The BMS Algorithm and Decoding of AG Codes

Shojiro Sakata

Abstract In this paper, we review various decoding methods of algebraic geometry (or algebraic-geometric) codes (Goppa in Soviet Math. Dokl. 24(1):170–172, 1981; Høholdt et al. in Handbook of coding theory, vols. I, II, North-Holland, Amsterdam, pp. 871–961, 1998; Geil in Algebraic geometry codes from order domains, this volume, pp. 121–141, 2009) mainly based on the Gröbner basis theory (Buchberger in Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal, Ph.D. thesis, Innsbruck, 1965; Aequationes Math. 4:374–383, 1970; Multidimensional systems theory, Reidel, Dordrecht, pp. 184–232, 1985; London Math. Soc. LNS 251:535–545, 1998; J. Symb. Comput. 41(3–4):475–511, 2006; Mora in Gröbner technology, this volume, pp. 11–25, 2009b) as well as the BMS algorithm (Sakata in J. Symbolic Comput. 5(3):321–337, 1988; Inform. and Comput. 84(2):207–239, 1990) and its variations (Sakata in n-dimensional Berlekamp–Massey algorithm for multiple arrays and construction of multivariate polynomials with preassigned zeros, LNCS, vol. 357, pp. 356–376, 1989; Finding a minimal polynomial vector set of a vector of nD arrays, LNCS, vol. 539, pp. 414–425, 1991), where the BMS algorithm itself is reviewed in another paper (Sakata in The BMS algorithm, this volume, pp. 143–163, 2009) in this issue. The main subjects are:

(1) Syndrome decoding of dual codes up to the designed distance (Saints and Heegard in IEEE Trans. Inform. Theory 41(6):1733–1751, 1995; Sakata et al. in Finite Fields Appl. 1(1):83–101, 1995b; IEEE Trans. on Inf. Th. 41(6):1672–1677, 1995c; IEEE Trans. on Inf. Th. 41(6):1762–1768, 1995a) by using the BMS algorithm. (There have been published several methods of decoding algebraic geometry codes, e.g. Kötter in On decoding of algebraic-geometric and cyclic codes, Ph.D. thesis, Linköping University, 1996; O'Sullivan in IEEE Trans. on Inf. Th. 41(6):1709–1719, 1995; Guerrini and Rimoldi in FGLM-like decoding: from Fitzpatrick's approach to recent developments, this volume, pp. 197–218, 2009, which are described in some terminology rather from the perspective of algebraic geometry, but are in principle equivalent to the BMS decoding method. We omit their descriptions here.)

(2) List decoding of primal codes (Numakami et al. in IEICE Trans. Fundamentals J83:1309–1317, 2000; Sakata in LNCS, vol. 2227, pp. 172–181, 2001; Proc. of ISIT2003, pp. 363–363, 2003). (The original list decoding algorithms are given for RS codes by Sudan in J. of Complexity 13:180–193, 1997, and for algebraic geometry codes by Shokrollahi and Wassermann in IEEE Trans. on Inf. Th. 45(2):432–437,

S. Sakata
The University of Electro-Communications, Chofu-shi, Tokyo 182-8585, Japan
e-mail: sakata@ice.uec.ac.jp

M. Sala et al. (eds.), *Gröbner Bases, Coding, and Cryptography*,
DOI 10.1007/978-3-540-93806-4_10, © Springer-Verlag Berlin Heidelberg 2009

1999, and their improved versions by Guruswami and Sudan in IEEE Trans. on Inf. Th. 45:(6):1757–1767, 1999.)

(3) Other relevant decoding algorithms of primal and dual codes (Augot in Proc. of ISIT2002, pp. 86–86, 2002; Justesen and Høholdt in A course in error-correcting codes, EMS Textbooks in Mathematics, EMS, 2004; Fujisawa and Sakata in Proc. of SITA2005, pp. 543–546, 2005; Sakata and Fujisawa in Proc. of SITA2006, pp. 93–96, 2006; Fujisawa et al. in Proc. of SITA2006, pp. 101–104, 2006).

