), \qquad i = 0, 1, \ldots, m-1.$$

Note that $\boldsymbol{v}_I$ and $\boldsymbol{v}_i$ are punctured vectors of V_I and V_i, respectively, with the first digits dropped. Let G_u^* be the matrix with $\boldsymbol{v}_I$ and $\boldsymbol{v}_0^{k_0} \boldsymbol{v}_1^{k_1} \cdots \boldsymbol{v}_{m-1}^{k_{m-1}}$ as rows for all nonnegative integers $k_0, k_1, \ldots, k_{m-1}$ such that $\sum_{t=0}^{m-1} k_t \le u$. We denote the code over $\mathbb{F}_q$ generated by G_u^* as $\mathcal{RM}_q^*(u, m)$. It is easy to see that $\mathcal{RM}_q^*(u, m)$ is the punctured code of $\mathcal{RM}_q(u, m)$ with the first digit dropped. Conversely, $\mathcal{RM}_q(u, m)$ is the extended code of $\mathcal{RM}_q^*(u, m)$. Hence,

$(\xi, \boldsymbol{c}^*) \in \mathcal{RM}_q(u, m)$ if and only if

$$\boldsymbol{c}^* \in \mathcal{RM}_q^*(u, m) \text{ and } \xi + \sum c_i^* = 0.$$

It is well known that for given q, m, and u, letting $u^\perp = m(q-1) - u - 1$, the dual code of $\mathcal{RM}_q(u, m)$ is equal to $\mathcal{RM}_q(u^\perp, m)$. Let ρ be the remainder after division of $u^\perp + 1$ by $q-1$ with quotient σ, that is,

$$u^\perp + 1 = \sigma(q-1) + \rho, \qquad \text{where } \rho < q - 1.$$

Let h be an integer such that $0 \le h \le q^m - 1$. Express h in radix-q form

$$h = \delta_0 + \delta_1 q + \delta_2 q^2 + \cdots + \delta_{m-1} q^{m-1}.$$

Define the weight of h as

$$W(h) = \delta_0 + \delta_1 + \delta_2 + \cdots + \delta_{m-1}.$$

The following proposition is taken from [6, Corollary 2].

Proposition 2.1: The code $\mathcal{RM}_q^*(u, m)$ is the cyclic code over $\mathbb{F}_q$ with generator polynomial $g(X)$ such that ζ^h is a zero of $g(X)$ if and only if $0 < W(h) \le u^\perp$.

The following theorem is taken from [6, Theorem 5].

Theorem 2.2: Define $d = (\rho + 1)q^\sigma$. Then the q-ary code $\mathcal{RM}_q^*(u, m)$ is a subcode of the Boise–Chaudhuri–Hocquenghem (BCH) code over $\mathbb{F}_q$ whose generator polynomial has $\zeta, \zeta^2, \ldots, \zeta^{d-2}$ as its roots, and $d-1$ is the minimum distance of $\mathcal{RM}_q^*(u, m)$.

The following example shows that the punctured RM code is a proper subcode of the binary BCH code. Take $q = 2$, $m = 6$, and $u = 3$. Then $u^\perp = 2$, $\sigma = 3$, and $\rho = 0$. So $d = 2^3 = 8$. The code $\mathcal{RM}_2^*(3, 6)$ has parameters $[63, 42, 7]$. The binary BCH code with zeros ζ^i with $i \in \{1, 2, 3, 4, 5, 6\}$ has complete defining set the union of the sets: $\{1, 2, 4, 8, 16, 32\}$, $\{3, 6, 12, 24, 28, 33\}$, $\{5, 10, 20, 40, 17, 34\}$. So the dimension of the BCH code is $63 - 3 \cdot 6 = 45$. Therefore, the BCH code has parameters $[63, 45, 7]$ and it has the punctured RM code as a subcode, but they are not equal. This is explained by the zero $9 = 1 + 2^3$ having 2-weight equal to $2 \le u^\perp$, whereas no element of the cyclotomic coset $\{9, 18, 36\}$ of 9 is in the set $\{1, 2, 3, 4, 5, 6\}$.

