Fast Decoding of Projective Reed–Muller Codes by Dividing a Projective Space into Affine Spaces

Norihiro Nakashima,* Hajime Matsui†
Toyota Technological Institute, Nagoya 468-8511, Japan.

Abstract

A projective Reed–Muller (PRM) code, obtained by modifying a (classical) Reed–Muller code with respect to a projective space, is a doubly extended Reed–Solomon code when the dimension of the related projective space is equal to 1. The minimum distance and dual code of a PRM code are known, and some decoding examples have been represented for the case of a low-dimensional projective space. In this study, we construct an efficient decoding algorithm for all PRM codes. For this purpose, we divide a projective space into a union of affine spaces. In addition, we evaluate the computational complexity and number of correctable errors of our algorithm. Finally, we compare the codeword error rate of our algorithm with that of minimum distance decoding.

Key Words: error-correcting codes, affine variety codes, Gröbner basis, Berlekamp–Massey–Sakata algorithm, discrete Fourier transform.

1 Introduction

Projective Reed–Muller (PRM) codes have been investigated extensively since they were first introduced by Lachaud [15] in 1988. Sørensen [27] determined the minimum distances of PRM codes and proved that the dual codes of a PRM code is also a PRM code or spanned by a PRM code and a vector of which all entries are 1. In addition, Berger and Maximy [3] presented conditions under which PRM codes are cyclic or quasi-cyclic. Recently, Ballet and Rolland [2] examined low-weight codewords of PRM codes and obtained an estimation of the second weight. The PRM codes of 1-dimensional projective spaces are also considered as doubly extended Reed–Solomon (RS) codes. Dür [8] proposed a decoding method for doubly extended RS codes using the discrete Fourier transform (DFT). This is also described by Hirotomo [13]. Duursma [9] presented a decoding example of a PRM code related to a 2-dimensional projective space using error-locating pairs. Further, the authors also proposed a decoding method for PRM codes related to 2-dimensional projective spaces in a previous study [20].

The objective of the present study is to construct an efficient decoding algorithm for all PRM codes. Although PRM codes are expressed as affine variety codes, there exists an example for

*Email: nakashima@toyota-ti.ac.jp
†Email: matsui@toyota-ti.ac.jp
which a decoding algorithm proposed previously [17] does not work directly. Therefore, after presenting a Gr"{o}bner basis for an evaluation map, we calculate a reduced basis for a PRM code over a field modulo the kernel of the evaluation map. Then, we construct a decoding algorithm for PRM codes by dividing a projective space into a union of affine spaces. In this algorithm, for each affine component of a projective space, we adopt the Berlekamp–Massey–Sakata (BMS) algorithm [23], [24], [25], [26] to obtain a Gr"{o}bner basis related to the error locations and we use the DFT to determine the error values for further details regarding the procedure for each affine component, see [17].

We evaluate the performance of proposed algorithm by comparing it with that of other algorithms. First, we prove that the computational complexity of our algorithm is \( O(wn^2) \), where \( n \) is the code length, \( O \) is Landau’s symbol, and \( w \) is the maximum of the finite-field cardinality and the cardinalities of Gr"{o}bner bases obtained by BMS algorithm for all affine components. Thus, the complexity of our algorithm is less than that of Feng–Rao decoding algorithm [1], [10], [18], [19] and the algorithm that uses error-correction pairs [21] (i.e., \( O(n^3) \)). Next, we consider the number of errors that can be corrected by our algorithm. Because the decoding procedure is divided into components of a projective space, our algorithm corrects special errors that occur component-wise. We determine the numbers of such errors that can be corrected. Further, we determine the number of correctable errors for an arbitrary location. Finally, we compare the codeword error rate of our algorithm with that of minimum distance decoding (MDD) [14], [16] and find them to be similarly for some high-order PRM codes.

The remainder of this paper is organized as follows. In Section 2 we present some preliminary notations and recall the algorithm for affine variety codes that was proposed in a previous study [17]. In Section 3 we represent PRM codes as affine variety codes and provide an example of a reduced basis. In Section 4 we construct a decoding algorithm for PRM codes and compute its computational complexity. In Section 5 we determine the number of errors that can be corrected by our algorithm. In Section 6 we calculate a numerical example of the decoding procedure described in Section 4. In Section 7 we compare the codeword error rate of our algorithm with that of MDD. Finally, in Section 8 we summarize our findings and conclude the paper by briefly discussing the scope for future investigation.

## 2 Preliminaries

Throughout this paper, let \( q \) be a prime power and let \( \mathbb{F}_q \) denote a finite field consisting of \( q \) elements. Let \( R \) denote the polynomial ring \( \mathbb{F}_q[X_0, X_1, \ldots, X_m] \) over \( \mathbb{F}_q \) in variables \( X_0, X_1, \ldots, X_m \), and let \( R_\nu \) denote the linear subspace of \( R \) consisting of homogeneous polynomials of degree \( \nu \). We define

\[
\mathbb{A}_m(\mathbb{F}_q) := \{(a_1, \ldots, a_m) \mid a_1, \ldots, a_m \in \mathbb{F}_q\}.
\]

Then, \( \mathbb{A}_m(\mathbb{F}_q) \) is called an \( m \)-dimensional affine space over \( \mathbb{F}_q \). We often omit a coefficient field \( \mathbb{F}_q \) and write \( \mathbb{A}_m(\mathbb{F}_q) = \mathbb{A}_m \) for short. Set \( \mathbb{A}_m^{*+1} := \mathbb{A}_m+1 \setminus \{0\} \). We define

\[
\mathbb{P}_m := \mathbb{A}_m^{*+1} / \sim
\]

with the equivalence relation

\[
P_1 \sim P_2 \quad \text{if} \quad P_1 = \lambda P_2 \quad \text{for some} \quad \lambda \in \mathbb{F}_q \setminus \{0\}.
\]
Then, \( \mathbb{P}_m(\mathbb{F}_q) \) is called an \( m \)-dimensional projective space over \( \mathbb{F}_q \), and we often write \( \mathbb{P}_m(\mathbb{F}_q) = \mathbb{P}_m \).

We express the equivalence class of a representative \((\omega_0, \omega_1, \ldots, \omega_m)\) as \((\omega_0 : \omega_1 : \cdots : \omega_m)\). Let \( P = (\omega_0 : \omega_1 : \cdots : \omega_m) \in \mathbb{P}_m \) and \( F \in R \). There exists an integer \( i \) such that \( \omega_i \neq 0 \) and \( \omega_j = 0 \) for all \( j < i \). Then, \((0, \ldots, 0, 1, \omega_{i+1}', \ldots, \omega_m')\) is a representative of \( P \), where \( \omega_j' = \frac{\omega_j}{\omega_i} \) for \( j > i \). The value \( f(P) \) is defined by \( f(0, \ldots, 0, 1, \omega_{i+1}', \ldots, \omega_m') \); this is uniquely determined.

First, we define a Reed-Muller code. Let \( P_1, \ldots, P_{q^m} \) be the elements in \( \mathbb{A}_m \).

**Definition 2.1** (Reed-Muller code). A Reed-Muller code over \( \mathbb{F}_q \) of order \( \nu \) is defined by

\[
\text{RM}_\nu(m, q) = \{(f(P_1), \ldots, f(P_{q^m})) \mid f \in R_{\nu}^m\},
\]

where \( R_{\nu}^m := \mathbb{F}_q[X_1, \ldots, X_m]_{\leq \nu} \) is the set of polynomials in \( \mathbb{F}_q[X_1, \ldots, X_m] \) of degree \( \leq \nu \).

It has been shown (cf. [4]) that the dimension \( k \) of \( \text{RM}_\nu(m, q) \) and the minimum distance \( d \) are

\[
k = \sum_{t=0}^{\nu_1} \sum_{j=0}^{m} (-1)^j \binom{m}{j} \left(\frac{t - jq + m - 1}{t - jq}\right),
\]

\[
d = (q - s_1)q^{m-r_1-1}, \tag{2.1}
\]

where \( s_1 \) and \( r_1 \) are integers satisfying \( 0 \leq s_1 < q - 1, 0 \leq r_1 < m - 1 \) and \( \nu_1 = r_1(q - 1) + s_1 \). The dual code of \( \text{RM}_\nu(m, q) \) is obtained by

\[
\text{RM}_{\nu_1}(m, q)^\perp = \text{RM}_{m(q-1)-\nu_1-1}(m, q). \tag{2.2}
\]

Next, we define a projective Reed-Muller code. Set \( n := \frac{q^{m+1}-1}{q-1} = q^m + \cdots + q + 1 \); then, \( n \) is the number of elements in \( \mathbb{P}_m \). Let \( P_1, \ldots, P_n \) be the elements in \( \mathbb{P}_m \).

