射影空間の分解を用いた射影Reed–Muller符号の復号法とその性能評価

中島　規博　(豊田工業大学)*

概　　要

誤り訂正符号の符号化・復号化のプロセスでは，ディジタル通信などにおいて生じる誤りを自動的に修正し元の情報を復元することを目的とする．宇宙船通信の分野では，訂正能力の高い代数的符号であるReed–Solomon(RS)符号・Golay符号・Reed–Muller(RM)符号などの復号法の研究が進み，1972年のマリナー計画では符号長32の1次RM符号を使って火星写真の電送に成功した．本講演ではRM符号の射影化として定義された射影RM符号の復号法について発表する．本研究は豊田工業大学松井一氏との共同研究である．

1. 序文

誤り訂正符号では，以下に示されるようにディジタル通信などにおいて生じるエラーを自動的に修正し元の情報を復元することを目的とする．以下ではcは符号語，eは誤り（ベクトル），$r = c + e$は受信語を表す．

送信元 $\xrightarrow{\text{情報}}$ 符号化器 $\xrightarrow{c}$ 通信路 $\xrightarrow{r}$ 復号器 $\xrightarrow{\text{元情報}}$ 受信者

誤り訂正符号は，Reed–Solomon(RS)符号，Golay符号・Reed–Muller(RM)符号といった代数的符号と畳み込み符号，Low-Density Parity–Check(LDPC)符号といった非代数的符号に大別される．代数的符号の符号化・復号化の過程は処理速度の点で非代数的符号（特にLDPC符号）に劣るが，理論的な訂正可能数が求まる場合が多いため非代数的符号のデータ処理と比べて高い信頼制度を有する．特にRS符号は，現代の社会生活に欠かせないCD，DVD，ハードディスク，二次元バーコード（QRコード）の誤り訂正に応用されている．

本稿で扱う射影RM符号は（古典的な）RM符号の射影化として1988年にLachaud [10]によって定義された．その後すぐにSørensen [16]により，射影RM符号の最小距離と双対符号が決定された．またBergerとMaximy [3]は射影RM符号が巡回符号あるいは準巡回符号であるための条件を与えた．最近の研究では，BalletとRolland [2]による低重みの符号語の検証と二番目の重みの評価がなされている．一方で射影RM符号の復号法に関する研究は低次元の射影空間に対応する射影RM符号の計算例が知られているのみである．(例えば[7]には1次元射影空間，[8]には2次元射影空間に対応する符号の復号計算例がある．)

本研究の目的はすべての射影RM符号に有効に働く復号法を構成することである．そのために代数幾何学の基礎である射影空間のアフィン空間の和集合への分解を用いる．射影空間の各アフィン成分に対して，誤り位置の情報を持つイデアルのグレブナー基

本研究は科研費 (課題番号:26887043) の助成を受けたものである。
2010 Mathematics Subject Classification: 94B35, 13P10
キーワード : error-correcting codes, projective Reed–Muller codes, Gröbner basis, Berlekamp–Massey–Sakata algorithm, discrete Fourier transform

* 〒 468-8511 愛知県名古屋市天白区久方二丁目12番地1　豊田工業大学
e-mail: nakashima@toyota-ti.ac.jp

底を得るためにBerlekamp–Massey–Sakata(BMS)アルゴリズム[14], [15]を採用し，誤り値決定のために離散フーリエ変換(DFT)を用いた復号法[12]を適用する．また，本研究で構成した復号法の計算量の評価，誤り訂正数の決定を行い，復号誤り率を最小距離復号法と比較する．

本研究は豊田工業大学の松井一氏との共同研究に基づく．

2. 定義

$q = p^e$ を素数べきとし，$\mathbb{F}_q$ を q 元からなる有限体とする．また $\mathbb{F}_q[X_0, X_1, \ldots, X_m]$ は $\mathbb{F}_q$ 上 $m+1$ 変数の多項式環を表すこととする．

$$\begin{aligned}\mathbb{A}^m :=& \{(\omega_1, \ldots, \omega_m) \,|\, \omega_1, \ldots, \omega_m \in \mathbb{F}_q\} = \mathbb{F}_q^m,\\ \mathbb{P}^m :=& (\mathbb{A}^{m+1} \setminus \{0\})/\sim\\ =& \bigcup_{i=0}^{m} \{(0 : \cdots : 0 : 1 : \omega_{i+1} : \cdots : \omega_m) \mid \omega_j \in \mathbb{F}_q, j > i\}\end{aligned}$$