The minimum distance of $\mathcal{RM}_q(u, m)$ is equal to $d = (\rho + 1)q^\sigma$.

Denote by C_{BCH} the BCH code over $\mathbb{F}_q$ whose generator polynomial has ζ^i with $i = 1, \ldots, d-2$ as its roots. Then the complete zero set consists of all ζ^{iq^j} with $i = 1, \ldots, d-2$ and $j = 1, \ldots, m$. Denote by $\tilde{C}_{\mathrm{BCH}}$ the BCH code over $\mathbb{F}_{q^m}$ whose generator polynomial has ζ^i with $i = 1, \ldots, d-2$ as all its roots. Then $C_{\mathrm{BCH}} = (\tilde{C}_{\mathrm{BCH}} \cap \mathbb{F}_q^{n-1})$. So

$$\mathcal{RM}_q^*(u, m) \subseteq \left(\tilde{C}_{\mathrm{BCH}} \cap \mathbb{F}_q^{n-1}\right)$$

by Theorem 2.2. The following matrix H is a parity-check matrix of $\tilde{C}_{\mathrm{BCH}}$:

$$H = \begin{pmatrix} 1 & \zeta & \zeta^2 & \cdots & \zeta^{n-2} \\ 1 & \zeta^2 & \zeta^4 & \cdots & \zeta^{2(n-2)} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \zeta^{d-2} & \zeta^{2(d-2)} & \cdots & \zeta^{(d-2)(n-2)} \end{pmatrix}.$$

Let $\boldsymbol{a}^* = (1, \zeta, \zeta^2, \ldots, \zeta^{n-2})$. Then the matrix H is a generator matrix of the generalized RS code $\mathrm{GRS}_{d-2}(\boldsymbol{a}^*, \boldsymbol{a}^*)$ over $\mathbb{F}_{q^m}$, see [7, Ch. 10 Sec.8]. So $\tilde{C}_{\mathrm{BCH}}$ is the dual code of $\mathrm{GRS}_{d-2}(\boldsymbol{a}^*, \boldsymbol{a}^*)$.

By [7, Theorem 4, Ch. 10, Sec.8], the dual of $\mathrm{GRS}_{d-2}(\boldsymbol{a}^*, \boldsymbol{a}^*)$ is a generalized RS code $\mathrm{GRS}_{n-d+1}(\boldsymbol{a}^*, \boldsymbol{b}^*)$ for some $\boldsymbol{b}^*$. From the fact that

$$1 + \zeta^i + \zeta^{2i} + \cdots + \zeta^{(n-1)i} = 0, \qquad \text{for } 1 \le i \le n-2$$

we have that

$$G = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \zeta & \zeta^2 & \cdots & \zeta^{n-2} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \zeta^{n-d} & \zeta^{2(n-d)} & \cdots & \zeta^{(n-2)(n-d)} \end{pmatrix}$$

$$\mathcal{RM}_q(u, m) = \{(f(P_0), f(P_1), \ldots, f(P_{n-1})) | f \in \mathbb{F}_q[X_1, \ldots, X_m], \deg(f) \le u\}.$$

is a generator matrix of $\mathrm{GRS}_{n-d+1}(\boldsymbol{a}^*, \boldsymbol{b}^*)$ with $\boldsymbol{b}^* = \mathbf{1} = (1, \ldots, 1)$. And $\mathrm{GRS}_{n-d+1}(\boldsymbol{a}^*, \mathbf{1})$ has a parity-check matrix H. Hence,

$$\tilde{C}_{\mathrm{BCH}} = \mathrm{GRS}_{n-d+1}(\boldsymbol{a}^*, \mathbf{1}).$$

Therefore, we have embedded $\mathcal{RM}_q^*(u, m)$ into $\mathrm{GRS}_{n-d+1}(\boldsymbol{a}^*, \mathbf{1})$ as a subfield subcode.