**Definition 2.2** (Projective Reed-Muller code). A projective Reed-Muller code over \( \mathbb{F}_q \) of order \( \nu \) and length \( n \) is defined by

\[
\text{PRM}_\nu(m, q) = \{(f(P_1), \ldots, f(P_n)) \mid f \in R_\nu\}.
\]

A PRM code is trivial when \( \nu \) is greater than \( m(q-1) \) (see [27, Remark 3]). Therefore, in the rest of this paper, we assume that \( 0 < \nu \leq m(q-1) \). It has been shown (cf. [27]) that \( \text{PRM}_{\nu_2}(m, q) \) is an \([n, k, d]\)-code with

\[
k = \sum_{t=0}^{r_2} \left(\sum_{j=0}^{m+1} (-1)^j \binom{m+1}{j} \left(\frac{s_2 + m - t + (t - jq)q}{s_2 + 1 - t + (t - jq)q}\right)\right),
\]

\[
d = (q - s_2)q^{m-r_2-1}, \tag{2.3}
\]

where \( s_2 \) and \( r_2 \) are integers satisfying \( 0 \leq s_2 < q - 1, 0 \leq r_2 < m \) and \( \nu_2 - 1 = r_2(q - 1) + s_2 \). Table [1] lists some dimensions and minimum distances of \( \text{PRM}_\nu(2, 16) \).

Let \( \Psi \subset \mathbb{A}_m \). We define an ideal \( Z(\Psi) \) of \( \mathbb{F}_q[X_1, \ldots, X_m] \) by

\[
Z(\Psi) = \{ f \in \mathbb{F}_q[X_1, \ldots, X_m] \mid f(P) = 0 \text{ for all } P \in \Psi \}.
\]
Table 1: Parameters of PRM_ν(2, 16)

| ν  | 5   | 8   | 11  | 14  | 17  | 20  | 23  | 26  | 29  |
|----|-----|-----|-----|-----|-----|-----|-----|-----|-----|
| k  | 21  | 45  | 78  | 120 | 168 | 207 | 237 | 258 | 270 |
| d  | 192 | 144 | 96  | 48  | 15  | 12  | 9   | 6   | 3   |

**Definition 2.3** (Affine variety code). For an \(F_q\)-subspace \(L \subseteq R/Z(\Psi)\), we define an affine variety code

\[
C(L, \Psi) := \{(f(P))_{P \in \Psi} \in F_q^\Psi \mid f \in L\},
\]

where \(F_q^\Omega := \{(c_P)_{P \in \Omega} \mid c_P \in F_q\}\) is the \(F_q\)-linear space indexed by \(\Omega\) for any set \(\Omega\).

We have proposed a decoding algorithm [17, Algorithm 2] for affine variety codes using the BMS algorithm and DFT. Let \(M = \{X_1^{a_1} \cdots X_m^{a_m} \mid (a_1, \ldots, a_m) \in \mathbb{Z}_q^m, 0 \leq a_1, \ldots, a_m \leq q - 1\}\).

**Definition 2.4** (Discrete Fourier transform). A linear map \(\mathcal{F}\) is defined by

\[
\mathcal{F} : F_q^{A_m} \to F_q^M, \quad (c_P)_{P \in A_m} \mapsto \left(\sum_{P \in A_m} c_P h(P)\right)_{h \in M}.
\]

The map \(\mathcal{F}\) is called a discrete Fourier transform (DFT) on \(F_q^{A_m}\).

The following map is the inverse of \(\mathcal{F}\) (cf. [17]), and it is called an inverse discrete Fourier transform (IDFT).

**Definition 2.5.** For each \(P = (\omega_1, \ldots, \omega_m) \in A_m\), we define a subset \(\text{supp}(P)\) of \(\{1, \ldots, m\}\) by \(\text{supp}(P) := \{i \mid a_i \neq 0 \ (1 \leq i \leq m)\}\). Then a linear map \(\mathcal{F}^{-1}\) is defined by

\[
\mathcal{F}^{-1} : F_q^M \to F_q^{A_m}, \quad (r_h)_{h \in M} \mapsto (c_P)_{P \in A_m},
\]

where

\[
c_P = (-1)^{\sharp \text{supp}(P)} \times \
\sum_{l_1, \ldots, l_{\sharp \text{supp}(P)} = 1} \left\{ \sum_{J \subseteq \text{supp}(P)^c} (-1)^{|J|} r_{h(P, l, J)} \right\} \prod_{i \in \text{supp}(P)} a_i^{-l_i},
\]

\(J\) runs over all subsets of \(\{1, \ldots, m\} \setminus \text{supp}(P)\), and \(h(P, l, J) = X_1^{b_1} \cdots X_m^{b_m}\) is a monomial such that

\[
b_i = \begin{cases} 
  l_i & \text{if } i \in \text{supp}(P), \\
  q - 1 & \text{if } i \in J, \\
  0 & \text{if } i \notin \text{supp}(P) \cup J.
\end{cases}
\]

Fix a monomial order \(\prec\) of \(M\), and let \(G_{\Psi}\) be a Gröbner basis for the ideal \(Z(\Psi)\) (see [6], [7] or [22] for the theory of Gröbner basis). Let \(f \in F_q[X_1, \ldots, X_m]\), where \(f = \sum_{h \in M} \lambda_h h\) for
some coefficients $\lambda_h \in \mathbb{F}_q$. We define the leading monomial $\text{LM}(f)$ of $f(X)$ with respect to $\prec$ by

$$\text{LM}(f) = \max_{h \in M} \{ h \in M \mid \lambda_h \neq 0 \}. \quad (2.5)$$

Define $\text{mdeg}(X_1^{a_1} \cdots X_m^{a_m}) := (a_1, \ldots, a_m)$. For a subset $\Phi \subset \Psi$, we define a subset $D(\Phi)$ of $M$ such that

$$D(\Phi) = \mathbb{N}_0^m \setminus \{ \text{mdeg}(\text{LM}(f)) \mid 0 \neq f \in Z(\Phi) \}, \quad (2.6)$$

where $\mathbb{N}_0$ is the set that consists of 0 and natural numbers. The set $D = D(\Phi)$ is called the delta set of $\Phi$ (cf. [22]).

**Definition 2.6.** We define a linear map $\mathcal{E}_\Phi$ by

$$\mathcal{E}_\Phi : \mathbb{F}_q^{D(\Phi)} \to \mathbb{F}_q^M, \quad (r_h)_{h \in D(\Phi)} \mapsto (r_g)_{g \in M},$$

where for $g \in M$,

$$r_g = \sum_{h \in D(\Phi)} v_h r_h,$$

$v_h$ is obtained by the division algorithm by $G_{\Phi} = \{ f^{(w)} \}_{0 \leq w < z}$:

$$g(X) = \sum_{0 \leq w < z} u^{(w)}(X) f^{(w)}(X) + v(X)$$

for some $u^{(w)}(X) \in \mathbb{F}_q[X_1, \ldots, X_m]$ and $v(X) := \sum_{h \in D(\Phi)} v_h h \in \mathbb{F}_q[X_1, \ldots, X_m]$.

**Definition 2.7.** A linear map $\mathcal{C}_\Phi$ is defined by the composition $\mathcal{C}_\Phi = \mathcal{R}_\Phi \circ \mathcal{F}^{-1} \circ \mathcal{E}_\Phi : \mathbb{F}_q^{D(\Phi)} \to \mathbb{F}_q^\Phi$, where $\mathcal{R}_\Phi$ is the restriction map from $\mathbb{F}_q^{\Lambda_m}$ to $\mathbb{F}_q^\Phi$.

It has been shown [17] that $\mathcal{C}_\Phi$ is a linear isomorphism. Algorithm 1 is a decoding algorithm for affine variety codes. Let $\Phi_0$ be a subset of $\Psi$ such that $\text{span}_{\mathbb{F}_q}(D(\Phi_0)) = L$, and let $B = D(\Phi_0)$. Suppose that $\Phi \subset \Psi$ is equal to the set of error locations of a received word.