とおく．ただし，同値関係 $\sim$ は次で定める：

$$P_1 \sim P_2 \quad \text{if} \quad P_1 = \lambda P_2 \text{ for some } \lambda \in \mathbb{F}_q \setminus \{0\}.$$

$\mathbb{A}^m(\mathbb{F}_q) = \mathbb{A}^m$ を $\mathbb{F}_q$ 上のアフィン空間，$\mathbb{P}^m(\mathbb{F}_q) = \mathbb{P}^m$ を $\mathbb{F}_q$ 上の射影空間という．$i = 0, 1, \ldots, m$ に対して $\Psi_i := \{(0 : \cdots : 0 : 1 : \omega_{i+1} : \cdots : \omega_m) \in \mathbb{P}^m \mid \omega_j \in \mathbb{F}_q,\, j > i\} \simeq \mathbb{A}^{m-i}$ とおくと，明らかに

$$\mathbb{P}^m = \Psi_m \cup \Psi_{m-1} \cup \cdots \cup \Psi_1 \cup \Psi_0$$

である．

定義 1 (Reed-Muller 符号)．$\mathbb{A}^m = \{P_1, \ldots, P_{q^m}\}$ とする．

$$\mathrm{RM}_\nu(m, q) = \{(f(P_1), \ldots, f(P_{q^m})) \,|\, f \in \mathbb{F}_q[X_1, \ldots, X_m]_{\le \nu}\},$$

を次数 ν の Reed–Muller(RM) 符号という．ただし，$\mathbb{F}_q[X_1, \ldots, X_m]_{\le \nu}$ は次数 $\le \nu$ の多項式全体とする．

定義 2 (射影 Reed-Muller 符号)．$n := \frac{q^{m+1}-1}{q-1} = q^m + \cdots + q + 1$，$\mathbb{P}^m = \{P_1, \ldots, P_n\}$ とおく．このとき

$$\mathrm{PRM}_\nu(m, q) := \{(f(P_1), \ldots, f(P_n)) \,|\, f \in \mathbb{F}_q[X_0, X_1, \ldots, X_m]_\nu\}$$

を符号長 n，次数 ν の射影 Reed–Muller(RM) 符号という．ただし，
$\mathbb{F}_q[X_0, X_1, \ldots, X_m]_\nu$ は次数 ν の斉次多項式全体とし，$P = (0 : \cdots : 0 : 1 : \omega_{i+1} : \cdots : \omega_m)$ に対し $f(P) = f(0, \cdots, 0, 1, \omega_{i+1}, \cdots, \omega_m)$ とする．

注意: $\nu > m(q-1)$ のとき，射影 RM 符号は自明な符号である [16, Remark 3]. したがって以下では $\nu \le m(q-1)$ を仮定する．

定義 3.

$$\mathrm{ev} : \mathbb{F}_q[X_0, X_1, \ldots, X_m] \to \mathbb{F}_q^n, \quad \mathrm{ev}(f) := (f(P))_{P \in \mathbb{P}^m}$$

を評価写像とよぶ．

3. 射影RM符号の基底

本節では$q > 2$とする．$\boldsymbol{a} = (a_0, a_1, \ldots, a_m) \in \mathbb{N}_0^{m+1}$に対して，$X^{\boldsymbol{a}} := X_0^{a_0} X_1^{a_1} \cdots X_m^{a_m}$，$|\boldsymbol{a}| := a_0 + a_1 + \cdots + a_m$と定める．単項式順序$\prec$を次の方法で定義する：“$|\boldsymbol{a}| < |\boldsymbol{b}|$”あるいは“$|\boldsymbol{a}| = |\boldsymbol{b}|$かつ$a_m = b_m, a_{m-1} = b_{m-1}, \ldots, a_{\ell+1} = b_{\ell+1}$ and $a_\ell < b_\ell$をみたすインデックスℓが存在する”とき，$X^{\boldsymbol{a}} \prec X^{\boldsymbol{b}}$とする．