Let $\boldsymbol{a} = (0, \boldsymbol{a}^*) = (0, 1, \zeta, \ldots, \zeta^{n-2})$. Then $\mathrm{GRS}_{n-d+1}(\boldsymbol{a}, \mathbf{1})$ is the extended code of $\mathrm{GRS}_{n-d+1}(\boldsymbol{a}^*, \mathbf{1})$. Hence, $\mathcal{RM}_q(u, m)$ is a subcode of $\mathrm{GRS}_{n-d+1}(\boldsymbol{a}, \mathbf{1})$, where d is the minimum distance of $\mathcal{RM}_q(u, m)$, i.e.,

$$\mathcal{RM}_q(u, m) \subseteq \left(\mathrm{GRS}_{n-d+1}(\boldsymbol{a}, \mathbf{1}) \cap \mathbb{F}_q^n\right).$$

III. List Decoding of RM Codes

We have shown that $\mathcal{RM}_q(u, m) \subseteq \left(\mathrm{GRS}_{n-d+1}(\boldsymbol{a}, \mathbf{1}) \cap \mathbb{F}_q^n\right)$. The code $\mathrm{GRS}_{n-d+1}(\boldsymbol{a}, \mathbf{1})$ is an $[n, n-d+1, d]$ RS code over $\mathbb{F}_{q^m}$. Using the list-decoding algorithm for $\mathrm{GRS}_{n-d+1}(\boldsymbol{a}, \mathbf{1})$ in [5], we give a list-decoding algorithm for $\mathcal{RM}_q(u, m)$ as follows.

Algorithm 3.1 (*List Decoding Algorithm of RM Codes*)

Input: $n = q^m$, $\boldsymbol{y} = (y_0, y_1, \ldots, y_{n-1}) \in \mathbb{F}_q^n$.

Step 0: 1) Compute the minimum distance d of $\mathcal{RM}_q(u, m)$ and a parameter

$$E = \lceil n - \sqrt{n(n-d)} - 1 \rceil.$$

2) Construct the extension field $\mathbb{F}_{q^m}$ using an irreducible polynomial of degree m over $\mathbb{F}_q$.

3) Find a primitive element ζ of $\mathbb{F}_{q^m}$. Generate the code $\mathrm{GRS}_{n-d+1}(\boldsymbol{a}, \mathbf{1})$ with $\boldsymbol{a} = (0, 1, \zeta, \ldots, \zeta^{n-2})$.

4) Construct a parity check matrix H_0 over $\mathbb{F}_q$ for the code $\mathcal{RM}_q(u, m)$.

Step 1: Using the list-decoding algorithm for an RS code over $\mathbb{F}_{q^m}$ in **[5]** find the set $\mathcal{L}^{(1)}$ of all the codewords $\boldsymbol{c}$ of $\mathrm{GRS}_{n-d+1}(\boldsymbol{a}, \mathbf{1})$ satisfying

$$d(\boldsymbol{c}, \boldsymbol{y}) \leq E.$$

Step 2: For every $\boldsymbol{c} \in \mathcal{L}^{(1)}$, check if $\boldsymbol{c} \in \mathbb{F}_q^n$, if so, append $\boldsymbol{c}$ to $\mathcal{L}^{(2)}$.

Step 3: For every $\boldsymbol{c} \in \mathcal{L}^{(2)}$, check if $H_0 \boldsymbol{c}^{\boldsymbol{T}} = \mathbf{0}$, if so, append $\boldsymbol{c}$ to $\mathcal{L}$. Output $\mathcal{L}$.

From [5, Theorem 8 and Proposition 9] we have the following theorem.

Theorem 3.1: Assume d is the minimum distance of the q-ary RM code $\mathcal{RM}_q(u, m)$. Then $\mathcal{RM}_q(u, m)$ is (E, M)-decodable, provided that

$$E < n - \sqrt{n(n-d)} \quad \text{and} \quad M = O\left(\sqrt{(n-d)n^3}\right).$$

Algorithm 3.1 correctly finds all the E-consistent codewords for any received vector $\boldsymbol{y} \in \mathbb{F}_q^n$.