**Remark.** This algorithm works if $2|\Phi| < d_{\text{FR}}(C(L, \Psi))$, where $d_{\text{FR}}(C(L, \Psi))$ is a Feng-Rao bound (see [1], [7], [10], [19] for Feng-Rao bounds).

**Algorithm 1** Decoding of affine variety codes (cf. [17])

**Input:** A received word $(r_P)_{P \in \Psi} \in \mathbb{F}_q^\Psi$

**Output:** $(c_P)_{P \in \Psi} \in C^\perp(L, \Psi)$

Step 1. $(\bar{r}_h)_{h \in B} := (\sum_{P \in \Psi} r_{ph}(P))_{h \in B}$.

Step 2. Calculate $G_{\Phi}$ from the syndrome $(\bar{r}_h)_{h \in B}$ by BMS algorithm (cf. [5], [7]).

Step 3. $(e_P)_{P \in \Psi} = \mathcal{C}_\Phi((\bar{r}_h)_{h \in B})$.

Step 4. $(c_P)_{P \in \Psi} = (r_P)_{P \in \Psi} - (e_P)_{P \in \Psi} \in C^\perp(L, \Psi)$. 

5
3 Representation as Affine Variety Codes

Although a PRM code is expressed as an affine variety code, in this section, we represent an example of a PRM code to which Algorithm 1 does not apply directly. We assume that $q > 2$.

**Definition 3.1.** The evaluation map

\[ \text{ev} : R \rightarrow \mathbb{F}_q^n \] (3.1)

is defined by

\[ \text{ev}(f) := (f(P))_{P \in \mathbb{F}_q^n} \] (3.2)

for $f \in R$.

Then, ev is a surjective $\mathbb{F}$-algebra homomorphism (see [11] or [17]). We write $X^a := X_0^{a_0}X_1^{a_1} \cdots X_m^{a_m}$ and $|a| := a_0 + a_1 + \cdots + a_m$ for $a = (a_0, a_1, \ldots, a_m) \in \mathbb{N}_0^{m+1}$. We define a monomial order $\prec$ as following manner: $X^a \prec X^b$ if “$|a| < |b|$” or “$|a| = |b|$ and there exists an index $\ell$ such that $a_m = b_m, a_{m-1} = b_{m-1}, \ldots, a_{\ell+1} = b_{\ell+1}$ and $a_{\ell} < b_{\ell}$.”

First, we present examples of Gröbner bases for $\ker(\text{ev})$ with respect to $\prec$ in low-dimensional cases.

**Definition 3.2.** We define a set of polynomials $\mathcal{G}$ as follows:

1. When $m = 1$, we set

\[ \mathcal{G} := \{ X_1^q - X_1, (X_1 - 1)(X_0 - 1), X_0^2 - X_0 \} \]

2. When $m = 2$, we set

\[ \mathcal{G} := \{ X_2^q - X_2, X_1^q - X_1, (X_2 - 1)(X_1 - 1)(X_0 - 1), (X_1^2 - X_1)(X_0 - 1), X_0^2 - X_0 \} \]

3. When $m = 3$, we set

\[ \mathcal{G} := \{ X_3^q - X_3, X_2^q - X_2, X_1^q - X_1, (X_3 - 1)(X_2 - 1)(X_1 - 1)(X_0 - 1), (X_2^2 - X_2)(X_1 - 1)(X_0 - 1), (X_1^2 - X_1)(X_0 - 1), X_0^2 - X_0 \} \]

The inclusion $\mathcal{G} \subseteq \ker(\text{ev})$ immediately follows. Let $\langle \mathcal{G} \rangle$ denote the ideal generated by $\mathcal{G}$. By Buchberger’s criterion (see [4, Theorem 2.6.6]), we can directly verify that $\mathcal{G}$ is a Gröbner basis for $\langle \mathcal{G} \rangle$.

For an ideal $J$ of $R$, the delta set $\Delta(J)$ of $J$ is defined by

\[ \Delta(J) := \mathbb{N}_0^{m+1} \setminus \{ \text{LM}(f) \mid 0 \neq f \in J \} \] (3.3)

Then, the elements in $\{ X^a \mid a \in \Delta(J) \}$ are called standard monomials. It is known that the standard monomials form a basis for $R/J$ over $\mathbb{F}_q$ (see [22, Theorem 19]).
**Proposition 3.3.** The set of standard monomials for \( \langle G \rangle \) is as follows:

1. \( \{X_0X_1^a \mid 0 \leq a \leq q - 1\} \cup \{X_0\} \) if \( m = 1 \),
2. \( \{X_0^aX_2^b \mid 0 \leq a, b \leq q - 1\} \cup \{X_0X_2^a \mid 0 \leq a \leq q - 1\} \cup \{X_0X_1\} \) if \( m = 2 \),
3. \( \{X_0^aX_2^bX_3^c \mid 0 \leq a, b, c \leq q - 1\} \cup \{X_0X_2^aX_3^b \mid 0 \leq a, b \leq q - 1\} \cup \{X_0X_1X_3^a \mid 0 \leq a \leq q - 1\} \cup \{X_0X_1X_2\} \) if \( m = 3 \).

We note that the cardinality of \( G \) is given by \( n = q^m + q^{m-1} + \cdots + 1 \) for all \( m = 1, 2, 3 \). On one hand, we recall that \( \langle G \rangle \subset \ker(\text{ev}) \). This guarantees that the natural linear map \( R/\langle G \rangle \ni \overline{f} \mapsto \overline{f} \in R/\ker(\text{ev}) \) is well-defined and surjective. Therefore, \( n = \dim_{\mathbb{F}_q}(R/\langle G \rangle) \geq \dim_{\mathbb{F}_q}(R/\ker(\text{ev})) \). On the other hand, the surjectivity of the evaluation map (3.1) implies that \( \dim_{\mathbb{F}_q}(R/\ker(\text{ev})) \geq \dim_{\mathbb{F}_q}(\mathbb{P}_q^n) = n \). Hence we have the following.

**Corollary 3.4.** Let \( q > 2 \) and \( m = 1, 2, 3 \). We have that \( \dim_{\mathbb{F}_q}(R/\ker(\text{ev})) = n \) and \( G \) is a Gröbner basis for \( \ker(\text{ev}) \).

Now, we verify that a PRM code is an affine variety code. Recall that affine variety codes are expressed as

\[
C(L, \Psi) = \{(f(P))_{P \in \Psi} \in \mathbb{F}_q^{|\Psi|} \mid f \in L\},
\]

where \( \Psi \subset \mathbb{A}^{m+1} \) and \( L \) is an \( \mathbb{F}_q \)-subspace of \( R/Z(\Psi) \). A projective space \( \mathbb{P}_m \) is identified with a set of representatives such as \( (0, \ldots, 0, 1, a_{i+1}, \ldots, a_{n}) \); then, \( \mathbb{P}_m \subset \mathbb{A}^{m+1} \). Let \( \Psi = \mathbb{P}_m \). Then, \( \ker(\text{ev}) = Z(\Psi) \). Indeed, \( f(P) = 0 \) for all \( P \in \mathbb{P}_m = \Psi \) if and only if \( (f(P))_{P \in \mathbb{P}_m} = 0 \). We also assume that \( L = \{\overline{X^a} \in R/\ker(\text{ev}) \mid a \in \mathbb{N}_{m+1}^n, |a| = \nu\} \). Then, \( C(L, \Psi) \) coincides with PRM\(_m\)(\( m, q \)) = \( \{\text{ev}(f) \mid f \in R_{\nu}\} \).

However, there is an example for which a PRM code does not have bases consisting of standard monomials for \( \ker(\text{ev}) \). In this case, Algorithm [1] cannot be applied directly [17].

