Fast decoding of dual multipoint codes from algebraic curves up to the Kirfel-Pellikaan bound

Masaya Fujisawa, Shojiro Sakata

Fast decoding of dual multipoint codes from algebraic curves up to the Kirfel-Pellikaan bound

Masaya Fujisawa[1] and Shojiro Sakata[2]

[1] The Tokyo University of Science, Tokyo, Japan
[2] Emeritus Professor, The University of Electro-Communications, Tokyo, Japan

Abstract. Multipoint codes are a broad class of algebraic geometry codes derived from algebraic functions which have multiple poles/zeros on their defining curves. The one-point codes which are viewed as its subclass can be decoded efficiently up to the Feng-Rao bound by using the BMS algorithm with majority logic [1]. Recently we published [2] a fast method for decoding primal multipoint codes from curves based on the vectorial BMS algorithm [3]. Although the simulation shows that the method can correct most error patterns of weight up to $\frac{1}{2}d_{\mathrm{G}}$, it is guaranteed theoretically that every error of weight only up to $\frac{1}{2}(d_{\mathrm{G}} - g)$ can be corrected, where g is the genus of the defining curve. In this paper we present a fast method for decoding dual multipoint codes from algebraic curves up to the Kirfel-Pellikaan bound, based on the vectorial BMS algorithm with majority logic.

1 Introduction

Multipoint codes are a broad class of algebraic geometry codes derived from algebraic functions which have multiple poles/zeros on their defining curves. Thus, those are more general than *one-point* codes which are an important class of algebraic geometry codes in the sense that these codes can be decoded efficiently by using the Berlekamp-Massey-Sakata (BMS) algorithm [1][4] or by other relevant methods [5], etc. (See also [6][7].) Furthermore, some multipoint codes have better performance than comparable one-point codes from the same curves [8][9]. The basic lower bound for the minimum distance of algebraic geometry codes was given by Goppa [10], and for one-point codes, an improved lower bound called the *Feng-Rao bound* was shown by Feng and Rao [11], and its generalization called the *order bound* was given (See [12]). By Beelen [13] the *order bound* was extended to multipoint codes and it is shown that the *Kirfel-Pellikaan bound* [14] is a special case of the order bound. Thus, various kinds of lower bounds have been given (See Duursma et al. [15]).

Recently we published [2] a fast method for decoding multipoint codes from curves based on the vectorial BMS algorithm [3]. But, that is for primal codes. Since primal codes are equivalent to dual codes, one can decode them as either primal or dual codes, while their decoding methods are different. Although the simulation shows that our method for primal codes can correct most error

patterns of weight up to $\lfloor \frac{1}{2}(d_{\rm G} - 1) \rfloor$, where $d_{\rm G}$ is the Goppa bound of the primal code, it is guaranteed theoretically that every error of weight only up to $\lfloor \frac{1}{2}(d_{\rm G} - g - 1) \rfloor$ can be corrected, where g is the genus of the defining curve. Recently a fast method for decoding dual multipoint codes from curves was published [16].

In this paper we present a fast method for decoding dual multipoint codes from algebraic curves up to the Kirfel-Pellikaan bound, based on the vectorial BMS algorithm with majority logic, and show that algebraic geometry codes from a general algebraic curve embedded in the M-dimensional affine space $\mathbb{F}_q^M$ over a finite field $\mathbb{F}_q$ can be decoded up to $\lfloor \frac{1}{2}(d_{\rm G}^{\perp} - 1) \rfloor$ errors efficiently, where $d_{\rm G}^{\perp}$ is the Goppa bound of the dual code, if the dimension M of the affine space including the defining curve is small. Our method is motivated by the observation that any multipoint codes are sub- (or super-)codes of one-point codes [9], and that the error locator ideal of a dual code is taken in some specific ideal of the ring of multivariate polynomials. Although the method given by [16] is based somehow on the Gröbner basis theory and has a similar complexity of computation, our approach is quite different and it is a natural extension of the original BMS algorithm for decoding dual one-point codes from curves.

2 Preliminaries

2.1 The codes

A *multipoint* code from an algebraic curve is defined by the following three algebraic ingredients:

(1) An information symbol set, i.e. a finite field $\mathbb{F}_q$;

(2) A symbol locator set $\mathcal{P} := \{P_i \mid 1 \leq i \leq n\}$, which is a subset of $\mathbb{F}_q$-rational points on an irreducible and non-singular algebraic curve $\mathcal{X}$, where $n(= \#\mathcal{P})$ is the code length.

(3) A divisor $G := \sum_{1 \leq i \leq a} m_i Q_i - \sum_{1 \leq j \leq b} n_j R_j$ for any given positive integers m_i, $1 \leq i \leq a$ and n_j, $1 \leq j \leq b$, and any given sets $\mathcal{Q} := \{Q_j \mid 1 \leq j \leq a\}$, $\mathcal{R} := \{R_k \mid 1 \leq k \leq b\}$ of points on the curve s.t. the sets $\mathcal{P}, \mathcal{Q}$ and $\mathcal{R}$ are pairwise disjoint, or rather the linear space $\mathcal{L}(G)$ of algebraic functions f defined by the divisor G, i.e. having only points Q_i as poles with (pole) order $o_i(f) = -v_{Q_i}(f) \leq m_i$, $1 \leq i \leq a$, and only points R_j as zeros with (zero) order $v_{R_j}(f) \geq n_j$, $1 \leq j \leq b$, where the integer $v_P(f)$ is the valuation of function f at the point P.

Then, we have two kinds of linear codes, which we call *primal* and *dual* codes (often called $\mathcal{L}$-codes and Ω-codes) respectively:

$$C(G) := \{\underline{c} = \mathrm{eval}(f) \mid f \in \mathcal{L}(G)\},$$
$$C^{\perp}(G) := \{\underline{c} \in \mathbb{F}_q^n \mid \underline{c} \cdot \mathrm{eval}(f) = 0,\ f \in \mathcal{L}(G)\},$$

where $\mathrm{eval}(f) := (f(P_i))_{1 \leq i \leq n} \in \mathbb{F}_q^n$ and $\underline{c} \cdot \mathrm{eval}(f) := \sum_{1 \leq i \leq n} c_i f(P_i) \in \mathbb{F}_q$ is the inner product of n-dimensional (n-D) vectors $\underline{c} = (c_i)_{1 \leq i \leq n}$ and $\mathrm{eval}(f)$.