Remark 3.1: Note that Algorithm 3.1 outputs a set of E-consistent codewords of the q-ary RM code defined by the enumeration of points of $\mathbb{F}_q^m$, say $P_0, P_1, \ldots, P_{n-1}$, given by (2.1). If $\mathcal{RM}_q(u, m)$ is defined by another enumeration of the points of $\mathbb{F}_q^m$, namely, $P_0', P_1', \ldots, P_{n-1}'$, we can get the correct E-consistent codewords by the following steps: 1) Find the permutation π such that $P_i = P'_{\pi(i)}$, $i = 0, 1, \ldots, n-1$, and the inverse permutation π^{-1}. 2) Let

$$\boldsymbol{y}^* = \left(y_{\pi(0)}, y_{\pi(1)}, \ldots, y_{\pi(n-1)}\right).$$

Then, go to Steps 0–2 of Algorithm 3.1 with $\boldsymbol{y}^*$. 3) For every codeword $\boldsymbol{c} = (c_0, c_1, \ldots, c_{n-1}) \in \mathcal{L}$, let

$$\pi^{-1}\left(\boldsymbol{c}\right) = \left(c_{\pi^{-1}(0)}, c_{\pi^{-1}(1)}, \ldots, c_{\pi^{-1}(n-1)}\right).$$

Then

$$\pi^{-1}(\mathcal{L}) = \{\pi^{-1}(\boldsymbol{c}) \mid \boldsymbol{c} \in \mathcal{L}\}$$

is the set of E-consistent codewords of $\mathcal{RM}_q(u, m)$. □

Remark 3.2: It is clear that Algorithm 3.1 works for $\mathcal{RM}_q(u, m)$ with any $u > 0$. So the algorithm is applicable to q-ary RM codes of any rates. Theorem 3.1 gives an error-correction bound of Algorithm 3.1, $E < n - \sqrt{n(n-d)}$. When $u < q$, the minimum distance of $\mathcal{RM}_q(u, m)$ is given by $d = (q-u)q^{m-1}$. So

$$n - \sqrt{n(n-d)} = n\left(1 - \sqrt{u/q}\right) > n\left(1 - \sqrt{2u/q}\right).$$

Algorithm 3.1 has a better error-correction capability than the algorithm in [15]. □

Now, let us consider the complexity of Algorithm 3.1. In Step 0, to construct the extension field $\mathbb{F}_{q^m}$, it is necessary to find an irreducible polynomial $g(x)$ of degree m over $\mathbb{F}_q$. It is well known that there are efficient algorithms for finding irreducible polynomials over finite fields [13]. In [11], a probabilistic algorithm is given for finding an irreducible polynomial of degree m over $\mathbb{F}_q$ with expected number of

$$O((m^2 \log m + m \log q) \log m \log \log m)$$

field operations in $\mathbb{F}_q$.

To generate the RS code $\mathrm{GRS}_{n-d+1}(\boldsymbol{a}, \mathbf{1})$ over $\mathbb{F}_{q^m}$, we need to find a primitive element of $\mathbb{F}_{q^m}$. From [12], [13], a primitive element of $\mathbb{F}_{q^m}$ can be found in deterministic time $O((q^m)^{1/4+\varepsilon}) = O(n^{1/4+\varepsilon})$, where $n = q^m$ is the length of the code, ε denotes an arbitrary positive number.

Step 1 of Algorithm 3.1 can be implemented using the list-decoding algorithm in [5] for RS code $\mathrm{GRS}_{n-d+1}(\boldsymbol{a}, \mathbf{1})$ over $\mathbb{F}_{q^m}$. From [5, Theorem 12 and Corollary 13], if $t^2 > (1+\delta)n(n-d)$ and $E = n - t < n - \sqrt{n(n-d)}$, then the list-decoding algorithm in [5] can be implemented to run in $O(n^3 \delta^{-6})$ field operations in $\mathbb{F}_{q^m}$. If, furthermore, the rate of RS codes is fixed, the complexity of this algorithm is $O(n^3)$.