すべての$i = 1, \ldots, m$に対して$f_i := X_i^q - X_i$と定め，$i = 0, \ldots, m$, と$\ell \in \{0, 1\}$に対して$g_{(i,\ell)} := X_i^\ell (X_i - 1) \cdots (X_1 - 1)(X_0 - 1) = X_i^\ell \prod_{j=0}^{i} (X_j - 1)$と定める．このとき次が成り立つ．

定理 4. $2m + 1$個の多項式からなる集合

$$\mathcal{G} := \{f_i, g_{(m,0)}, g_{(j,1)} \mid i = 1, \ldots, m,\ j = 0, 1, \ldots, m - 1\}$$

は$\ker(\mathrm{ev})$の$\prec$に関するグレブナー基底である．

例 5. $m = 1, 2, 3$の場合の$\mathcal{G}$の具体例を挙げる．

1. $m = 1$のとき
$$\mathcal{G} = \{X_1^q - X_1, (X_1 - 1)(X_0 - 1), X_0^2 - X_0\}.$$

2. $m = 2$のとき
$$\begin{aligned}\mathcal{G} := \{&X_2^q - X_2, X_1^q - X_1,\\ &(X_2 - 1)(X_1 - 1)(X_0 - 1),\\ &(X_1^2 - X_1)(X_0 - 1),\\ &X_0^2 - X_0\}.\end{aligned}$$

3. $m = 3$のとき
$$\begin{aligned}\mathcal{G} := \{&X_3^q - X_3, X_2^q - X_2, X_1^q - X_1,\\ &(X_3 - 1)(X_2 - 1)(X_1 - 1)(X_0 - 1),\\ &(X_2^2 - X_2)(X_1 - 1)(X_0 - 1),\\ &(X_1^2 - X_1)(X_0 - 1),\\ &X_0^2 - X_0\}.\end{aligned}$$

また標準単項式は次で与えられる．

1. $m = 1$のとき，$\{X_0 X_1^a \mid 0 \le a \le q - 1\} \cup \{X_0\}$,
2. $m = 2$のとき，$\{X_1^a X_2^b \mid 0 \le a, b \le q - 1\} \cup \{X_0 X_2^a \mid 0 \le a \le q - 1\} \cup \{X_0 X_1\}$,
3. $m = 3$のとき，$\{X_1^a X_2^b X_3^c \mid 0 \le a, b, c \le q - 1\} \cup \{X_0 X_2^a X_3^b \mid 0 \le a, b \le q - 1\} \cup \{X_0 X_1 X_3^a \mid 0 \le a \le q - 1\} \cup \{X_0 X_1 X_2\}$.

例 6. $\mathrm{PRM}_3(2,9)$ の $\mathbb{F}_9$ 上の基底を標準単項式の線形結合の形で表す．$\{\mathrm{ev}(X^{\boldsymbol{a}}) \mid |\boldsymbol{a}| = 3\}$ は（標準単項式の線形結合で表されていない）$\mathrm{PRM}_3(2,9)$ の基底であることを考えると

$$\begin{aligned}
&\mathrm{ev}(X_0^3) = \mathrm{ev}(X_0),\\
&\mathrm{ev}(X_1X_0^2) = \mathrm{ev}(X_1X_0),\\
&\mathrm{ev}(X_2X_0^2) = \mathrm{ev}(X_2X_0),\\
&\mathrm{ev}(X_1^2X_0) = \mathrm{ev}(X_1^2 + X_1X_0 - X_1),\\
&\mathrm{ev}(X_2X_1X_0)\\
&= \mathrm{ev}(X_2X_1 + X_2X_0 + X_1X_0 - X_2 - X_1 - X_0 + 1),\\
&\mathrm{ev}(X_2^2X_0),\\
&\mathrm{ev}(X_1^3), \mathrm{ev}(X_1^2X_2), \mathrm{ev}(X_1X_2^2), \mathrm{ev}(X_2^3)
\end{aligned}$$