In case of $G = mP_\infty$, i.e. $\mathcal{Q} = \{P_\infty\}$ and $\mathcal{R} = \emptyset$, codes $C(G)$ and $C^\perp(G)$ are called primal and dual *one-point* codes respectively, where P_∞ can be any rational point of the curve, but we usually take the infinity point. It is shown [9] that any primal multipoint code $C(G)$ is equivalent to a sub-code $C(mP_\infty - \sum_{1\le j\le b} n_j R_j)$ of a one-point code $C(mP_\infty)$, where m and n_j, $1 \le j \le b$ are certain positive integers and $\mathcal{R} := \{R_k \mid 1 \le k \le b\}$ is a set of points on the curve s.t. $\mathcal{P} \cap \mathcal{R} = \emptyset$, and $\mathcal{P} \cup \mathcal{R} \not\ni P_\infty$. The inclusion $\mathcal{L}(mP_\infty - \sum_{1\le j\le b} n_j R_j) \subset \mathcal{L}(mP_\infty)$ is parallel to the extended inclusion $\cup_{i\ge 0}\mathcal{L}(iP_\infty - \sum_{1\le j\le b} n_j R_j) \subset \cup_{i\ge 0}\mathcal{L}(iP_\infty)$, where

$$I_{\mathcal{R}} := \cup_{i\ge 0}\mathcal{L}(iP_\infty - \sum_{1\le j\le b} n_j R_j) \tag{1}$$

is an ideal of the ring $R := \cup_{i\ge 0}\mathcal{L}(iP_\infty)$. Any $f \in R$ has a single pole at P_∞, and so, roughly speaking, the ring is apparently the same as the ring of all polynomials.

We can use the inclusion $I_{\mathcal{R}} \subset R$ to decode a generic dual multipoint code $C^\perp(mP_\infty - \sum_{1\le j\le b} n_j R_j)$. The key point is that the syndrome array is taken in the sigma set Σ of the ideal $I_{\mathcal{R}}$ and that the error locator ideal $I(\mathcal{E})$ can be taken as a sub-ideal of the ideal $I_{\mathcal{R}}$.

From now on we consider for $m < n$ only supercodes of dual one-point codes

$$C^\perp(G)(\supset C^\perp(mP_\infty)),\ G = mP_\infty - \sum_{1\le j\le b} n_j R_j \tag{2}$$

from an irreducible non-singular algebraic curve $\mathcal{X}$ over the finite field $\mathbb{F}_q$. The linear code $C^\perp(G)$ has dimension $k \ge n - (m - \sum_{1\le j\le b} n_j) + g - 1$ and the minimum distance $\ge d_{\mathrm{G}}^\perp = m - \sum_{1\le j\le b} n_j - 2g + 2$, where g is the genus of the defining curve $\mathcal{X}$ and $d_{\mathrm{G}}^\perp$ is the Goppa bound of the code $C^\perp(G)$.

We rely on the standard form of algebraic curves introduced by Pellikaan[17] and by Miura and Matsumoto[18]. The following descriptions are based on its review given by Geil, Matsumoto and Ruano[19]. We can assume that the Weierstrass semigroup $H(P_\infty)$ at P_∞, which is the set of pole orders $o(f) := -v_{P_\infty}(f)$ of algebraic functions f in R, is generated by positive integers $a_1, \cdots, a_M$ s.t. $o(x_i) = a_i$ for certain algebraic functions $x_i \in R$, $1 \le i \le M$, and particularly we take $a_1 := \min\{m \in H(P_\infty) \mid m \ne 0\}$. From now on, we call $o(f)$ simply as *order* of f. Then, we can express the ring R as a residue class ring $\mathbb{F}_q[\underline{X}]/I_{\mathcal{X}}$ of the polynomial ring $\mathbb{F}_q[\underline{X}]$, $\underline{X} = (X_1, \cdots, X_M)$, where $X_1, \cdots, X_M$ are transcendental over $\mathbb{F}_q$, and $I_{\mathcal{X}}$ is the kernel of the canonical homomorphism sending X_i to x_i, $1 \le i \le M$. Thus, $R = \mathbb{F}_q[\underline{x}]$, $\underline{x} = (x_1, \cdots, x_M)$ and the zero set $V_q(I_{\mathcal{X}})$ of the ideal $I_{\mathcal{X}}$ is just the set of all $\mathbb{F}_q$-rational points on the curve $\mathcal{X}$ except for P_∞, which is viewed as a curve embedded in the M-D affine space $\mathbb{F}_q^M$.

2.2 The Gröbner bases and standard form of the curve

Let $\mathbf{N}_0$ be the set of non-negative integers, and we take the M-D integral lattice $\mathbf{N}_0^M$ which is the set of M-tuples $\underline{i} := (i_1, \cdots, i_M)$ of non-negative integers,