**Example 3.5.** Let \( q = 9, m = 2, \nu = 3 \). The set \( \{X_0^3 | \ |a| = 3\} \) forms a basis for PRM\(_3\)(2, 9). Since \( (X_2-1)(X_1-1)(X_0-1) = X_2X_1X_0-X_2X_1-X_2X_0-X_1X_0+X_2+X_1+X_0-1 \) and \( (X_1^2-X_1)(X_0-1) = X_1^2X_0-X_1^2-X_1X_0+X_1 \), the elements of the basis can be reduced as follows:

\[
\begin{align*}
\text{ev}(X_0^3) &= \text{ev}(X_0), \\
\text{ev}(X_1X_0^2) &= \text{ev}(X_1X_0), \\
\text{ev}(X_2X_0^2) &= \text{ev}(X_2X_0), \\
\text{ev}(X_1^2X_0) &= \text{ev}(X_1^2+X_1X_0-X_1), \\
\text{ev}(X_2X_1X_0) &= \text{ev}(X_2X_1+X_2X_0+X_1X_0-X_2-X_1-X_0+1), \\
\text{ev}(X_2^2X_0) &= \text{ev}(X_1^3), \\
\text{ev}(X_1X_2) &= \text{ev}(X_1^2X_2), \text{ev}(X_1X_2^2), \text{ev}(X_2^3).
\end{align*}
\]

Therefore \( \text{ev}(X_0X_1X_2) \) can transform into \( \text{ev}(X_2X_1-X_2-X_1+1) \) by a linear transformation of PRM\(_3\)(2, 9), but it cannot transform into a standard monomial by any linear transformations.
4 Decoding Algorithm

In this section, we construct a decoding algorithm for PRM codes using the BMS algorithm and DFT. For this purpose, we divide our decoding procedure into \( m + 1 \) components identified with affine spaces, and we apply the decoding algorithm to RM codes in the separated areas. We know a decoding algorithm (Algorithm 1) for affine variety codes, including RM codes such, whereby the BMS algorithm is used to determine the error positions and the DFT is used to determine the error values.

We set \( \Psi_m := \{(0 : \cdots : 0 : 1)\} \subset \mathbb{F}_q^{m+1} \) and

\[
\Psi_i := \{(0 : \cdots : 0 : 1 : \omega_{i+1} : \cdots : \omega_m) \mid \omega_j \in \mathbb{F}_q, i + 1 \leq j \leq m\} \subset \mathbb{F}_q^{m+1}
\]

for \( i = 0, \ldots, m - 1 \). Then, \( \Psi_i \) is regarded as an \( m - i \)-dimensional affine space \( \mathbb{A}_{m-i} \) for all \( i = 0, \ldots, m \). Let \( n_{-1} := 0 \) and

\[
n_i := \sum_{j=0}^{i} q^{m-j} = q^m + q^{m-1} + \cdots + q^{m-i}
\]

for \( i = 0, \ldots, m \). Note that \( n_{i-1} + q^{m-i} = n_i \). Let \( P_1, \ldots, P_n \) be the elements in \( \mathbb{P}_m \) such that, for all \( i \),

\[
\{P_{n_{i-1}+1}, P_{n_{i-1}+2}, \ldots, P_{n_i}\} = \Psi_i.
\]

Let \( \nu \) be an integer with \( 0 < \nu \leq m(q - 1) \). Set \( \mu := m(q - 1) - \nu \). Theorem 4.1 has been proved by Sørensen [27, Theorem 2].

**Theorem 4.1.** We have the following:

1. \( \text{PRM}_\nu(m, q) \perp = \text{PRM}_\mu(m, q) \) if \( \nu \neq 0 \) (mod \( q - 1 \)),

2. \( \text{PRM}_\nu(m, q) \perp = \text{span}_{\mathbb{F}_q} \{1, \text{PRM}_\mu(m, q)\} \) if \( \nu \equiv 0 \) (mod \( q - 1 \)), where \( 1 = (1, \ldots, 1) \in \mathbb{F}_q^n \).

Fix an integer \( i \) with \( 0 \leq i \leq m \). Let \( \mathbf{a} = (a_0, a_1, \ldots, a_m) \in \mathbb{N}_0^{m+1} \) such that \( |\mathbf{a}| = \mu \) and \( a_0 = a_1 = \cdots = a_{i-1} = 0, a_i > 0 \). Let \( h := X^{a_0}X_{i+1}^{a_{i+1}} \cdots X_m^{a_m} \) and \( \tilde{h} := X_{i+1}^{a_{i+1}} \cdots X_m^{a_m} \). Then, \( \tilde{h} \) is a monomial of degree less than \( \mu \) in \( X_{i+1}, \ldots, X_m \).

Let \( (c_P)_{P \in \mathbb{F}_m} \) be a codeword in \( \text{PRM}_\nu(m, q) \). There exists a homogeneous polynomial \( f \in R \) of degree \( \nu \) such that \( (c_P)_{P \in \mathbb{F}_m} = (f(P))_{P \in \mathbb{F}_m} \). After an error vector \( (e_P)_{P \in \mathbb{F}_m} \) occurs, assume that we receive the word \( (r_P)_{P \in \mathbb{F}_m} = (c_P)_{P \in \mathbb{F}_m} + (e_P)_{P \in \mathbb{F}_m} \). Set \( B_i := \{X^{\mathbf{a}} \in R \mid |\mathbf{a}| = \nu\} \), \( B_i(\mu) := \{X^{\mathbf{a}} \in B_i \mid |\mathbf{a}| = \mu\} \) for any \( i = 0, 1, \ldots, m \). The set of monomials in \( R_\mu \) is divided into the disjoint union \( \bigcup_{i=0}^m B_i(\mu) \). Let

\[
(\overline{v}_P)_{P \in \mathbb{A}_{m-i}} := (v_P)_{P \in \Psi_i} = (v_{P_{n_{i-1}+1}}, \ldots, v_{P_{n_i}})
\]

for \( (v_P)_{P \in \mathbb{F}_m} = (v_{P_1}, \ldots, v_{P_n}) \in \mathbb{F}_q^n \). We set \( \overline{P} := (\omega_{i+1}, \ldots, \omega_m) \in \mathbb{F}_q^{m-i} \) for \( P = (0 : \cdots : 0 : 1 : \omega_{i+1} : \cdots : \omega_m) \in \mathbb{F}_q^{m+1} \).

When \( 0 \leq i \leq m \), the decoding algorithm proceeds inductively. Suppose that we already know error vectors in the \( \Psi_0, \Psi_1, \ldots, \Psi_{i-1} \) parts, i.e., the value \( e_{P_j} \) has been determined for \( P \in \bigcup_{j=0}^{i-1} \Psi_j \). Set \( r_P^{(i)} := r_P - e_P \) for \( P \in \bigcup_{j=0}^{i-1} \Psi_j \) and \( r_P^{(i)} := r_P \) for \( P \in \bigcup_{j=i}^m \Psi_j \). Then

\[
(r_P^{(i)})_{P \in \mathbb{F}_m} = (r_P) - (e_{P_1}, \ldots, e_{P_{n_{i-1}}}, 0, \ldots, 0) = (c_P) + (0, \ldots, 0, e_{P_{n_{i-1}+1}}, \ldots, e_{P_n}).
\]
Theorem 4.2. Fix an integer \( i \) with \( 0 \leq i \leq m \). Let \( f \in R_\nu \) and \( c_P := f(P) \) for all \( P \in \mathbb{P}_m \). Let \((e_P)_{P \in \mathbb{P}_m} \in \mathbb{F}_q^m\) such that \( e_P = 0 \) for all \( P \in \bigcup_{j=1}^{i-1} \Psi_j \). Set \((r_P)_{P \in \mathbb{P}_m} := (c_P)_{P \in \mathbb{P}_m} + (e_P)_{P \in \mathbb{P}_m}\). Then, for a monomial \( h = X_i^{a_i}X_{i+1}^{a_{i+1}} \cdots X_m^{a_m} \) of degree \( \mu \) with \( a_i > 0 \), we have

\[
\langle (r_P)_{P \in \mathbb{P}_m}, (h(P))_{P \in \mathbb{P}_m} \rangle = \langle (\tilde{r}_P)_{\tilde{P} \in A_{m-i}}, (\tilde{h}(\tilde{P}))_{\tilde{P} \in A_{m-i}} \rangle.
\]

Proof. We note that \( h(P) = 0 \) if \( P \in \bigcup_{j=i+1}^m \Psi_j \), since the \( i \)-th exponent of \( h \) is positive and the \( i \)-th entry of \( P \) is 0. Therefore

\[
\langle (r_P)_{P \in \mathbb{P}_m}, (h(P))_{P \in \mathbb{P}_m} \rangle = \langle (e_P)_{P \in \mathbb{P}_m}, (h(P))_{P \in \mathbb{P}_m} \rangle
\]