So, the implementation of Algorithm 3.1 requires $O(n)$ field operations in $\mathbb{F}_q$ and $O(n^3)$ field operations in $\mathbb{F}_{q^m}$.

IV. Generalized Guruswami–Sudan Algorithm

The following algorithm is a straightforward generalization of the list-decoding algorithm in [5]. We denote $R = \mathbb{F}_q[X_1, \ldots, X_m]$, and $n = q^m$ the length of the code $\mathcal{RM}_q(u, m)$.

Algorithm 4.1 (*Generalized Guruswami-Sudan Algorithm for RM Codes*)
Input: n, t, u, $(y_1,\ldots,y_n)\in\mathbb{F}_q^n$, and

$$P_i:=(x_{i1},\ldots,x_{im})\in\mathbb{F}_q^m,\qquad i=1,\ldots,n.$$

Step 0: Choose the parameters r, v such that

- (A.1) $s:=\lfloor\frac{v}{u}\rfloor$ and

$$\sum_{j=0}^{s}\binom{v-ju+m}{m}>n\binom{m+r}{m+1};$$

- (A.2) $E:=n-t$, $w:=\lfloor\frac{v}{q}\rfloor$ and

$$\binom{m+r-1}{m}E<\binom{m+r-w-1}{m}q^m-(v-qw)\binom{m+r-w-2}{m-1}q^{m-1}.$$

Step 1: Find a nonzero polynomial $H(T)\in R[T]$ of the form

$$H(T)=H(X;T)=\sum_{j=0}^{s}h_j(X)T^j$$

where for $j=0,1,\ldots,s$

$$h_j(X)=\sum h_{j_1,\ldots,j_m;j}X_1^{j_1}\cdots X_m^{j_m},\qquad\text{and }\deg(h_j(X))\le v-ju$$

such that for all $i=1,\ldots,n$, and for any $j_1,\ldots,j_m$, $j\ge 0$ and $j_1+\cdots+j_m+j\le r-1$

$$h^{(i)}_{j_1,\ldots,j_m;j}:=\sum_{j'_1\ge j_1}\cdots\sum_{j'_m\ge j_m}\sum_{j'\ge j}\binom{j'_1}{j_1}\cdots\binom{j'_m}{j_m}\binom{j'}{j}h_{j'_1,\ldots,j'_m;j}x_{i1}^{j'_1-j_1}\cdots x_{im}^{j'_m-j_m}y_i^{j'-j}=0.$$

Step 2: Using the root-finding algorithm in **[17]**, **[18]**, find all the roots $f(X)$ with $\deg(f(X))\le u$ of the polynomial $H(T)$. For each such $f(X)$, check if $f(P_i)=y_i$ for at least t values of $i\in\{1,\ldots,n\}$, and if so, include $f(X)$ in output list.

Using the theories of Gröbner bases and of order domains [4] and a generalization of the Footprint bound [3], we can prove that Algorithm 4.1 decodes up to

$$E<n\left(1-\sqrt[m+1]{u/q}\right)^m$$

errors. Note that when $m=1$,

$$n\left(1-\sqrt[m+1]{u/q}\right)^m=n-\sqrt{nu}$$

which is exactly the error-correction capability of the algorithm for RS codes by Guruswami and Sudan in [5]. Comparing with $n(1-\sqrt{2u/q})$, the error-correction capability of the algorithm in [15], we see that when u is close to $q/2$, Algorithm 4.1 achieves a better error-correction capability than the algorithm in [15]. The time complexity of Algorithm 4.1 is $O(N^3)$, where N denotes the number of coefficients of $H(T)$ and $N=O(m^{2(m+1)}u^{-m}n^{m+2}k)$.