and denote for $\underline{i} \in \mathbf{N}_0^M$, $\underline{x}^{\underline{i}} := x_1^{i_1} \cdots x_M^{i_M}$. Any polynomial (function) $f \in \mathbb{F}_q[\underline{x}]$ is written as $f = \sum_{\underline{i} \in \mathrm{Supp}(f)} \mathrm{coeff}(f, \underline{i}) \underline{x}^{\underline{i}}$ with a finite subset $\mathrm{Supp}(f) := \{\underline{i} \mid \mathrm{coeff}(f, \underline{i}) (\in \mathbb{F}_q) \neq 0\} \subset \mathbf{N}_0^M$ which is called the *support* of f. According to the order $o(\underline{x}^{\underline{i}})$, $\underline{i} \in \mathbf{N}_0^M$, the graded reverse lexicographic term ordering $<_T$ is defined over $\mathbf{N}_0^M$ s.t. for $\underline{i} = (i_1, \cdots, i_M), \underline{j} = (j_1, \cdots, j_M) \in \mathbf{N}_0^M$, $\underline{i} >_T \underline{j}$ and $\underline{x}^{\underline{i}} >_T \underline{x}^{\underline{j}}$ iff either $\sum_{1 \leq k \leq M} a_k i_k > \sum_{1 \leq k \leq M} a_k j_k$ or $\sum_{1 \leq k \leq M} a_k i_k = \sum_{1 \leq k \leq M} a_k j_k$ and $i_1 = j_1, \cdots, i_{k-1} = j_{k-1}, i_k < j_k, 1 \leq^{\exists} k \leq M$ holds. For $f \in \mathbb{F}_q[\underline{x}]$, let the definitions of (multi-)degree $\deg(f) \in \mathbf{N}_0^M$, the head (leading) term $\mathrm{ht}(f)$, the head (leading) coefficient $\mathrm{hc}(f)$, etc. be the same as in [20] as well as in the usual theory of Gröbner basis ([21],etc.).

Only monomials $\{\underline{x}^{\underline{i}} \mid \underline{i} \in \Delta(I_{\mathcal{X}})\}$ are linearly independent over $\mathbb{F}_q$ as algebraic functions on the curve $\mathcal{X}$, where $\Delta(I_{\mathcal{X}}) \subset \mathbf{N}_0^M$ is the delta set (Gröbner escalier [21]) of a Gröbner basis $B(I_{\mathcal{X}}) \subset \mathbb{F}_q[\underline{X}]$ of the ideal $I_{\mathcal{X}}$ w.r.t. the term ordering $<_T$. This fact can be said in terms of the order $o(f)$, $f \in \mathbb{F}_q[\underline{x}]$. That is, if $o(\underline{x}^{\underline{i}}) = o(\underline{x}^{\underline{j}})$ and $\underline{x}^{\underline{i}} \neq \underline{x}^{\underline{j}}$, then $\underline{x}^{\underline{i}} = c\underline{x}^{\underline{j}} + g$, where $g \in R$ s.t. $\mathrm{Supp}(g) \subset \{\underline{k} \in \Delta(I_{\mathcal{X}}) \mid o(\underline{x}^{\underline{k}}) < o(\underline{x}^{\underline{i}})\}$ and $c (\neq 0) \in \mathbb{F}_q$. The set of functions in a reduced Gröbner basis $B(I_{\mathcal{X}})$ gives a defining set of equations of the curve $\mathcal{X}$ (in the Pellikann-Miura standard form).

For $i = 0, \cdots, a_1 - 1$, we define $b_i := \min\{j \in H(P_\infty) \mid j \equiv i \mod a_1\}$, and $\underline{m}^{(i)} = (m_1^{(i)}, \cdots, m_M^{(i)}) \in \mathbf{N}_0^M$ to be the minimum element w.r.t. $<_T$ s.t. $o(\underline{x}^{\underline{m}^{(i)}}) = b_i$, $0 \leq i \leq a_1 - 1$. Then, we have $b_0 = 0$, $\underline{m}^{(0)} = (0 \cdots, 0)$ and $m_1^{(i)} = 0$, $0 \leq i \leq a_1 - 1$. For each $\underline{m}^{(i)} = (m_1^{(i)}, \cdots, m_M^{(i)})$, let $y^{(i)} := \underline{x}^{\underline{m}^{(i)}} (= x_2^{m_2^{(i)}} \cdots x_M^{m_M^{(i)}} \in R)$, $0 \leq i \leq a_1 - 1$. ($y^{(0)} = 1$.) Two distinct elements of the set $\Omega_0 := \{x_1^m y^{(i)} \mid m \in \mathbf{N}_0, i = 0, \cdots, a_1 - 1\}$ have different orders (as functions over the closure $\bar{\mathbb{F}}_q := \cup_{j \geq 0} \mathbb{F}_{q^j}$). R is a free $\mathbb{F}_q[x_1]$-module with a basis $\{y^{(0)}, \cdots, y^{(a_1-1)}\}$. We denote $\Pi := \cup_{i=0}^{a_1-1} \{(m, m_2^{(i)}, \cdots, m_M^{(i)}) \in \mathbf{N}_0^M \mid m \in \mathbf{N}_0\}$, i.e. $\Omega_0 = \{\underline{x}^{\underline{i}} \mid \underline{i} \in \Pi\}$.

Since $\mathcal{L}(G) \subset R$, the free $\mathbb{F}_q[x_1]$-submodule $\mathcal{L}(G)$ of the free $\mathbb{F}_q[x_1]$-module R has a Gröbner basis $B_G = \{f^{(i)} \in \langle 1, y^{(1)}, \cdots, y^{(a_1-1)} \rangle_{\mathbb{F}_q[x_1]} \mid \mathrm{ht}(f^{(i)}) = x_1^{l^{(i)}} y^{(i)}, 0 \leq i \leq a_1 - 1\}$ for certain nonnegative integers $l^{(i)} \in \mathbf{N}_0$, $0 \leq i \leq a_1 - 1$. Let $\Delta(I_{\mathcal{R}})$ be the delta set of a reduced Gröbner basis B_G of the ideal $I_{\mathcal{R}}$ (1). Then, $\Delta(I_{\mathcal{R}}) \subset \Pi$, and we define

$$\Pi_{\mathcal{R}} := \Pi \setminus \Delta(I_{\mathcal{R}}) = \cup_{0 \leq j \leq a_1 - 1} \{(m, 0, \cdots, 0) + \underline{i}^{(j)} \in \mathbf{N}_0^M \mid m \in \mathbf{N_0}\}, \quad (3)$$

where $\deg(f^{(j)}) = \underline{i}^{(j)} = (l^{(j)}, m_2^{(j)}, \cdots, m_M^{(j)}) \in \mathbf{N}_0^M$, $0 \leq j \leq a_1 - 1$. Then, the linear space $\mathcal{L}(G)$ (over $\mathbb{F}_q$) with $\dim_{\mathbb{F}_q}(\mathcal{L}(G)) = n - k$ is spanned by the polynomials $\{f \in \mathcal{L}(G) \mid \deg(f) \in \Pi_{\mathcal{R}}(m)\}$, where $\Pi_{\mathcal{R}}(m) := \{\underline{i} \in \Pi_{\mathcal{R}} \mid o(\underline{x}^{\underline{i}}) \leq m\}$, in particular by the polynomials of the form

$$\{g^{(i)} \in \mathcal{L}(G) \mid 1 \leq i \leq n - k\} := \{x_1^{i_1} f^{(j)} \mid 0 \leq j \leq a_1 - 1, a_1 i_1 + o(f^{(j)}) \leq m\}.$$