(since \( \text{PRM}_\mu(m, q) \subset \text{PRM}_\nu(m, q) \perp \) by Theorem 4.1)

\[
= \sum_{P \in \bigcup_{j=i+1}^m \Psi_j} e_P h(P)
\]

\[
= \sum_{P \in \Psi_i} e_P h(P)
\]

(since \( h(P) = 0 \) for \( P \in \bigcup_{j=i+1}^m \Psi_j \))

\[
= \langle (\tilde{r}_P)_{\tilde{P} \in A_{m-i}}, (\tilde{h}(\tilde{P}))_{\tilde{P} \in A_{m-i}} \rangle,
\]

as desired. \( \square \)

Theorem 4.2 implies that the temporary received word \((r_P^{(i)})_{P \in \mathbb{P}_m}\) produces syndromes for \( \text{RM}_{\mu-1}(m-i, q) \perp \). By (2.2), the order of \( \text{RM}_{\mu-1}(m-i, q) \perp \) is

\[
(m-i)(q-1) - (\mu-1) - 1 = m(q-1) - \mu - i(q-1) = \nu - i(q-1),
\]

and thus

\[
\text{RM}_{\mu-1}(m-i, q) \perp = \text{RM}_{\nu-i(q-1)}(m, q).
\] (4.2)

If \( i \) satisfies \( \mu-1 < (m-i)(q-1) \) (or equivalently \( \nu - i(q-1) \geq 0 \)), by Theorem 4.2 we obtain the syndromes related to \( \text{RM}_{\mu-1}(m-i, q) \perp = \text{RM}_{\nu-i(q-1)}(m, q) \). Therefore, after applying Algorithm 1 we obtain the error vector in the \( \Psi_i \)-part.

If \( i \) satisfies \( \mu-1 \geq (m-i)(q-1) \) (or equivalently \( \nu - i(q-1) < 0 \)), then \( \text{RM}_{\mu-1}(m-i, q) = \mathbb{F}_q^{m-i} \) and syndromes obtained by Theorem 4.2 occupy all the entries of \( \mathbb{F}_q^{m-i} \). Therefore, the IDFT corrects arbitrary errors that occurred in the \( \Psi_i \)-part. Indeed, we have

\[
\mathcal{F}^{-1}_i((r_P)_{P \in \mathbb{P}_m}, (h(P))_{P \in \mathbb{P}_m}))_{h \in B_i(\mu)} = \mathcal{F}^{-1}_i(\sum_{\tilde{P} \in A_{m-i}} \tilde{e}_{\tilde{P}} \tilde{h}(\tilde{P}))_{h \in B_i(\mu)}
\]

\[
= \mathcal{F}^{-1}_i(\tilde{e}_P)_{\tilde{P} \in A_{m-i}}
\]

\[
= (\tilde{e}_{\tilde{P}})_{\tilde{P} \in A_{m-i}}.
\]
where $\mathcal{F}_i$ and $\mathcal{F}_i^{-1}$ are the DFT and IDFT corresponding to $A_{m-i}$ respectively.

Remark. We always apply Algorithm 1 to the $\Psi_0$-part and the IDFT to the $\Psi_m$-part, since $\mu - 1 < m(q - 1)$ and $\mu - 1 > 0$. Algorithm 2 is a summary of the decoding method described above.

Next, we calculate the total complexity of Algorithm 2.

**Definition 4.3.** Let $N_i = q^{m-i}$ be the cardinality of an $(m-i)$-dimensional affine space. The computational complexities of error-detection and error-evaluation for an affine variety code are $O(z_i N_i^2) = O(z_i q^{2m-2i})$ [3], [7] and $O(q N_i^2) = O(q^{2m-2i+1})$ [17], respectively, where $z_i$ is the cardinality of the Gröbner basis obtained by the BMS algorithm for the $\Psi_i$-part. We note that $z_i < q^{m-i}$ for all $i = 0, 1, \ldots, m$. Then the computational complexity of the $\Psi_i$-part is $O(w_i q^{2m-2i})$, where $w_i := \max\{z_i, q\}$. Therefore, the total computational complexity of Algorithm 2 is

$$O(w_0 q^{2m} + w_1 q^{2m-2} + w_2 q^{2m-4} + \cdots + w_m).$$

Moreover, we have the following.

**Proposition 4.4.** Let $n = q^m + q^{m-1} + q^{m-2} + \cdots + 1$ be the length of $\text{PRM}_\nu(m, q)$. Let $z_i$ be the cardinality of the Gröbner basis obtained by the BMS algorithm for the $\Psi_i$-part. We set $w := \max\{q, z_0, z_1, \ldots, z_m\} < q^m < n$. Then, the total complexity of Algorithm 2 is $O(wn^2)$.

**Proof.** For all $q > 1$, we have $q^2 < q^2 - 1$. Therefore

$$w_0 q^{2m} + w_1 q^{2m-2} + w_2 q^{2m-4} + \cdots + w_m \leq w(q^{2m} + q^{2(m-1)} + q^{2(m-2)} + \cdots + 1^2) = \frac{w q^{2m+2} - 1}{q^2 - 1} \leq \frac{2q^{2m+2}}{q^2} = 2w q^{2m}.$$

In addition, we prove that $wn^2 = \theta(wq^{2m})$. The inequality $wq^{2m} < wn^2$ is clear for all $q > 1$. For all $q > 3$, we have

$$(q - 1)^2 - \frac{q^2}{2} = \frac{1}{2}(q^2 - 4q + 2) = \frac{1}{2}(q - 2)^2 - 1 > 0,$$

and thus $\frac{1}{(q-1)^2} < \frac{2}{q^2}$. Therefore

$$wn^2 = w \left(\frac{q^{m+1} - 1}{q - 1}\right)^2 < w \frac{q^{2m+2}}{(q - 1)^2} < 2wq^{2m}.$$

**Remark.** It is possible to apply the Feng–Rao decoding algorithm [1], [10], [18], [19] and the algorithm that uses error-correction pairs [21] to PRM codes. However, the total complexity of our algorithm is less than that of these two algorithms (i.e., $O(n^3)$).
Algorithm 2 Decoding algorithm for PRM$_\nu(m, q)$

Input: A received word $(r_P)_{P \in \mathbb{P}_m} \in \mathbb{F}_q^n$

Output: The error vector $(e_P)_{P \in \mathbb{P}_m}$ of $(r_P)_{P \in \mathbb{P}_m} \in \mathbb{F}_q^n$

for $i = 0, \ldots, m$

Step 1.

if $i = 0$

then

$r^{(0)}_P := r_P$.

else

$i > 0$

$r^{(i)}_P := r_P - e_P$ for $P \in \bigcup_{j=0}^{i-1} \Psi_j$,

$r^{(i)}_P := r_P$ for $P \notin \bigcup_{j=0}^{i-1} \Psi_j$.

end if

end for

Step 2. Let $S^{(i)}_u := \langle (r^{(i)}_P)_{P \in \mathbb{P}_m}, u \rangle$ for $u \in \text{ev}(B_i(\mu))$.

if $\nu - (q-1)i \geq 0$

then

Calculate $(e_P)_{P \in \Psi_i}$ by Algorithm 1 as decoding of RM$_{\nu-(q-1)i}(m, q)$ from syndromes $\{S^{(i)}_u\}_{u \in \text{ev}(B_i(\mu))}$.

else

Calculate $(e_P)_{P \in \Psi_i} = \mathcal{F}_i^{-1}((S^{(i)}_u)_{u \in \text{ev}(B_i(\mu))})$.

end if

end for

5 Numbers of Correctable Errors

Let $\mu = m(q-1) - \nu$. Let $i_0 \geq 0$ be the smallest integer such that RM$_{\mu-1}(m-i_0, q)$\perp = $\mathbb{F}_q^{m-i_0}$, i.e., $i_0$ is the smallest integer satisfying $\nu - i_0(q-1) \leq -1$. The numbers of errors that can be corrected by our algorithm (Algorithm 2) are discussed in Proposition 5.1 and listed in Table 2.