とかきかえることができる．ここで $\mathrm{ev}(X_0X_1X_2)$ に注目する．$\mathrm{ev}(X_0X_1X_2)$ は基底の線形変換で $\mathrm{ev}(X_2X_1 - X_2 - X_1 + 1)$ とかきかえられるが，どのような基底の線形変換でも 1 つの標準単項式（$\mathrm{ev}(X^{\boldsymbol{alpha}})$）の形にはかきかえられない．

例 6 のように標準単項式の形で表される元からなる基底を持たない場合には [12] に示される復号アルゴリズム（次節の Algorithm 1）が適用できない．

4. 復号法

Algorithm 1 は BMS アルゴリズムと DFT を用いた RM 符号の復号法である．（BMS アルゴリズムの詳細は [6] をみよ．）ここで $\mathcal{F}$ と $\mathcal{E}$ は以下で定義される写像であり，$\mathcal{F}$ の逆写像 $\mathcal{F}^{-1}$ を n^3 より小さいオーダーで計算する方法も知られている [12]．

定義 7 (離散フーリエ変換)．$M = \{X_1^{a_1} \cdots X_m^{a_m} \mid (a_1, \ldots, a_m) \in \mathbb{Z}^m,\ 0 \le a_1, \ldots, a_m \le q-1\}$ とする．線形写像 $\mathcal{F}$ を

$$\mathcal{F} : \mathbb{F}_q^{\mathbb{A}^m} \to \mathbb{F}_q^M, \quad (c_P)_{P\in\mathbb{A}^m} \mapsto \left(\sum_{P\in\mathbb{A}^m} c_P h(P) \right)_{h\in M},$$

で定義し，$\mathbb{F}_q^{\mathbb{A}^m}$ 上の離散フーリエ変換という．ただし，$\mathbb{F}_q^\Omega := \{(c_P)_{P\in\Omega} \mid c_P \in \mathbb{F}_q\}$ は集合 Ω で指数付けられた $\mathbb{F}_q$ 上の線形空間である．

定義 8. 写像 $\mathcal{E}_\Phi$ は

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

により定義される．ただし，$g \in M$ に対して

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

であり，v_h はグレブナー基底 $\mathcal{G} = \{f^{(w)}\}_{0\le w<z}$ の割り算アルゴリズムによって

$$g(X) = \sum_{0\le w<z} u^{(w)}(X) f^{(w)}(X) + v(X) \quad (v(X) := \sum_{h\in D(\Phi)} v_h h),$$

で与えられる．

Algorithm 2 は Algorithm 1 を使った射影 RM 符号の復号法の疑似コードである．

5. 計算量

本節ではAlgorithm 2の計算量について考察する．

定義 9. $f(q)$ と $g(q)$ を $\mathbb{R}$ の部分集合上で定義された関数とする．ある定数 q_0 と C が存在して，任意の $q > q_0$ に対して $|f(q)| \leq C|g(q)|$ が成り立つとき，$f(q) = O(g(q))$ とかく．O は *Landau* の記号とよばれる．さらに，$f(q) = O(g(q))$ かつ $g(q) = O(f(q))$ であるとき $f(q) = \theta(g(q))$ とかく．

$N_i = q^{m-i}$ を $(m-i)$ 次元アフィン空間の要素数とする．各アフィン成分におけるAlgorithm 1の復号に関して誤り位置決定と誤り値決定に要する計算量は，それぞれ $O(z_i N_i^2) = O(z_i q^{2m-2i})$([5], [6]) と $O(qN_i^2) = O(q^{2m-2i+1})$([12]) である．ただし，$z_i$ は Ψ_i 部分のBMSアルゴリズムで得られるグレブナー基底の要素数である．すべての $i = 0, 1, \ldots, m$ に対して，$z_i < q^{m-i}$ であるから，Ψ_i 部分の合計計算量 $O(w_i q^{2m-2i})$ は $O(n^3)$ より真に小さい[1]．ただし，$w_i := \max\{z_i, q\}$ である．

Algorithm 2全体で要する計算量は

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

であり，さらに次のこともわかる．

命題 10. $w := \max\{q, z_0, z_1, \ldots, z_m\} < q^m < n$ とおくと *Algorithm 2* の計算量は $O(wn^2)$ である．また $wn^2 = \theta(wq^{2m})$ である．