In a summary, $h \in \mathcal{L}(G)$ is written uniquely by

$$h = \sum_{0 \leq j \leq a_1 - 1} h^{(j)} f^{(j)} \quad (4)$$

with $h^{(j)}(= h^{(j)}(x_1)) \in \mathbb{F}_q[x_1]$, $o(h^{(j)}) + o(f^{(j)}) \leq m$, $0 \leq j \leq a_1 - 1$. Therefore, we can represent any polynomial $h \in \mathcal{L}(G)$ as a polynomial vector $\underline{h} = (h^{(0)}, h^{(1)}, \cdots, h^{(a_1-1)}) \in (\mathbb{F}_q[x_1])^{a_1}$.

3 Finding the error locators

3.1 Compound linear recurrence

Given a received word $\underline{r} = (r_l)_{1 \leq l \leq n} \in \mathbb{F}_q^n$, we try to find the codeword $\underline{c} = (c_l)_{1 \leq l \leq n} \in C^{\perp}(G)$ and/or the error vector $\underline{e} = (e_l)_{1 \leq l \leq n} \in \mathbb{F}_q^n$ s.t. $\underline{r} = \underline{c} + \underline{e}$. Particularly, we want to find the error symbol locator set

$$\mathcal{E} := \{P_l \in \mathcal{P} \mid e_l \neq 0,\ 1 \leq l \leq n\} \tag{5}$$

under the assumption that the number of errors $t = \#\mathcal{E}$ is less than half of the Goppa bound $d_{\mathrm{G}}^{\perp}$ (or half of a certain order bound).

Instead of the ordinary syndrome $S^{(i)} = \sum_{1 \leq l \leq n} e_l g^{(i)}(P_l)$, $1 \leq i \leq n - k$ for the basis $\{g^{(i)} \mid 1 \leq i \leq n - k\}$ of $\mathcal{L}(G)$, we introduce a set of M-D error syndrome arrays $u^{(j)} = (u_{\underline{i}}^{(j)})$, $\underline{i} \in \mathbf{N}_0^M$, $0 \leq j \leq a_1 - 1$ defined by

$$u_{\underline{i}}^{(j)} := \sum_{1 \leq l \leq n} e_l f^{(j)}(P_l) \underline{x}^{\underline{i}}(P_l),\ \underline{i} \in \mathbf{N}_0^M,\ 0 \leq j \leq a_1 - 1, \tag{6}$$

where $\{f^{(j)} \in I_{\mathcal{R}} \mid 0 \leq j \leq a_1 - 1\}$ is a Gröbner basis B_G introduced in the previous section. We remark that, for $\Pi^{(j)}(m) := \{\underline{i} \in \Pi \mid o(f^{(j)}) + o(\underline{x}^{\underline{i}}) \leq m\}$, $0 \leq j \leq a_1 - 1$, these components $u_{\underline{i}}^{(j)}$, $\underline{i} \in \Pi^{(j)}(m)$ coincide with those obtained from the received word: $S_{\underline{i}}^{(j)} := \sum_{1 \leq l \leq n} r_l f^{(j)}(P_l) \underline{x}^{\underline{i}}(P_l)$, $\underline{i} \in \Pi^{(j)}(m)$, because $\sum_{1 \leq l \leq n} c_l f^{(j)}(P_l) \underline{x}^{\underline{i}}(P_l) = 0$, $\underline{i} \in \Pi^{(j)}(m)$ in view of $f^{(j)} \underline{x}^{\underline{i}} \in \mathcal{L}(G)$ for $o(f^{(j)}) + o(\underline{x}^{\underline{i}}) \leq m$.

Now we introduce the error locator ideal

$$I(\mathcal{E}) := \{f \in I_{\mathcal{R}} \mid f(P_l) = 0,\ P_l \in \mathcal{E}\}. \tag{7}$$

Then, the key for decoding is given by the following

Theorem 1. *For $h \in \mathcal{L}(G)$, we take the corresponding polynomial vector $\underline{h} = (h^{(k)})_{0 \leq k \leq a_1 - 1}$ with the component polynomials*

$$h^{(k)} = \sum_{0 \leq i_1 \leq s^{(k)}} \mathrm{coeff}(h^{(k)}, i_1) x_1^{i_1} = \sum_{\underline{i} \in \mathrm{Supp}(h^{(k)})} \mathrm{coeff}(h^{(k)}, \underline{i}) \underline{x}^{\underline{i}},$$

where $s^{(k)}$ is the degree of polynomial $h^{(k)} \in \mathbb{F}_q[x_1]$ and $\mathrm{Supp}(h^{(k)}) \subseteq \{(i_1, 0, \cdots, 0) \in \mathbf{N}_0^M \mid 0 \leq i_1 \leq s^{(k)}\}$. Then, $h \in I(\mathcal{E})$ iff the following M-D compound linear recurrence holds

$$\sum_{0 \leq k \leq a_1 - 1} \sum_{\underline{i} \in \mathrm{Supp}(h^{(k)})} \mathrm{coeff}(h^{(k)}, \underline{i}) u_{\underline{i} + \underline{j}}^{(k)} = 0,\ \underline{j} \in \mathbf{N}_0^M. \tag{8}$$

The following corollary implies that every array $u^{(k)} = (u^{(k)}_{\underline{i}})$, $0 \le k \le a_1 - 1$ has intrinsically the same structure w.r.t. the error locator set $\mathcal{E}$.