In discussing list decoding and usual bounded-distance decoding of primal/dual codes we show that multi-variate interpolation problem is a key and that it can be solved by using the BMS algorithm efficiently. The computational complexities of our methods are less than the other decoding methods including the Feng–Rao (IEEE Trans. on Inf. Th. 39(1):37–45, 1993) algorithm simply based on Gaussian elimination. These reductions in computational complexity are based on the special structures or properties of the given input data (syndrome arrays, etc.) which originate in the definition of codes themselves and are used cleverly by the BMS algorithm. In Leonard (A tutorial on AG code decoding from a Gröbner basis perspective, this volume, pp. 187–196, 2009b), Guerrini and Rimoldi (FGLM-like decoding: from Fitzpatrick's approach to recent developments, this volume, pp. 197–218, 2009) in this issue, several other efficient decoding methods of algebraic geometry codes from Gröbner basis perspectives are reviewed. Additionally, we mention a recent development of decoding algorithm based on higher-dimensional interpolation (Parvaresh and Vardy in Proc. of IEEE FOCS2005, IEEE Computer Society, pp. 285–294, 2005), which has error correction performance superior to the improved list decoding by Guruswami and Sudan. As a general method of multivariate interpolation the BMS algorithm is an alternative of the Buchberger–Möller (The construction of multivariate polynomials with preassigned zeros, LNCS, vol. 144, pp. 24–31, 1982), Mora (The FGLM problem and Möller's algorithm on zero-dimensional ideals, this volume, pp. 27–45, 2009a) algorithm and the Marinani–Möller–Mora (AAECC 4:(2):103–145, 1993) algorithm, but any exact comparisons of computational complexities of these methods remain to be investigated.

1 Introduction

In this paper, we review various decoding methods of algebraic geometry (or algebraic-geometric) codes over finite fields, particularly one-point codes from algebraic curves mainly based on the BMS algorithm (Sakata 1988, 1990), which we review in another paper (Sakata 2009) in this issue, and we use almost the same terminology as *ibid*. These *algebraic geometry codes* are the most important class of error-correcting codes from both practical and theoretical viewpoints. They are a subclass of so-called *linear codes* which are defined as linear subspaces of the vector space $\mathbb{F}_q^n = (\mathbb{F}_q)^n$ over a finite field $\mathbb{F}_q$. Since most of the basic concepts in Coding Theory are introduced in another paper (Augot et al. 2009) in this issue, we omit many of their detailed descriptions here and assume that the readers know terminologies such as (n, k, d)-code C $(\subset \mathbb{F}_q^n)$ over $\mathbb{F}_q$, codelength n, dimension k, minimum distance d, the number $t = \lfloor \frac{d-1}{2} \rfloor$ of correctable errors, etc. Decoding, which is to recover or estimate the sent codeword $\mathbf{c} \in C$ from the given received word $\mathbf{r} \in \mathbb{F}_q^n$, is a kind of algebraic computation procedure over the finite field $\mathbb{F}_q$, and it is given basically in the form of an algorithm. If the received word $\mathbf{r}$ contains more errors than t, the decoding algorithm might output a wrong codeword which is different from the sent codeword. But, error events are probabilistic phenomena in practical applications, and more errors can occur with less probability, which usually is negligibly smaller. Therefore, in decoding, we have only to find candidate codewords which are as close to the received word $\mathbf{r}$ as possible.

The algebraic geometry codes which we are going to discuss in this paper are defined based on a triplet $(\mathcal{K}, \mathcal{L}, \mathcal{C})$, where $\mathcal{K}$ is the set of symbols carrying information with them and $\mathcal{L}$ is the set of *locators* (or labels) P_j denoting the position or index j of each component symbol c_j $(\in \mathbb{F}_q)$ of a codeword $\mathbf{c} = (c_j)_{0 \le j \le n-1}$. We call $\mathcal{K}$ and $\mathcal{L}$ the *information symbol set* and the *symbol locator set*, respectively. The set $\mathcal{C}$ is a linear space of functions defined on a domain including $\mathcal{L}$, from which we have two kinds of codes as follows. First, we have a code C which is the subspace of $(\mathbb{F}_q)^n$ composed of the vectors $\mathrm{ev}(f) := (f(P_0), \ldots, f(P_{n-1})) \in \mathbb{F}_q^n$ corresponding to a function $f \in \mathcal{C}$. Second, we have another code which is the orthogonal complement (*null space*) of the subspace C in $\mathbb{F}_q^n$

$$C^\perp := \{\mathbf{c} = (c_j) \in \mathbb{F}_q^n \mid \mathbf{c} \cdot \mathrm{ev}(f) = 0\},$$

where $\mathbf{c} \cdot \mathrm{ev}(f) := \sum_{0 \le j \le n-1} c_j f(P_j) (\in \mathbb{F}_q)$ is the inner product of two vectors $\mathbf{c}$ and $\mathrm{ev}(f)$ $(\in \mathbb{F}_q^n)$. Sometimes we call C and $C^\perp$ *primal* and *dual* codes, respectively.[1]