Proposition 5.1. Let PRM$_\nu(m, q)$ be a PRM code. Set

$$t_0 := \left\lfloor \frac{(q-s)q^{m-r-1}-1}{2} \right\rfloor,$$  \hspace{1cm} (5.1)

where $\nu = r(q-1) + s$, $0 \leq s < q - 1$, $0 \leq r \leq m - 1$. For our algorithm, the decoding method and the number of correctable errors for the $\Psi_i$-part are as follows:

1. If $0 \leq i \leq i_0$, then Algorithm 1 for RM$_{\nu-(q-1)i}(m-i, q)$ corrects $t_0$ errors.

2. If $i_0 < i \leq m$, then the IDFT corrects $q^{m-i}$ errors.

Proof. Point 2 has already been proved. We prove point 1. We recall that

$$d_{\text{min}}(\text{RM}_\nu(m, q)) = (q-s)q^{m-r-1},$$

$(\nu = r(q-1) + s$, $0 \leq s < q - 1$, $0 \leq r \leq m - 1)$.

In the $\Psi_0$-part of Algorithm 2, we always apply Algorithm 1 to RM$_{\mu-1}(m, q)$\perp = RM$_\nu(m, q)$. Since there exists an ordered basis for an RS code such that its Feng–Rao bound coincides with its minimum distance [12], the number of correctable errors in $\Psi_0$-part is $t_0$. 

11
Let $0 < i \leq i_0$. We apply Algorithm 1 to $\text{RM}_{\mu-1}(m-1, q) = \text{RM}_{\nu-i(q-1)}(m, q)$ in the $\Psi_i$-part (see Section 4). The quotient and remainder obtained when $\nu - i(q - 1)$ is divided by $q - 1$ are $r - i$ and $s$, respectively. Therefore,

$$d_{\text{FR}}(\text{RM}_{\nu-i(q-1)}(m - i, q)) = d_{\text{min}}(\text{RM}_{\nu-i(q-1)}(m - i, q)) = (q - s)q^{(m-i)-(r-i)-1} = (q - s)q^{m-r-1},$$

and the number of correctable errors in the $\Psi_i$-part coincides with that in the $\Psi_0$-part. \hfill \square

Proposition 5.1 immediately implies the following.

**Proposition 5.2.** Our decoding algorithm (Algorithm 2) for $\text{PRM}_{\nu}(m, q)$ always corrects $t_0 = \left\lfloor \frac{(q-s)q^{m-r-1}-1}{2} \right\rfloor$ errors, where $\nu = r(q - 1) + s$, $0 \leq s < q - 1$, $0 \leq r \leq m - 1$.

**Remark.** The number $t_0$ is the same as the number of correctable errors for the RM code corresponding to the $\Psi_0$-part by Algorithm 1. The advantages of our algorithm are that a PRM code is longer than the corresponding RM code and the code parameters are more flexible. Note that Table 2 lists the numbers of spacial errors which are limited component-wise. If we consider such situation, our algorithm can correct more errors than Algorithm 1 for the RM code corresponding to the $\Psi_0$-part.

| Component of $F_m$ | Corresponding code | Correctable |
|---------------------|--------------------|-------------|
| $\Psi_0$            | $\text{RM}_{\mu-1}(m, q)$ | $t_0$       |
| $\Psi_1$            | $\text{RM}_{\mu-1}(m - 1, q)$ | $t_0$       |
| $\Psi_2$            | $\text{RM}_{\mu-1}(m - 2, q)$ | $t_0$       |
| ...                 | ...                | ...         |
| $\Psi_{i_0-1}$      | $\text{RM}_{\mu-1}(m - i_0 + 1, q)$ | $t_0$       |
| $\Psi_{i_0}$        | $(F_q^{m-i_0})$ | $q^{m-i_0} - \sharp \Psi_{i_0}$ |
| ...                 | ...                | ...         |
| $\Psi_{m-1}$        | $(F_q^m)$ | $q^1 - \sharp \Psi_{m-1}$ |
| $\Psi_m$            | $F_q^m$ | $q^0 - \sharp \Psi_m$ |

**6 Numerical Example**

We assume that $m = 3$, $q = 4$ and $\nu = 5$. Then $\mu = 3(4 - 1) - 5 = 4$. Let $\alpha$ be a generator of the cyclic group $F_4^\times$ satisfying $\alpha^2 + \alpha + 1 = 0$, i.e., $F_q = \{0, 1, \alpha, \beta = \alpha^2\}$. Let us present a numerical example of Algorithm 2 for $\text{PRM}_{4}(3, 4)$. The parameters of $\text{PRM}_{5}(3, 4)$ are

$$k = \dim(\text{PRM}_{5}(3, 4)) = 50, \ n = 85,$$

$$d_{\text{min}}(\text{PRM}_{5}(3, 4)) = (4 - 1) \cdot 4^{3-1-1} = 12.$$
Since $5 - i(q - 1) > -1$ if $i = 0, 1$, we apply Algorithm $\textbf{II}$ to the corresponding RM codes in the $\Psi_0$-part and the $\Psi_1$-part. Since $5 - i(q - 1) \leq -1$ if $i = 2, 3$, we correct every error by applying the IDFT from syndromes in the $\Psi_2$-part and the $\Psi_3$-part. In the $\Psi_0$-part, the corresponding RM code is $\text{RM}_5(3, 4) = \{ (f(P))_{P \in \mathbb{F}_2} \mid f \in \mathbb{F}_4[X_1, X_2, X_3], \deg(f) \leq 5 \}$. Let $\prec$ be the monomial order of $\mathbb{F}_4[X_1, X_2, X_3]$ defined in Section $3$. Then

$$1 < X_1 < X_2 < X_3 < X_1^2 < X_2X_1 < X_2^2 < X_3X_1 < \ldots.$$  

The Feng–Rao bound of $\text{RM}_5(3, 4)$ with respect to $\prec$ is $8$. Therefore, our algorithm corrects $3$ errors in the $\Psi_0$-part. Similarly, in the $\Psi_1$-part, we consider $\text{RM}_2(2, 4) = \{ (f(P))_{P \in \mathbb{F}_2} \mid f \in \mathbb{F}_4[X_2, X_3], \deg(f) \leq 2 \}$ and

$$1 < X_2 < X_3 < X_2^2 < X_3X_2 < X_3^2 < X_2^3 < \ldots.$$  

The Feng–Rao bound of $\text{RM}_2(2, 4)$ with respect to $\prec$ is $8$, and therefore our algorithm corrects $3$ errors in the $\Psi_1$-part. Since $\#\Psi_2 = 4$ and $\#\Psi_3 = 1$, then our algorithm corrects $4$ errors and $1$ error in the $\Psi_2$-part and the $\Psi_3$-part respectively. As a result, our algorithm corrects a total of $3 + 3 + 4 + 1 = 11$ errors, although $\text{PRM}_5(3, 4)$ is a $5$ error-correcting code.

Let

$$[\beta, 1, 1, \alpha, 0, 1, 1, 0, \beta, \beta, 1, 0, \beta, \alpha, 1, \alpha, 1, 0, \beta, \beta, 1, 0, 0, \beta, 0, \alpha, \alpha, 0]$$  

be the coefficients of an information polynomial, which are arranged with respect to $\prec$, i.e.,

$$X_0^5 < X_1^4X_2 < X_0^4X_3 < X_2^3X_1^2 < X_0^3X_1X_2 < X_2^3X_1X_3 < X_0^3X_2X_3 < X_3^2X_2^2 < X_3^2X_1^2 < X_2^2X_1X_2 < X_2^2X_1X_3 < X_2^2X_2X_3 < X_3^2X_2^2 < X_3^2X_2X_3 < X_3^2X_1^2 < X_2^2X_1X_2 < X_2^2X_1X_3 < X_2^2X_2X_3.$$  

In Tables $3$, $4$, and $5$, the top $4$ matrices describe the $\Psi_0$-part, the next $4 \times 4$ matrix is the $\Psi_1$-part, the next $1 \times 4$ matrix is the $\Psi_2$-part and the bottom matrix is the $\Psi_3$-part. In the left-most matrix of the $\Psi_0$-part, the $(\omega_1, \omega_2)$-entry is the value of the location indexed by $(1 : \omega_1 : \omega_2 : 0)$. In the second matrix from the left of the $\Psi_0$-part, the $(\omega_1, \omega_2)$-entry is the value of the location indexed by $(1 : \omega_1 : \omega_2 : 1)$; similarly, so are the entries in the third and last matrices. In the $\Psi_1$-part, the $(\omega_2, \omega_3)$-entry is the value of the location indexed by $(0 : 1 : \omega_2 : \omega_3)$. Similarly, in the $\Psi_2$-part, the $(1, \omega)$-entry is indexed by $(0 : 0 : 1 : \omega_3)$, and the entry in the $\Psi_3$-part is indexed by $(0 : 0 : 0 : 1)$.