Corollary 1. *For $h \in \mathbb{F}_q[\underline{x}]$, it holds that $h \in I(\mathcal{E})$ only if every array $u^{(k)}$, $0 \le k \le a_1 - 1$ satisfies the following (simple) linear recurrence*

$$\sum_{\underline{i} \in \mathrm{Supp}(h)} \mathrm{coeff}(h, \underline{i}) u^{(k)}_{\underline{i}+\underline{j}} = 0,\ \underline{j} \in \mathbf{N}_0^M. \tag{9}$$

Instead of the polynomials $h^{(k)}$ and syndrome arrays $u^{(k)}$, $0 \le k \le a_1 - 1$, we use their *shifted* versions $\tilde{h}^{(k)} := \underline{x}^{\underline{i}^{(k)}} h^{(k)}$ having $\deg(\tilde{h}^{(k)}) = \underline{i}^{(k)} + \deg(h^{(k)})$ and $\mathrm{Supp}(\tilde{h}^{(k)}) := \{\underline{i} = \underline{i}^{(k)} + \underline{j} \in \mathbf{N}_0 \mid \underline{j} \in \mathrm{Supp}(h^{(k)})\}$ and $\tilde{u}^{(k)} = (\tilde{u}^{(k)}_{\underline{i}})$ with $\tilde{u}^{(k)}_{\underline{i}} = u^{(k)}_{\underline{i}-\underline{i}^{(k)}}$, $\underline{i} \ge_P \underline{i}^{(k)}$, where $\le_P$ is the usual partial ordering defined by $\underline{i} = (i_1, \cdots, i_M) \le_P \underline{j} = (j_1, \cdots, j_M) \Leftrightarrow i_k \le j_k$, $1 \le k \le M$. Then, we can rewrite the compound linear recurrence by

$$\sum_{0 \le k \le a_1 - 1} \sum_{\underline{i} \in \mathrm{Supp}(\tilde{h}^{(k)})} \mathrm{coeff}(\tilde{h}^{(k)}, \underline{i}) \tilde{u}^{(k)}_{\underline{i}+\underline{j}} = 0,\ \underline{j} \in \mathbf{N}_0^M. \tag{10}$$

3.2 Vectorial BMS algorithm

We invoke the vectorial M-D BMS algorithm [3][20] for purpose of finding a Gröbner basis of the error locator ideal $I(\mathcal{E})$. Each polynomial $h = \sum_{0 \le k \le a_1 - 1} h^{(k)} f^{(k)} \in I_{\mathcal{R}}$ is represented as the shifted polynomial vector $\underline{\tilde{h}} = (\tilde{h}^{(k)})_{0 \le k \le a_1 - 1}$ instead of the polynomial vector $\underline{h} = (h^{(k)})_{0 \le k \le a_1 - 1}$. For simplicity, we denote $\underline{\tilde{h}}$ as $\underline{h}$, and so $\underline{h} = (\tilde{h}^{(k)})_{0 \le k \le a_1 - 1}$ from now on.

As in [20], for a polynomial vector $\underline{h}^{(k)}$, we define its degree and head position by $\deg(\underline{h}^{(k)})(= \underline{d}^{(k)}) := \max_T\{\deg(\tilde{h}^{(k,k')}) \mid 0 \le k' \le a_1 - 1\}$, $\mathrm{hp}(\underline{h}^{(k)}) := \max\{k' \mid \deg(\tilde{h}^{(k,k')}) = \underline{d}^{(k)}, 0 \le k' \le a_1 - 1\}$.

For $\underline{i}^{(k)} + \Pi := \{\underline{i}^{(k)} + \underline{j} \mid \underline{j} \in \Pi\} \subset \Pi_{\mathcal{R}} + \Pi$ $(:= \{\underline{i} + \underline{j} \mid \underline{i} \in \Pi_{\mathcal{R}}, \underline{j} \in \Pi\})$, we assume that all the components of the error syndrome arrays $\tilde{u}^{(k)} = (\tilde{u}^{(k)}_{\underline{j}})$, $\underline{j} \in \underline{i}^{(k)} + \Pi$, $0 \le k \le a_1 - 1$ are given, so that we have an error syndrome array vector $\underline{u} = (\tilde{u}^{(k)})$. We try to find a set of minimal polynomial vectors $H = \{\underline{h}^{(k)} = (\tilde{h}^{(k,k')})_{0 \le k' \le a_1 - 1} \mid 0 \le k \le a_1 - 1\}$ for the array vector $\underline{u} = (\tilde{u}^{(k')})_{0 \le k' \le a_1 - 1}$ s.t. $\underline{h}^{(k)}[\underline{u}]_{\underline{j}} :=$

$$\sum_{0 \le k' \le a_1 - 1} \sum_{\underline{i} \in \mathrm{Supp}(\tilde{h}^{(k,k')})} \mathrm{coeff}(\tilde{h}^{(k,k')}, \underline{i}) \tilde{u}^{(k')}_{\underline{i}+\underline{j}-\underline{d}^{(k)}} = 0,\ \underline{d}^{(k)} \le_P \underline{i} \le_T \underline{i}(m), \tag{11}$$

where $\underline{i}(m) \in \Pi$ is s.t. $o(\underline{x}^{\underline{i}(m)}) = m$ (we assume its existence), and the set H should be a reduced Gröebner basis of the error locator ideal $I_{\mathcal{E}}$. We take the total ordering $<_{\tilde{T}}$ defined over the components $\tilde{u}^{(k)}_{\underline{i}}$ of the given M-D arrays $\tilde{u}^{(k)} = (\tilde{u}^{(k)}_{\underline{i}})$, $\underline{i} \in \underline{i}^{(k)} + \Pi$, $0 \le k \le a_1 - 1$ by $(\underline{i}, k) <_{\tilde{T}} (\underline{j}, l) \Leftrightarrow \underline{i} <_T \underline{j} \vee (\underline{i} = \underline{j} \wedge k < l)$. Then, by adapting the results about the vectorial BMS algorithm[20] to suit the present case, we have the following:

Proposition 1. *We can find a reduced Gröbner basis of the error locator ideal $I(\mathcal{E})$ by applying the vectorial M-D BMS algorithm[20] to the error syndrome array vector $\underline{u}$ (if given) w.r.t. the total ordering $<_{\tilde{T}}$.*

In the whole process of the vectorial BMS algorithm, at each iteration with $(\underline{i},k)$ along the total ordering $<_{\tilde{T}}$, we find from the set of minimal polynomial vectors $\underline{h}^{(k)}$ for the subarray vector $\underline{u}^{(\underline{i},k)} := (\tilde{u}^{(l)}_{\underline{j}})$, $(\underline{0},0) \leq_{\tilde{T}} (\underline{j},l) <_{\tilde{T}} (\underline{i},k)$ a set of minimal polynomial vectors for the *appended* subarray vector $\underline{u}^{(\underline{i},k)\oplus} := (\tilde{u}^{(l)}_{\underline{j}})$, $(\underline{0},0) \leq_{\tilde{T}} (\underline{j},l) \leq_{\tilde{T}} (\underline{i},k)$, where the discrepancy $\underline{h}^{(k)}[\underline{u}]_{\underline{i}}$ is calculated and used in updating the set of minimal polynomial vectors. We can keep the identity $\mathrm{hp}(\underline{h}^{(k)}) = k$, $\underline{d}^{(k)} = \deg(\tilde{h}^{(k,k)})$, $0 \leq k \leq a_1 - 1$. In addition, we can assume that every minimal polynomial vector $\underline{h}^{(k)}$, $0 \leq k \leq a_1 - 1$ is monic, i.e. the head coefficient $\mathrm{coeff}(\tilde{h}^{(k,k)}, \underline{d}^{(k)}) = 1$.

4 Decoding up to the Kirfel-Pellikaan bound

4.1 Kirfel-Pellikaan bound

As a lower bound for the minimum distance $d(C^{\perp}(G))$ of the multipoint code $C^{\perp}(G)$, Kirfel and Pellikaan [14] gave a formula, which is called the *Kirfel-Pellikaan bound*, similar to the Feng-Rao bound [11] and the order bound of one-point codes. The following is a formulation of the Kirfel-Pellikaan bound of the dual multipoint code (cf. [13]).

For a divisor B and a point Q on a curve, let

$$H(Q;B) := \rho_Q\Big(\bigcup_{i=-\deg(B)}^{\infty} \mathcal{L}(iQ+B) \setminus \{0\}\Big), \tag{12}$$

where $\rho_Q(S)$ is the set of orders (at Q) of functions $f \in S$, and for divisors B_1, B_2

$$N(Q,B_1,B_2) := \{(i,j) \in \mathbf{N}_0^2 \mid i+j \in \rho_Q(B_1+B_2), i \in H(Q;B_1),\ j \in H(Q;B_2)\},$$
$$\nu(Q,B_1,B_2) := \#N(Q,B_1,B_2).$$

In particular, for $Q = P_\infty$, $B_1 = G = mP_\infty - \sum_{1\leq j\leq b} n_j R_j$, $B_2 = 0$, we have

$$\nu(P_\infty, G, 0) = \#\{(i,j) \in \mathbf{N}_0^2 \mid i+j = m, i \in H(P_\infty;G), j \in H(P_\infty;0)\}, \tag{13}$$

where $H(P_\infty;0)$ $(= H(P_\infty)$ mentioned in Section 2) is the set of orders (at P_∞) of functions in the ring R, and $i = \sum_{1\leq k\leq M} a_k i_k$ for $\underline{i} = (i_1, \cdots, i_M) \in \Pi_{\mathcal{R}}$, and $j = \sum_{1\leq k\leq M} a_k j_k$ for $\underline{j} = (j_1, \cdots, j_M) \in \Pi$. We denote $\nu(l) := \nu(P_\infty, lP_\infty - \sum_{1\leq j\leq b} n_j R_j, 0)$ for $l \in \mathbf{N}_0$. As a conclusion, the Kirfel-Pellikaan bound of the dual multipoint code $C^{\perp}(G)$ with $G = mP_\infty - \sum_{1\leq j\leq b} n_j R_j$ is given as

$$d_{\mathrm{KP}} := d_{\mathrm{KP}}(C^{\perp}(G)) = \min\{\nu(l) \mid l \geq m+1\}. \tag{14}$$

It is a kind of order bound similar to the Feng-Rao bound [11] for one-point codes [1], and it is shown by Riemann's theorem that $d_{\mathrm{KP}} \geq d_{\mathrm{G}}^{\perp}$.

Now we remark that $\nu(l) = \#(\cup_{\underline{i} \in \Pi_{\mathcal{R}} + \Pi \text{ s.t. } o(\underline{x}^{\underline{i}}) = l} \Gamma(\underline{i})) \cap \Pi_{\mathcal{R}}$, where $\Gamma(\underline{i}) := \{\underline{j} \in \Pi_{\mathcal{R}} + \Pi \mid \underline{j} \leq_P \underline{i}\}$.

4.2 Decoding with majority logic

First, we mention some definitions and facts necessary for full decoding. For any point $\underline{j} \in (\Pi_{\mathcal{R}} + \Pi) \setminus \Pi$ there exists a unique point $\underline{i} \in \Pi_{\mathcal{R}}$ s.t. $o(\underline{x}^{\underline{i}}) = o(\underline{x}^{\underline{j}})$. We call such a pair of points $\underline{i}$, $\underline{j}$ *conjugate* (with each other). The error syndrome values $u_{\underline{i}}^{(k)}$ and $u_{\underline{j}}^{(k)}$ at a pair of conjugate points $\underline{i}$ and $\underline{j}$ are related by the following linear recurrence (we call *permanent*)

$$f_{\mathcal{X}}[u^{(k)}]_{\underline{i}} = 0,\ \underline{i} \in \underline{i}^{(k)} + \Pi \tag{15}$$

corresponding to any curve defining polynomial $f_{\mathcal{X}} \in B(I_{\mathcal{X}})$.