For example, primal and dual Reed–Solomon codes C and $C^\perp$, which are nowadays one of the most practically used algebraic error-correcting codes, are defined[2] by taking $\mathcal{K} := \mathbb{F}_q$, $n := q - 1$, $\mathcal{L} := \{P_j (:= \alpha^j) \mid 0 \le j \le n - 1 (= q - 2)\} (= \mathbb{F}_q \setminus \{0\})$, and $\mathcal{C} := \{f \in \mathbb{F}_q[x] \mid \deg(f) \le h - 1\}$ for a certain integer h s.t. $0 < h < n$. Their dimensions and minimum distances are

$$k(C) = h, \qquad k(C^\perp) = n - h; \qquad d(C) = n - h + 1, \qquad d(C^\perp) = h + 1.$$

RS codes are among the broader class of *one-point* codes from algebraic curves which contains codes having better performance and greater potentialities in the near future. One-point codes from an algebraic curve $\mathcal{X}$ over a finite field $\mathbb{F}_q$ are

---

[1] About the definition of these codes, see also another paper (Leonard 2009a) in this issue, where C and $C^\perp$ are called *functionally encoded* and *functionally decoded codes*, respectively. Furthermore, about codes from order domains, which are a generalization of these codes and can be decoded by our methods, see Geil (2009).

[2] This definition of the dual RS code $C^\perp$ is equivalent to the conventional definition $C^\perp := \{c(x) = a(x)g(x) \mid a(x) \in \mathbb{F}_q[x],\ \deg(a) \le n - h - 1\}$ s.t. each codeword $\mathbf{c} = (c_j) \in C^\perp$ is represented as a polynomial $c(x) = \sum_{0 \le j \le n-1} c_j x^j$, where $g(x) := \prod_{0 \le i \le h-1} (x - \alpha^i)$ is the generator polynomial of the code.

defined by taking $\mathcal{K} := \mathbb{F}_q$, $\mathcal{L} := \{P_j \mid 0 \le j \le n-1\}$, which is a set of $\mathbb{F}_q$-rational points on the curve $\mathcal{X}$, and $\mathcal{C} := L(mP_\infty)$, which is the set of algebraic functions on the curve $\mathcal{X}$ having a single pole at the infinity point P_∞ with *pole order* less than or equal to m, where m is a given integer. Similarly, we have primal and dual codes C and $C^\perp$. As a special case, if we take as $\mathcal{X}$ the projective line over $\mathbb{F}_q$ containing the infinity point P_∞ as well, and let $\mathcal{L}$ be the set of all affine points on $\mathcal{X}$ or equivalently the finite field $\mathbb{F}_q$, then we have the *extended* RS code with length $n = q$. By deleting 0 from $\mathcal{L}$, we have the ordinary RS code of length $n = q-1$.

Although we can take the defining curve $\mathcal{X}$ in the projective space of any dimension N, we restrict to a plane curve $\mathcal{X}$ (i.e. $N = 2$) or particularly the Hermitian curve over $\mathbb{F}_q$ as follows, where $q = q_1^2$.

$$\mathcal{X} : y^{q_1} - x^{q_1+1} + y = 0.$$

We take as $\mathcal{L}$ all the $\mathbb{F}_q$-rational points on $\mathcal{X}$ excluding the infinity point P_∞, where we remember that the coordinate functions x and y have pole orders $o(x) = q_1$ and $o(y) = q_1 + 1$, respectively at the single pole P_∞. For $a = (a_1, a_2) \in \mathbf{N}^2$. we denote $X^a := x^{a_1} y^{a_2}$, which has pole order $o(X^a) = q_1 a_1 + (q_1+1)a_2$. Letting $\Pi := \{a = (a_1, a_2) \in \mathbf{N}^2 \mid 0 \le a_2 \le q_1 - 1\}$, $\Pi(m) := \{a = (a_1, a_2) \in \Pi \mid o(X^a) = q_1 a_1 + (q_1+1)a_2 \le m\}$, and $\mathcal{C} = \langle X^a = x^{a_1} y^{a_2} \mid a = (a_1, a_2) \in \Pi(m)\rangle_{\mathbb{F}_q} \subset \mathbb{F}_q[\Pi]$ $(:= \langle X^a \mid a \in \Pi\rangle_{\mathbb{F}_q})$, we can have the primal code $C = C(m)$ and the dual code $C^\perp = C^\perp(m)$ with length $n := q_1^3$, whose dimensions and minimum distances are as follows in case of $2g - 1 \le m < n$, where $g = \frac{q_1(q_1-1)}{2}$ is the genus of the curve $\mathcal{X}$:

$$k(C) = m - g + 1, \qquad d(C) \ge n - m;$$
$$k(C^\perp) = n - m + g - 1, \qquad d(C^\perp) \ge m - 2g + 2,$$

where $d_G := n - m$ and $d_G^\perp := m - 2g + 2$ are called *Goppa bound*s of the primal code C and the dual code $C^\perp$, respectively. Actually, if $m + m' = q_1^3 + q_1^2 - q_1 - 2$, the primal Hermitian code $C(m)$ and the dual Hermitian code $C^\perp(m')$ are equivalent (Stichtenoth 1988).

2 Syndrome Decoding of Dual Codes

First we show that decoding of a dual RS code $C^\perp$ with minimum distance $d = h + 1$ is reduced to the problem of finding a polynomial in $\mathbb{F}_q[x]$ which is *valid* for a certain one-dimensional (1-D) array derived from the received word. Let $\mathbf{c} = (c_j)_{0 \le j \le n-1} \in C^\perp$ and $\mathbf{e} = (e_j)_{0 \le j \le n-1} \in \mathbb{F}_q^n$ be a *sent* codeword and an *error vector*, respectively. Then, the received word is $\mathbf{r} = \mathbf{c} + \mathbf{e} = (r_j)_{0 \le j \le n-1} \in \mathbb{F}_q^n$, where $r_j = c_j + e_j$, $0 \le j \le n-1$. We assume that the number of errors, or in other words the size of the set $\mathcal{E} := \{P_j \mid e_j \ne 0\}$ $(\subset \mathcal{L})$ of *error locators*, is $t' := \#\mathcal{E} \le t$, where t $(= \lfloor \frac{h}{2} \rfloor)$ is the number of correctable errors. The receiver gets the received word $\mathbf{r} = (r_j)$, but he has no knowledge of both $\mathbf{c}$ and $\mathbf{e}$. How can he find either $\mathbf{c}$ or

e from **r**? Since no error, i.e. the case of $\mathbf{e} = 0$ is the most likely in actual channels, he begins with checking whether the received word **r** contains any error or not. For a dual RS code, it is very easy and he has only to check for some $f \in \mathcal{C}$ whether the inner product $\mathbf{r} \cdot \mathrm{ev}(f) = 0$ or not. More precisely, he calculates the syndromes $s_i := \mathbf{r} \cdot \mathrm{ev}(x^i)$ corresponding to the basis functions x^i, $0 \le i \le h-1$ of the function space $\mathcal{C}$, and obtains the array $s = (s_i)_{0 \le i \le h-1}$. If $s = 0$, then he most probably can suppose no error so that he does not need to go further. But, if $s \neq 0$, then he enters the procedure of decoding. A basic decoding method consists of two stages, finding the error locators, i.e. the unknown j_i or α^{j_i}, $1 \le i \le t'$ for $\mathcal{E} = \{\alpha^{j_i} \mid 1 \le i \le t'\}$, and calculating the error values e_{j_i}, $1 \le i \le t'$. Provided the error locators $\mathcal{E}$ are found in the first stage, the second stage is easier and reduced to finding the unique solution e_{j_i}, $1 \le i \le t'$ of the linear system of equations: $\sum_{1 \le i \le t'} e_{j_i} \alpha^{j_i j} = s_j$, $0 \le j \le h-1$.

Now, our main concern is in the first stage. Assuming $t' \le t$ for $\mathcal{E} = \{\alpha^{j_i} \mid 1 \le i \le t'\}$, where t' and j_i, $1 \le i \le t'$ are unknown, we consider an infinite array $u = (u_j)$ defined by $u_j := \mathbf{e} \cdot \mathrm{ev}(x^j) = \sum_{1 \le i \le t'} e_{j_i} \alpha^{j_i j}$, $j \in \mathbf{N}$ instead of s, and further the ideal $\mathbf{I} = \mathbf{I}(u) := \{f \in \mathbb{F}_q[x] \mid f \circ u = 0\}$, which is called the *characteristic ideal* of u, as well as the zero variety $V(\mathbf{I}) := \{\gamma \in \mathbb{F}_q \mid f(\gamma) = 0,\ \forall f \in \mathbf{I}\}$ defined by it, where for $f = f(x) = \sum_{0 \le l \le d} f_l x^l$, $v = f \circ u := (v_j)_{j \in \mathbf{N}}$ is the array defined by $v_j := \sum_{0 \le l \le d} f_l u_{l+j}$, $j \in \mathbf{N}$ (see Sakata 2009). Actually, we have

Lemma 1 $\mathcal{E} = V(\mathbf{I})$.