Tables $6$ and $7$ describe the decoding procedure in the $\Psi_0$-part. In Tables $6$ and $7$, the $(a_1, a_2)$-entry of the left-most matrix is indexed by a monomial $X_1^{a_1}X_2^{a_2}X_3^{a_3}$. The $(a_1, a_2)$-entry of the second matrix from the left is indexed by a monomial $X_1^{a_1}X_2^{a_2}X_3^{a_3}$; similarly, so are the
From the syndrome described in Table 6, we obtain the following Gröbner basis:

\[ g^{(0)}_1 = X_2^2 + \alpha X_2 + \beta X_1, \]
\[ g^{(0)}_2 = X_2 X_1 + X_2 + \alpha X_1 + \alpha, \]
\[ g^{(0)}_3 = X_1^2 + X_1, \]
\[ g^{(0)}_4 = X_3 + \alpha X_2 + 1. \]

The contents of Table 7 are obtained by applying \( E_{\Psi_0} \) to the syndrome. Therefore, by applying the IDFT to Table 7, we obtain the error vector in the \( \Psi_0 \)-part.

In the \( \Psi_1 \)-part decoding, first, we set \( r^{(1)}_P = r_P - e_P \) for \( P \in \Psi_0 \) and \( r^{(1)}_P = r_P \) for \( P \in \mathbb{F}_3 \setminus \Psi_0 \). The decoding procedure is shown in Tables 8 and 9. We obtain the following Gröbner basis:

\[ g^{(1)}_1 = X_3^2 + \beta X_2 + \beta, \]
\[ g^{(1)}_2 = X_3 X_2 + X_3 + \alpha, \]
\[ g^{(1)}_3 = X_2^2 + \beta X_2 + 1. \]

Tables 10 and 11 show syndromes obtained by the decoding procedure of the \( \Psi_2 \)-part and the \( \Psi_3 \)-part, respectively.

### Table 3: Codeword \((c_P)_{P \in \mathbb{F}_3}\)

| \( \beta \) | \( \alpha \) | 0 | \( \alpha \) | 1 | \( \beta \) | 1 | \( \beta \) | 1 | \( 1 \) | \( \alpha \) | 1 | 0 | 0 | 1 | 1 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| \( \alpha \) | \( \alpha \) | 0 | \( \alpha \) | \( \beta \) | 0 | 0 | \( \beta \) | \( \beta \) | 0 | \( \alpha \) | 0 | 0 | \( \alpha \) | \( \alpha \) | \( \alpha \) |
| 0 | 1 | \( \beta \) | \( \alpha \) | \( \alpha \) | \( \alpha \) | \( \alpha \) | \( \beta \) | 0 | 0 | 1 | 0 | 0 | \( \alpha \) | \( \alpha \) | \( \alpha \) |
| \( \alpha \) | \( \alpha \) | 0 | \( \beta \) | 1 | \( 1 \) | \( \beta \) | 1 | \( 1 \) | \( \alpha \) | \( \beta \) | 1 | 0 | 0 | \( \alpha \) | \( \alpha \) |
| 1 | \( \alpha \) | 0 | \( \beta \) | \( \beta \) | \( \beta \) | \( \beta \) | \( \beta \) | \( \beta \) | \( \beta \) | \( \beta \) | \( \beta \) | \( \beta \) | \( \beta \) | \( \beta \) | \( \beta \) |

### 7 Codeword Error Rate Comparison with MDD

In this section, we investigate the codeword error rate of our algorithm (Algorithm 2) and compare it with that of MDD (see [14], [10] for MDD). We consider two types of correctable errors. In the first case, the number of correctable errors is \( t_0 \), and such errors are always correctable (see Proposition 5.2). The second case is a specialized case, for which the numbers of correctable errors have been listed in Table 2. These two cases have different codeword error rates. We express the decoding method for the first case as Proposed Method 1 (PM1), and that for the second case as Proposed Method 2 (PM2). Let \( p \) be a symbol error rate. Then the
Table 4: Received word \((r_P)_{P \in \mathbb{F}_3}\)

\[
\begin{array}{cccccccc}
\beta & \alpha & 0 & \alpha & 1 & \beta & 1 & \beta \\
\alpha & \alpha & 0 & 0 & \alpha & \beta & 0 & 0 \\
0 & 1 & \beta & \alpha & 1 & \alpha & \alpha & \alpha \\
\alpha & 0 & 0 & \beta & \alpha & 0 & \beta & \alpha \\
1 & \alpha & 0 & \beta & \beta & \beta & \alpha & \alpha \\
\alpha & \alpha & \alpha & \alpha & \alpha & 0 & \beta & \alpha \\
1 & \beta & 0 & \alpha & \beta & \alpha & \alpha & 0 \\
\beta & \alpha & \alpha & 0 & \beta & \alpha & \alpha & 0 \\
\end{array}
\]

Table 5: Error \((e_P)_{P \in \mathbb{F}_3}\)

\[
\begin{array}{cccccccc}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\end{array}
\]

codeword error rate of PM1 is \(1 - P\), where \(P = \sum_{j=0}^{t_0} \binom{n}{j} p^j (1 - p)^{n-j}\). The codeword error rate of PM2 is \(1 - \prod_{i=0}^{t_0-1} P_i\), where

\[
P_i = \sum_{j=0}^{t_0} \binom{q^{m-i}}{j} p^j (1 - p)^j
\]

for \(i = 0, 1, \ldots, i_0 - 1\).

Tables 12, 13, and 14 list numerical examples of the numbers of correctable errors by PM1 and MDD. In these tables, the double lines denote the turning positions of the quotient obtained when \(\nu\) is divided by \(q - 1\). The difference between the decoding rates decreases when the above-mentioned quotient increases. Now, let \(t_{MD}\) be the number of correctable errors by MDD. The codeword error rate of MDD is

\[
1 - \sum_{j=0}^{t_{MD}} \binom{n}{j} p^j (1 - p)^{n-j} = 1 - P - \sum_{j=t_0+1}^{t_{MD}} \binom{n}{j} p^j (1 - p)^{n-j}.
\]

Recall that \(1 - P\) is the codeword error rate of PM1. Therefore, the lower the difference \(t_{MD} - t_0\) between the number of correctable errors by PM1 and MDD, the lower is the difference between
their codeword error rate. In the right hand side of tables 12, 13, and 14, i.e., where the quotient obtained by dividing \( \nu \) by \( q - 1 \) is \( m - 1 \), the difference is 1 or less. Further, in some cases, the codeword error rate of PM1 coincides with that of MDD.

Figs. 1, 2, and 3 show the codeword error rate for PRM\(_{14}(2,16)\), PRM\(_{17}(2,16)\), and PRM\(_9(3,8)\). Fig. 4 shows that the performance curves for PM1 and PM2 coincide; MDD yields better performance than both PM1 and PM2.

On the other hand, when \( \nu \) is sufficiently large, the performance curves of PM1 and PM2 are close to that of MDD, as shown in Fig. 2. Fig. 3 shows that the performance curve of PM2 is distinct from those of PM1 and MDD because the cardinality and number of correctable errors in this case are not negligible.