In connection with majority voting for decoding up to the Kirfel-Pellikaan bound, we need the following theorem derived from the Buchberger criterion, which implies a linear dependence among shifted component arrays.

Theorem 2. *There exist* $c_l \in \mathbb{F}_q$ *and* $\underline{\delta}^{(l)} >_T \underline{0}$, $0 \leq l \leq a_1 - 1$ *s.t. the following identities hold:*

$$\tilde{u}_{\underline{i}}^{(j)} = \tilde{u}_{\underline{i}}^{(k)} + \sum_{0 \leq l \leq a_1 - 1} c_l \tilde{u}_{\underline{i} - \underline{\delta}^{(l)}}^{(l)} \tag{16}$$

for any $0 \leq j \neq k \leq a_1 - 1$ *and* $\underline{i} \in \Sigma^{(j,k)}$*, where* $\Sigma^{(j,k)}$ *is a subset of* $\mathbf{N}_0^M$ *which contains* $\Sigma'^{(j,k)} := \{\underline{i} \mid \underline{i} \geq_P \underline{i}^{(j)} \text{ or } \underline{i} \geq_P \underline{i}^{(k)}\} \cap (\cap_{0 \leq l \leq a_1 - 1} \{\underline{i} \mid \underline{i} \geq_P \underline{i}^{(l)} + \delta^{(l)}\})$.

In sequel we consider the vectorial BMS algorithm and its application to the syndrome array vector accompanied with the values extrapolated by using the identities (14).

In decoding, the method mentioned in 3.2 does not always work because we are given only the syndrome values calculated from the received word $\underline{r}$

$$u_{\underline{j}}^{(k)} = S_{\underline{j}}^{(k)},\ \underline{j} \in \Pi^{(k)}(m),\ 0 \leq k \leq a_1 - 1,$$

which are called *known* syndromes and the other are *unknown*. From the known syndromes, we can decode correctly provided that the number of errors $t \leq \lfloor \frac{1}{2}(d_{\mathrm{G}}^{\perp} - g - 1) \rfloor$. For the full decoding up to the Goppa bound, we need some majority voting scheme to find the unknown syndrome values $u_{\underline{j}}^{(k)}$, $\underline{j} \notin \Pi^{(k)}(m)$, $0 \leq k \leq a_1 - 1$ as in decoding of one-point codes[1].

From the known syndromes, we can get a minimal polynomial vector set H and an auxiliary polynomial vector set A of the subarray vector $\underline{u}^{m+1} := \underline{u}^{(\underline{i}(m), a_1 - 1)}$. Now, assume that we have got already the syndrome subarray vector

$\underline{u}^l$ for some $l > m$ together with a pair of H and A of $\underline{u}^l$, which is accompanied with the following subsets

$$\Sigma(H) := \{\underline{i} \in \Pi_{\mathcal{R}} \mid \underline{i} \geq_P \deg(\underline{h}^{(j)}),\, \underline{h}^{(j)} \in H, 0 \leq j \leq a_1 - 1\},$$
$$\Delta(A) := \{\underline{i} \in \Pi \mid \underline{i} \leq_P \mathrm{span}(\underline{g}),\, \underline{g} \in A\},$$

where the *span* of a polynomial vector $\underline{g}$ is defined to be $\mathrm{span}(\underline{g}) := \underline{i} - \deg(\underline{g}) \in \Pi$ for the point $\underline{i}$ where the polynomial vector $\underline{g}$ had the discrepancy $\underline{g}[\underline{u}^{(k)}]_{\underline{i}} \neq 0$ (i.e. $\underline{g}$ was not valid for $\underline{u}^{(k)}$, $0 \leq^{\exists} k \leq a_1 - 1$) for the first time as a member of a minimal polynomial vector set at $\underline{i}$ (About these details, see [20]).

Now, at every $\underline{i} \in \Pi_{\mathcal{R}} + \Pi$ s.t. $o(\underline{x}^{\underline{i}}) = l$, for each $\underline{h}^{(k)} \in H$, $0 \leq k \leq a_1 - 1$ s.t. $\deg(\underline{h}^{(k)}) \leq_P \underline{i}$, we calculate the candidate values $\hat{u}_{\underline{i}}^{(k)}$

$$\hat{u}_{\underline{i}}^{(k)} = - \sum_{\underline{j} \in \mathrm{Supp}(\tilde{h}^{(k,k)}) \setminus \{\underline{d}^{(k)}\}} \mathrm{coeff}(\tilde{h}^{(k,k)}, \underline{j}) \tilde{u}^{(k)}_{\underline{i}+\underline{j}-\underline{d}^{(k)}}$$
$$- \sum_{k' \neq k,\, 0 \leq k' \leq a_1 - 1} \sum_{\underline{j} \in \mathrm{Supp}(\tilde{h}^{(k,k')})} \mathrm{coeff}(\tilde{h}^{(k,k')}, \underline{j}) \tilde{u}^{(k')}_{\underline{i}+\underline{j}-\underline{d}^{(k)}}.$$

Furthermore, we use also the permanent recurrence to find some additional candidate values, if possible. Then, we define a party as a maximal subset $H' \subset H$ which satisfies the following condition:

> ($\star$) All $\underline{h}^{(k)} \in H'$ give the candidate values at conjugate points $\underline{i}$ s.t. $o(\underline{x}^{\underline{i}}) = l$ which are *consistent* with each other in the sense that any linear dependence (16) shown in Theorem 2 is not violated.