Proof For $f = f(x) = \sum_{0 \le l \le d} f_l x^l$, we have

$$\begin{aligned} f(\alpha^{j_i}) = 0, \quad 1 \le i \le t' \quad &\Leftrightarrow \quad \sum_{0 \le l \le d} f_l \alpha^{j_i l} = 0, \quad 1 \le i \le t' \\ &\Leftrightarrow \quad \sum_{1 \le i \le t'} \Bigg(\sum_{0 \le l \le d} f_l \alpha^{j_i l} \Bigg) e_{j_i} \alpha^{j_i j} = 0, \quad \forall j \in \mathbf{N} \\ &\Leftrightarrow \quad \sum_{0 \le l \le d} f_l \sum_{1 \le i \le t'} e_{j_i} \alpha^{j_i (l+j)} = 0, \quad \forall j \in \mathbf{N}, \end{aligned}$$

where the last identity is equivalent to $\sum_{0 \le l \le d} f_l u_{l+j} = 0$, $\forall j \in \mathbf{N}$, i.e. $f \circ u = 0$. By the way, the equivalence between the second and third identities comes from the fact that t' arrays $u^{(i)} := (u_j^{(i)})$, $1 \le i \le t'$ which are defined by $u_j^{(i)} := \alpha^{j_i j}$ are linearly independent of each other. $\square$

Since we have that $s_i = \mathbf{r} \cdot \mathrm{ev}(x^i) = (\mathbf{c} + \mathbf{e}) \cdot \mathrm{ev}(x^i) = \mathbf{e} \cdot \mathrm{ev}(x^i)$, $0 \le i \le h-1$, the subarray $u^h := (u_j)_{0 \le j \le h-1}$ of the above infinite array u coincides with the syndrome array $s = (s_j)_{0 \le j \le h-1}$, although we cannot obtain the whole infinite array u. Particularly, the values u_j, $j \ge h$ sometimes are called *unknown syndromes*. However, if $\deg(f) = t' \le t$, in view of $h - 1 - t' \ge t' - 1$, for $1 \le i \le t'$, we have t' finite arrays $u_j^{(i)} := \alpha^{j_i j}$, $0 \le j \le h - 1 - t'$, which also are linearly independent of each other. Consequently, we have for $V(f) := \{\gamma \in \mathbb{F}_q \mid f(\gamma) = 0\}$,

$$\mathcal{E} = V(f) \quad \Leftrightarrow \quad \sum_{0 \le l \le t'} f_l u_{l+j} = 0, \quad 0 \le j \le h - 1 - t', \tag{1}$$

which implies that we can find the error locators $\mathcal{E}$ as the roots of a polynomial f which is valid for the *known syndromes* $u_i (= s_i)$, $0 \le i \le h - 1$ obtained from the received word $\mathbf{r}$ and has the minimum degree, provided the actual number t' of errors contained in $\mathbf{r}$ does not exceed the number t of correctable errors.

As we have seen, the problem of decoding dual RS codes is reduced to finding a valid polynomial for a certain finite (1-D) array. Naturally this fact can be extended to the problem of decoding more general codes including *codes from algebraic curves*. Particularly, in the multidimensional case, it also implies that we must find a Gröbner basis of the characteristic ideal of the array. Below we will show that the decoding of a dual Hermitian code $C^\perp$ is reduced to the problem of finding a minimal polynomial set (in $\mathbb{F}_q[x, y]$) of a certain 2-D array derived from a received word.