6. 訂正可能数

$\mu = m(q-1) - \nu$ とする．$i_0 \geq 0$ を $\nu - i_0(q-1) \leq -1$ なる最小の整数とすると，$i \geq i_0$ に対して $\mathrm{RM}_{\mu-1}(m-i, q) = \mathbb{F}_q^{q^{m-i}}$ となる．Algorithm 2を各アフィン成分にわけたときの成分ごとの訂正可能数は次のとおりである．

定理 11. $\mathrm{PRM}_\nu(m, q)$ を射影 *RM* 符号として，

$$t_0 := \left\lfloor \frac{(q-s)q^{m-r-1} - 1}{2} \right\rfloor, \tag{6.1}$$

とおく．ただし，$\nu = r(q-1) + s,\ 0 \leq s < q-1,\ 0 \leq r \leq m-1$ である．*Algorithm 2* において，Ψ_i-部分で適用する復号法と訂正可能な誤りの数は次のとおりである．

Algorithm 1 Decoding for affine variety codes (cf. [12])

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

Output: $(c_P)_{P \in \mathbb{A}^m} \in \mathrm{RM}_{\nu'}(m, q)$

Step 1. $(\widetilde{r}_h)_{h \in B} := \left(\sum_{P \in \mathbb{A}^m} r_P h(P)\right)_{h \in B}$.

Step 2. Calculate a Gröbner basis $\mathcal{G}$ from the syndrome $(\widetilde{r}_h)_{h \in B}$ by BMS algorithm.

Step 3. $(e_P)_{P \in \mathbb{A}^m} = \mathcal{F}^{-1} \circ \mathcal{E}\left((\widetilde{r}_h)_{h \in B}\right)$.

Step 4. $(c_P)_{P \in \mathbb{A}^m} = (r_P)_{P \in \mathbb{A}^m} - (e_P)_{P \in \mathbb{A}^m} \in \mathrm{RM}_{\nu'}(m, q)$.

Remark. This algorithm works if $2|\Phi| < d_{\mathrm{FR}}$, where d_{FR} is a Feng-Rao bound of $\mathrm{RM}_{\nu'}(m, q)^\perp$ (see [1], [6], [9], [13] for Feng-Rao bounds) and Φ is the set of error locations.

---

[1] より細かくいうと $w_i q^{2m-2i}$ は q^{3m-3i} より小さいが，計算量としては $n^3 = \theta(q^{3m-3i})$ であるので，符号長 n を使ってこのように表した．

1. $0 \le i < i_0$ ならば $\mathrm{RM}_{\nu-i(q-1)}(m-i,q)$ に関する *Algorithm 1* を適用して t_0 個の誤りを訂正できる．

2. $i_0 \le i \le m$ ならば *IDFT* を適用して q^{m-i} 個の誤りを訂正できる．

これは $\mathbb{P}_m$ の成分ごとに誤りの数を制限した特殊誤りが起こる場合の訂正可能数である．一方で，命題11から常に直せる誤りの数もわかる．

系 12. $\mathrm{PRM}_\nu(m,q)$ に対して *Algorithm 2* は任意に起こる t_0 個までの誤りを訂正できる．

7. 復号誤り率

Algorithm 2の復号誤り率を最小距離復号法(MDD)との比較をする[2]．Algorithm 2において訂正可能数は2種類考えることができる：一つは常に訂正可能である誤りの数 t_0 で（命題12），もう一つは成分ごとに誤りの数を制限した特殊誤りが起こる場合の訂正可能数（表2）である．この二つの場合には，復号誤り率が異なるので，常に訂正可能な数 t_0 を訂正する復号法をProposed method 1 (PM1)，特殊な場合の誤りを訂正する復号法をProposed method 2 (PM2)と書くこととする．このとき，p をシンボル誤り率（符号語の1つの成分が誤る確率）とすると，復号誤り率はそれぞれ