In addition, the number of votes for a party H' is defined as $v(H') :=$

$$\# \cup_{\underline{i} \in \Pi_{\mathcal{R}} + \Pi \text{ s.t. } o(\underline{x}^{\underline{i}}) = l} (\Gamma(\underline{i}) \cap \Pi_{\mathcal{R}} \cap \Sigma(H')) \setminus (\underline{i} - \Delta(A))$$

and the total number of votes at l is defined as $v(l) :=$

$$\cup_{\underline{i} \in \Pi_{\mathcal{R}} + \Pi \text{ s.t. } o(\underline{x}^{\underline{i}}) = l} (\Gamma(\underline{i}) \cap \Pi_{\mathcal{R}} \cap \Sigma(H)) \setminus (\underline{i} - \Delta(A)),$$

where $\underline{i} - \Delta(A) := \{\underline{i} - \underline{j} \in \Pi_{\mathcal{R}} + \Pi \mid \underline{j} \in \Delta(A)\}$. The above-defined number $v(H')$ of votes for a party $H' \subset H$ is just equal to the increase in the cardinality of the delta set at the iteration corresponding to the order l when polynomial vectors $\underline{h}^{(k)} \in H'$ are not valid so that they are updated and replaced by new polynomial vectors. Then, from the nature of iteration of BMS algorithm, we can prove the following theorem, which assures the validity of the vectorial BMS algorithm with majority voting for finding the correct values of the unknown syndrome in case of correctable number of errors (See the similar reasoning in decoding one-point codes with majority voting [4][1]).

Theorem 3. *Provided the actual number of errors is $t \leq t_{\mathrm{KP}}$, the party of polynomial vectors $\underline{h}$ in H which give the correct syndrome values $u_{\underline{i}}^{(k)}$ at points $\underline{i}$ conjugate with each other have the majority of votes among H.*

Thus, we can decode up to the Goppa bound with computational complexity $\mathcal{O}(a_1 n^2) \sim \mathcal{O}(g n^2)$, where the minimum nonzero pole order $a_1 \sim g$.

References

1. S. Sakata, H. Jensen, T. Høholdt, "Generalized Berlekamp-Massey decoding of algebraic geometric codes up to the Feng-Rao bound," *IEEE Trans. Inform. Th.*, 41, pp.1762–1768, 1995.
2. S. Sakata, M. Fujisawa, "Fast Decoding of Multipoint Codes from Algebraic Curves," *IEEE Trans. Inform. Th.*, 60, pp.2054–2064, 2014.
3. S. Sakata, "Finding a minimal polynomial vector set of a vector of nD arrays," *LNSC*, 539, Springer, pp.414–425, 1991.
4. S. Sakata, J. Justesen, Y. Madelung, H. Jensen, T. Høholdt, "A fast decoding method of AG codes from Miura-Kmiya curves up to half the Feng-Rao bound," *Finite Fields & Appl.*, 1, pp.83–101, 1994.
5. R. Kötter, "A fast parallel implementation of a Berlekamp-Massey algorithm for algebraic geometry codes," *IEEE Trans. Inform. Th.*, 44, pp.1358–1368, 1998.
6. P. Beelen, K. Brander, "Efficient list decoding of a class of algebraic geometry codes, " Advances in Mathematics of Communications, pp.485-518, Nov. 2010.
7. K. Lee, M.B. Amoros, M.E. O'Sullivan, "Unique decoding of plane AG codes via interpolation," *IEEE Trans. Inform. Th.*, 58, pp.3941–3950, 2012.
8. M. Homma, S.J. Kim, "The complete determination of the minimum distance of two-point codes on a Hermitian curve," *Designs, Codes & Crypt.*, 40, pp.5–24, 2006.
9. N. Drake and G. Matthews, "Minimum distance decoding of general algebraic geometry codes via lists," *IEEE Trans. Inform. Th.*, 56, pp.4335–4340, 2010.
10. V.D. Goppa, "Codes associated with divisors," *Probl. Pered. Inform.*, 13, pp.33-39, 1977. Translation: *Probl. Inform. Trans.*, 13, pp.22–26, 1977.
11. Gui-Liang Feng and T.R.N. Rao, "Decoding algebraic-geometric codes up to the designed minimum distance," *IEEE Trans. Inform. Th.*, 39, pp.37–45, 1993.
12. T. Høholdt, J.H. van Lint, R. Pellikaan, "algebraic geometry codes," in: V.S. Press, W.C. Huffman (Eds.), "*Handbook of Coding Theory*," Vol. I, II, North-Holland, Amsterdam, pp.871–961, 1998.
13. P. Beelen, "The order bound for general algebraic geometric codes," *Finite Fields & Appl.*, 13, pp.665-680, 2007.
14. K. Kirfel, R. Pellikaan, "The minimum distance of codes in an array coming from telescopic semigroups," *IEEE Trans. Inform. Th.*, 41, pp.1720–1732, 1995.
15. I.M. Duursma, R. Kirov, S. Park, "Distance bounds for algebraic geometric codes," *Journal of Pure and Applied Algebra*, 215, pp.1863–1878, 2011.
16. K. Lee, M.B. Amoros, M.E. O'Sullivan, "Unique decoding of general AG codes," *IEEE Trans. Inform. Th.*, 60, 2038–2053, 2014.
17. O. Geil, R. Pelikaan, "On the structure of order domain," *Finite Felds, & Appl.*, 8, pp.369–396, 2002.
18. R. Matsumoto, S. Miura, "On construction and generalization of algebraic geomery codes," in *Proc. Algebraic Geometry, Number Theory, Coding Theory and Cryptography*, T. Katsura et al., Eds. Univ. Tokyo, Japan, pp.3–15, 2000.
19. O. Geil, R. Matsumoto, D. Ruano, "List decoding algorithm based on voting in Gröbner bases for general one-point AG codes," Proc. of International Synposium on Information Theory, pp.86–90, 2012.
20. Sakata, "The BMS Algorithm" in *Groebner Bases, Coding, and Cryptography* (eds. Sala et.), Springer, pp.143–163, 2009.
21. T. Mora, "Groebner Thechnology," in *Groebner Bases, Coding, and Cryptography* (eds. Sala et.), Springer, pp.1–25, 2009.