8 Conclusion

In this paper, we have constructed a decoding algorithm by dividing a projective space into a union of affine spaces. We have presented an example of a decoding procedure related to
Table 12: Numbers of correctable errors for PRMν(2, 16) by Algorithm 2 and MDD

| ν   | 5 | 8 | 11 | 14 | 17 | 20 | 23 | 26 | 29 |
|-----|---|---|----|----|----|----|----|----|----|
| Algorithm 2 | 87 | 63 | 39 | 15 | 6  | 5  | 3  | 2  | 0  |
| MDD   | 95 | 71 | 47 | 23 | 7  | 5  | 4  | 2  | 1  |
| Difference | 8  | 8  | 8  | 8  | 1  | 0  | 1  | 0  | 1  |

Table 13: Numbers of correctable errors for PRMν(3, 8) by Algorithm 2 and MDD

| ν   | 2 | 4 | 6 | 8 | 10 | 12 | 14 | 16 | 18 |
|-----|---|---|---|---|----|----|----|----|----|
| Algorithm 2 | 191 | 127 | 63 | 27 | 19 | 11 | 7  | 3  | 2  |
| MDD   | 223 | 159 | 95 | 31 | 23 | 15 | 7  | 3  | 2  |
| Difference | 32 | 32 | 32 | 4  | 4  | 4  | 0  | 0  | 0  |

Table 14: Numbers of correctable errors for PRMν(3, 16) by Algorithm 2 and MDD

| ν   | 7 | 11 | 15 | 19 | 27 | 31 | 35 | 39 |
|-----|---|----|----|----|----|----|----|----|
| Algorithm 2 | 1151 | 639 | 127 | 95 | 31 | 7  | 5  | 3  |
| MDD   | 1279 | 767 | 255 | 103 | 39 | 7  | 5  | 3  |
| Difference | 128 | 128 | 128 | 8  | 8  | 8  | 0  | 0  |

a 3-dimensional projective space. To the best of our knowledge, this is the first example for the 3-dimensional case in the literature. Further, we have proved that the total complexity of our algorithm is $O(wn^2)$, where $w$ is the maximum of $q$ and the cardinalities of Gröbner bases obtained by the BMS algorithm for all affine components. Moreover, the complexity of our algorithm is less than that of Feng–Rao decoding algorithm and the algorithm that use error-correction pairs. We also have determined the number of correctable errors of our algorithm. Although it is the same as number of errors for the RM code corresponding to the $\Psi_0$-part, the advantages of our algorithm are that the codeword is longer and the choice of code parameters increases depending on the application. In addition, if we consider only limited errors component-wise, our algorithm provides greater correcting capability than the RM code corresponding to the $\Psi_0$-part. Finally, we have compared the codeword error rate of three types of decoding procedures. When the order of a PRM code is sufficiently high, the codeword error rates of our algorithm is close to that of MDD. In particular, the rates of our algorithm and MDD are the same for some high orders. Further improvement of our algorithm is required to decrease the difference between its codeword error rate and that of MDD. This could be a topic for future studies concerned with the decoding theory of PRM codes.

Acknowledgment

This work was supported in part by a Grant-in-Aid for Research Activity Start-up (26887043) from JSPS and a grant under the Strategic Research Foundation Grant-aided Project for Private Universities from MEXT (S1311034).
Figure 1: Comparison of codeword error rates for $\text{PRM}_{14}(2,16)$

Figure 2: Comparison of codeword error rates for $\text{PRM}_{17}(2,16)$

References

[1] H. E. Andersen, O. Geil, “Evaluation codes from order domain theory,” *Finite Fields Appl.*, vol.14, no.1, pp.92-123, Jan. 2008

[2] S. Ballet, R. Rolland, “On low weight codewords of generalized affine and projective Reed–Muller codes,” *Designs Codes Cryptogr.*, vol.73, no.2, pp.271-297, Nov. 2014

[3] T. P. Berger, L. de Maximy, “Cyclic Projective Reed–Muller Codes,” In Proc. of Applied Algebra, Algebraic Algorithms and Error Correcting Codes, vol. 2227, pp.77-81, Oct. 2001.

[4] I. F. Blake and R. C. Mullin, *The Mathematical Theory of Coding*, New York: Academic Press, 1975.
Figure 3: Comparison of codeword error rates for PRM₉(3, 8)

[5] M. Bras-Amoós, M. E. O'Sullivan, “The correction capability of the Berlekamp–Massey–Sakata algorithm with majority voting,” Appl. Algebr. Eng. Commun. Comput., vol.17, no.5 pp.315-335, May 2006.

[6] D. Cox, J. Little, D. O'Shea, Ideals, Varieties, and Algorithms, 2nd ed., Springer, Berlin, 1997.

[7] D. Cox, J. Little, D. O’Shea, “The Berlekamp–Massey–Sakata algorithm,” Using Algebraic Geometry, 2nd ed., Chapter 10, pp.494-532, Springer, Berlin, 2005.

[8] A. Dür, “The decoding of extended Reed–Solomon codes,” Discrete Math., vol.90, issue 1, pp.21-40, June 1991.

[9] I. Duursma, “Decoding codes from curves and cyclic codes,” PhD. Thesis, Technische Universität Eindhoven.

[10] G. L. Feng, T. R. N. Rao, “Decoding algebraic geometric codes up to the designed minimum distance,” IEEE Trans. Inf. Theory, vol.39, pp.36-47, Jan. 1993.

[11] J. Fitzgerald, R. F. Lax, “Decoding affine variety codes using Gröbner bases,” Designs Codes Cryptogr., vol.13, no.2, pp.147-158, Feb. 1998

[12] P. Hejinen, R. Pellikaan, “Generalized Hamming Weights of q-ary Reed–Muller codes,” IEEE Trans. Inf. Theory, vol.44, no.1, pp.181-196, Jan. 1998.

[13] M. Hirotomo, M. Morii, “Decoding for doubly lengthened Reed–Solomon codes,” The 23rd symposium on information theory and its applications (SITA2000), pp.173-176, Oct. 2000. (in Japanese)

[14] J. Justesen, T. Høholdt, A Course in Error-Correcting Codes, European Mathematical Society Publishing House, 2004.
[15] G. Lachaud, “Projective Reed–Muller codes,” in Lect. Notes in Comp. sci., vol.311, Berlin: Springer 1988.

[16] F. J. MacWilliams, N. J. A. Slone, The Theory of Error-Correcting Codes, North-Holland, 1997.

[17] H. Matsui, “Lemma for linear feedback shift registers and DFTs applied to affine variety codes,” IEEE Trans. Inf. Theory, vol.60, no.5, pp.2751-2769, May 2014.

[18] R. Matsumoto, S. Miura, “On the Feng–Rao bound for the $L$-construction of algebraic geometry codes,” IEICE Trans. Fundam. Electron. Commun. Comput., E83-A, no.5, pp.923-926, May 2000.

[19] S. Miura, “Linear codes on affine algebraic varieties,” Trans. IEICE, vol.J81-A, no.10, pp.1386-1397, Oct. 1998. (in Japanese)

[20] N. Nakashima, H. Matsui, “A decoding algorithm for projective Reed–Muller codes of 2-dimensional projective space with DFT,” 2014 international symposium on information theory and its applications (ISITA2014), Melbourne, Australia, pp.371-375, Oct. 26-29, 2014.

[21] R. Pellikaan, “On decoding by error location and dependent sets of error positions,” Discrete Math., vol.106/107, pp.369-381, Sep. 1992.

[22] K. Saints, C. Heegard, “Algebraic–geometric codes and multidimensional cyclic codes: Theory and algorithms for decoding using Gröbner bases,” IEEE Trans. Inf. Theory, vol.41, no.6, pp.1733-1751, Nov. 1995.

[23] S. Sakata, “Finding a minimal set of linear recurring relations capable of generating a given finite two-dimensional array,” J. Symb. Comput., vol.5, no.3, pp.321-337, June 1988.

[24] S. Sakata, “Extension of the Berlekamp–Massey algorithm to $n$ dimensions,” Inform. Comput., vol.39, no.2, pp.207-239, Feb. 1990.

[25] S. Sakata, H. E. Jensen, T. Høholdt, “Generalized Berlekamp–Massey decoding of algebraic-geometric codes up to half the Feng-Rao bound,” IEEE Trans. Inf. Theory, vol.41, no.6, Part I, pp.1762-1768, Nov. 1995.

[26] S. Sakata, D. A. Leonard, H. E. Jensen, T. Høholdt, “Fast erasure-and-error decoding of algebraic geometry codes up to the Feng–Rao bound,” IEEE Trans. Inf. Theory, vol.44, no.4, pp.1558-1564, July 1998.

[27] A. B. Sørensen, “Projective Reed–Muller codes,” IEEE Trans. Inf. Theory, vol.37, pp.1567-1576, Nov. 1991.