$$\begin{gathered}
\text{PM1: } 1-P \quad \left(P=\textstyle\sum_{j=0}^{t_0}\binom{n}{j}p^j(1-p)^{n-j}\right)\\
\text{PM2: } 1-\textstyle\prod_{i=0}^{i_0-1}P_i \quad \left(P_i=\sum_{j=0}^{t_0}\binom{q^{m-i}}{j}p^j(1-p)^j\right)\\
\text{MDD: } 1-P_{\mathrm{MD}} \quad \left(P_{\mathrm{MD}}=\textstyle\sum_{j=0}^{t_{\mathrm{MD}}}\binom{n}{j}p^j(1-p)^{n-j}\right)\\
\text{ただし，} t_{\mathrm{MD}} := \left\lfloor \tfrac{d_{\min}(\mathrm{PRM}_\nu(m,q))-1}{2} \right\rfloor
\end{gathered}$$

で与えられる．常に $t_{\mathrm{MD}} \ge t_0$ なので

$$1-P_{\mathrm{MD}} = 1-P-\sum_{j=t_0+1}^{t_{\mathrm{MD}}}\binom{n}{j}p^j(1-p)^{n-j}$$

である．したがって，復号誤り率を比べると常にMDDの方がPM1より性能がよいことがわかる[3]．一方で表2に表されるように ν が大きくなれば復号誤り率の差が少なくなる．特に $\mathrm{PRM}_{24}(2,16)$ のようにPM1がMDDと同じ復号誤り率をもつこともある．また，図1は $\mathrm{PRM}_{13}(2,16)$ と $\mathrm{PRM}_{19}(2,16)$ に関してPM1，PM2，MDDの復号誤り率を比較したグラフである．

参考文献

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

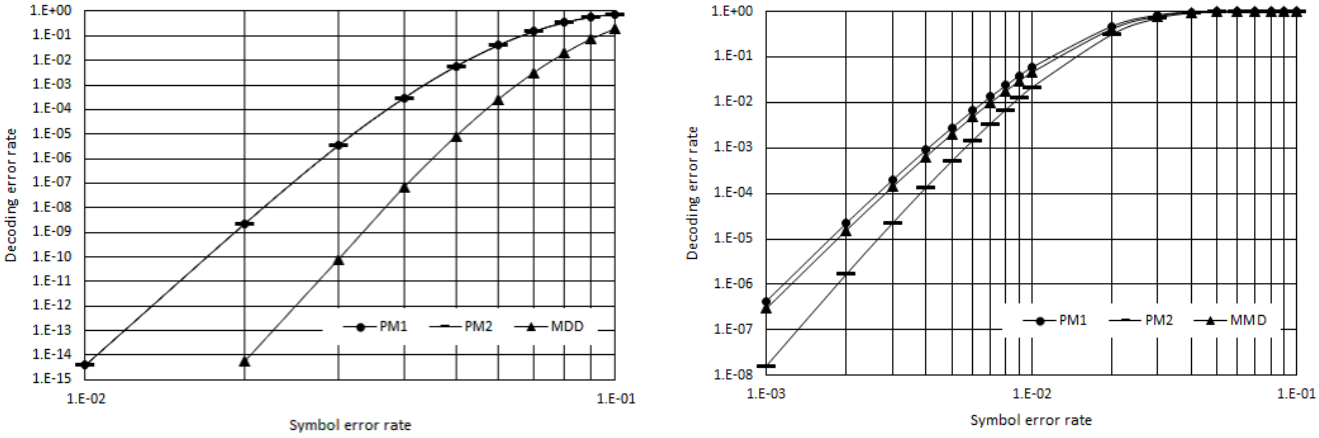
[2] S. Ballet, R. Rolland, “On low weight codewords of generalized affine and projective Reed–Muller codes,” *Designs Codes Cryptogr.,* vol.73, no.2, pp.271-297, 2014

[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, 2001.

[2] 復号誤り率とは復号結果とオリジナルの情報を符号化した語が一致しない率を表す．また，MDDは誤り訂正符号のほとんどの入門書で学ぶことができる．例えば[11]の1章3節を見てほしい．MDDは主に $q=2$ のときに考えられるが，一般の q の場合にも誤り位置決定に利用できる．

[3] MDDによる復号は復号誤り率の面で非常に高い性能を有するが，符号語の全探索を行わなければならないので計算量は指数オーダーである．処理速度を考えて実用化は非常に難しいとされる．

図 1: $\mathrm{PRM}_{13}(2,16)$(左) と $\mathrm{PRM}_{19}(2,16)$(右) に関する復号誤り率の比較



[4] I. F. Blake and R. C. Mullin, *The Mathematical Theory of Coding*, New York: Academic Press, 1975.