V. Conclusion

We show that a q-ary RM code is a subfield subcode of an RS code over $\mathbb{F}_{q^m}$. We then present a list-decoding algorithm for q-ary RM codes using the list-decoding algorithm for RS codes in [5]. This algorithm is applicable to RM codes of any rates, and achieves an error-correction bound $n(1-\sqrt{(n-d)/n})$. The implementation of the algorithm requires $O(n)$ field operations in $\mathbb{F}_q$ and $O(n^3)$ field operations in $\mathbb{F}_{q^m}$. We also present a straightforward generalization of the list-decoding algorithm in [5].

Acknowledgment

The authors wish to thank the anonymous referees whose thoughtful criticisms and valuable suggestions helped to improve the quality of this correspondence.

References

[1] S. Arora and M. Sudan, "Improved low-degree testing and its applications," in *Proc. 29th Annu. ACM Symp. Theory of Computing*, 1997, pp. 485–495.
[2] P. Elias, "List Decoding for Noisy Channel," Res. Lab. Electron., MIT, Cambridge, MA, Tech. Rep. 335, 1957.
[3] O. Geil and T. Høholdt, "Footprints or generalized Bezout's theorem," *IEEE Trans. Inform. Theory*, vol. 46, pp. 635–641, Mar. 2000.
[4] O. Geil and R. Pellikaan, "On the structure of order domains," *Finite Fields Their Applic.*, vol. 8, pp. 369–396, 2002.
[5] V. Guruswami and M. Sudan, "Improved decoding of Reed–Solomon and algebraic-geometry codes," *IEEE Trans. Inform. Theory*, vol. 45, pp. 1757–1767, Nov. 1999.
[6] T. Kasami, S. Lin, and W. Peterson, "New generalization of Reed-Muller codes, Part I: Primitive codes," *IEEE Trans. Inform. Theory*, vol. IT-14, pp. 189–199, Mar. 1968.
[7] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, ser. Math. Library, Elsevier Sci. Publ. New York: North-Holland, 1972, vol. 16.
[8] J. Rifa and J. Borrell, "A fast algorithm to compute irreducible and primitive polynomials in finite fields," *Math. Syst. Theory*, vol. 28, pp. 13–20, 1995.
[9] R. Roth and G. Ruckenstein, "Efficient decoding of Reed–Solomon codes beyond half the minimum distance," *IEEE Trans. Inform. Theory*, vol. 46, pp. 246–257, Jan. 2000.
[10] M. Shokrollahi and H. Wasserman, "List decoding of algebraic-geometric codes," *IEEE Trans. Inform. Theory*, vol. 45, pp. 432–437, Mar. 1999.
[11] V. Shoup, "Fast construction of irreducible polynomials over finite fields," *J. Symb. Comp.*, vol. 17, pp. 371–391, 1994.
[12] I. E. Shparlinski, "Finding irreducible and primitive polynomials," *Appl. Alg. Engin. Commun. Comp.*, vol. 4, pp. 263–268, 1993.
[13] ——, *Finite Fields: Theory and Computation*, ser. Mathematics and its Applications. Dordrecht, The Netherlands: Kluwer, 1999, vol. 477.
[14] M. Sudan, "Decoding of Reed–Solomon codes beyond the error-correction bound," *J. Complexity*, vol. 13, pp. 180–193, 1997.
[15] M. Sudan, L. Trevisan, and S. Vadhan, "Pseudorandom generators without the XOR lemma," in *Proc. 31st Annu. ACM Symp. Theory of Computing*, 1999, pp. 537–546.
[16] J. M. Wozencraft, "List decoding," in *Quarterly Progress Report*. Cambridge, MA: Res. Lab. Electronics, MIT, 1958, vol. 48, pp. 90–95.
[17] X.-W. Wu, "An algorithm for finding the roots of the polynomials over order domains," in *Proc. IEEE Int. Symp. Information Theory*, Lausanne, Switzerland, June/July 2002, p. 202.
[18] X.-W. Wu and P. H. Siegel, "Efficient root-finding algorithm with applications to list decoding of algebraic-geometric codes," *IEEE Trans. Inform. Theory*, vol. 47, pp. 2579–2587, Sept. 2001.