[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, 2006.

[6] 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.

[7] A. Dür, "The decoding of extended Reed–Solomon codes," *Discrete Math.,* vol.90, issue 1, pp.21-40, 1991.

[8] I. Duursma, "Decoding codes from curves and cyclic codes," PhD. Thesis, Technische Universiteit Eindhoven.

[9] 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, 1993.

[10] G. Lachaud, "Projective Reed–Muller codes," *in Lect. Notes in Comp. sci.,* vol.311, Berlin: Springer 1988.

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

[12] 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, 2014.

[13] S. Miura, "Linear codes on affine algebraic varieties," *Trans. IEICE,* vol.J81-A, no.10, pp.1386-1397, 1998. (in Japanese

[14] 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, 1988.

[15] S. Sakata, "Extension of the Berlekamp–Massey algorithm to n dimensions," *Inform. Comput.,* vol.39, no.2, pp.207-239, 1990.

[16] A. B. Sørensen, "Projective Reed–Muller codes," *IEEE Trans. Inf. Theory,* vol.37, pp.1567-1576, 1991.

Algorithm 2 Decoding algorithm for $\mathrm{PRM}_\nu(m,q)$

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 $i = 0, \ldots, m$ **do**

Step 1.

if $i = 0$ **then**

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

else $\{i > 0\}$

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

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

end if

Step 2. Let $S_{\boldsymbol{u}}^{(i)} := \langle (r_P^{(i)})_{P\in\mathbb{P}^m}, \boldsymbol{u}\rangle$ for $\boldsymbol{u} \in \mathrm{ev}(B_i(\mu))$.

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

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

else

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

end if

end for

Remark. Set $\mu := m(q-1) - \nu$, $B_i := \{X^{\boldsymbol{a}} \in R \mid \boldsymbol{a} = (a_i, \ldots, a_m),\ a_i > 0\}$, $B_i(\mu) := \{X^{\boldsymbol{a}} \in B_i \mid |\boldsymbol{a}| = \mu\}$ for any $i = 0, 1, \ldots, m$.

表 1: Algorithm 2 の成分ごとの訂正可能数

$\mathbb{P}^m$ の成分	復号法を適用する符号	訂正可能数
Ψ_0	$\mathrm{RM}_{\mu-1}(m,q)^\perp = \mathrm{RM}_\nu(m,q)$	t_0
Ψ_1	$\mathrm{RM}_{\mu-1}(m-1,q)^\perp = \mathrm{RM}_{\nu-(q-1)}(m-1,q)$	t_0
Ψ_2	$\mathrm{RM}_{\mu-1}(m-2,q)^\perp = \mathrm{RM}_{\nu-2(q-1)}(m-2,q)$	t_0
$\vdots$	$\vdots$	$\vdots$
Ψ_{i_0-1}	$\mathrm{RM}_{\mu-1}(m-i_0+1,q)^\perp = \mathrm{RM}_{\nu-(i_0-1)(q-1)}(m-i_0+1,q)$	t_0
Ψ_{i_0}	$(\mathbb{F}_q^{q^{m-i_0}})^\perp$	$q^{m-i_0} = \sharp\Psi_{i_0}$
$\vdots$	$\vdots$	$\vdots$
Ψ_{m-1}	$(\mathbb{F}_q^q)^\perp$	$q^1 = \sharp\Psi_{m-1}$
Ψ_m	$\mathbb{F}_q^\perp$	$q^0 = \sharp\Psi_m$

表 2: $\mathrm{PRM}_\nu(2,16)$ に関する Algorithm 2 と MDD の訂正可能数の差

ν	5	8	11	13	17	19	24	26	29
Algorithm 2	87	63	39	23	6	6	3	2	0
MDD	95	71	47	31	7	5	3	2	1
Difference	8	8	8	8	1	1	0	0	1