Let $\mathbf{c} = (c_j) \in C^\perp$, $\mathbf{e} = (e_j) \in \mathbb{F}_q^n$, $\mathbf{r} = \mathbf{c} + \mathbf{e} = (v_j) \in \mathbb{F}_q^n$ be the sent codeword, the error vector, and the received word, respectively. We assume that the size of the error locators $\mathcal{E} := \{P_j \mid e_j \neq 0\} = \{P_{l_i} \mid 1 \le i \le t'\} (\subset \mathcal{L})$ is $t' := \#\mathcal{E} \le t_G^\perp := \lfloor \frac{d_G^\perp - 1}{2} \rfloor$. As each point of the curve can be represented as $P_l = (\alpha_l, \beta_l) \in (\mathbb{F}_q)^2$, the syndrome $s = (s_a)$, with $a \in \Pi(m)$, obtained by $s_a := \mathbf{r} \cdot \mathrm{ev}(X^a)$ from the received word $\mathbf{r}$ is a finite subarray of the infinite 2-D array $u = (u_a)$, $a \in \mathbf{N}^2$, defined by

$$u_a := \mathbf{e} \cdot \mathrm{ev}(X^a) = \sum_{1 \le i \le t'} e_{l_i} \alpha_{l_i}^{a_1} \beta_{l_i}^{a_2}, \quad a = (a_1, a_2) \in \mathbf{N}^2,$$

which we call *error locator array*. About the *characteristic ideal* (*submodule*) $\mathbf{I} = \mathbf{I}(u) := \{f \in \mathbb{F}_q[\Pi] \mid f \circ u = 0\}$ of a 2-D array $u = (u_a)$, $a \in \mathbf{N}^2$ and its zero variety $V(\mathbf{I}) := \{P \in \mathcal{L} \mid f(P) = 0, \ \forall f \in \mathbf{I}\}$, we have the following lemma similar to Lemma 1. Thus, we call $\mathbf{I}$ also the *error locator ideal* (or *submodule*), and sometimes denote it as $\mathbf{I}(\mathbf{e})$ (or $\mathbf{M}(\mathbf{e})$).

Lemma 2 $\mathcal{E} = V(\mathbf{I})$.

Proof For $f = f(x, y) = f(X) = \sum_{a \in \mathrm{supp}(f)} c(f, a) X^a \in \mathbb{F}_q[\Pi]$, we have

$$\begin{aligned}
& f(\alpha_{l_i}, \beta_{l_i}) = 0, \quad 1 \le i \le t' \quad \Leftrightarrow \\
& \sum_{a = (a_1, a_2) \in \mathrm{supp}(f)} c(f, a) \alpha_{l_i}^{a_1} \beta_{l_i}^{a_2} = 0, \quad 1 \le i \le t' \quad \Leftrightarrow \\
& \sum_{1 \le i \le t'} \left(\sum_{a \in \mathrm{supp}(f)} c(f, a) \alpha_{l_i}^{a_1} \beta_{l_i}^{a_2} \right) e_{l_i} \alpha_{l_i}^{b_1} \beta_{l_i}^{b_2} = 0, \quad (*) \quad \Leftrightarrow \\
& \sum_{a \in \mathrm{supp}(f)} c(f, a) \sum_{1 \le i \le t'} e_{l_i} \alpha_{l_i}^{a_1 + b_1} \beta_{l_i}^{a_2 + b_2} = 0, \quad (*)
\end{aligned}$$

where $(*)$ implies "$\forall b = (b_1, b_2) \in \mathbf{N}^2$". The last identity is equivalent to $\sum_{a \in \mathrm{supp}(f)} c(f, a) u_{a+b} = 0$, $\forall b \in \mathbf{N}^2$, i.e. $f \circ u = 0$. The equivalence between the second and third identities comes from the fact that t' arrays $u^{(l)} := (u_a^{(l)})$, $1 \le l \le t'$ defined by $u_a^{(l)} := \alpha_l^{a_1} \beta_l^{a_2}$, $a \in \mathbf{N}^2$, are linearly independent from each other. □

In the above, for the ring $\mathcal{P} := \mathbb{F}_q[x, y]$, the function space $\mathbb{F}_q[\Pi] := \langle X^a = x^{a_1} y^{a_2} \mid a = (a_1, a_2) \in \Pi \rangle_{\mathbb{F}_q}$ is viewed as a $\mathcal{P}$-submodule which coincides with the whole set $\mathcal{P}$ (as a module) modulo the $\mathcal{P}$-submodule $\mathbf{M}_{\mathcal{X}} := \langle y^{q_1} - x^{q_1+1} + y \rangle_{\mathcal{P}}$. The known syndromes $s_a = \mathbf{r} \cdot \mathrm{ev}(X^a)$, $a \in \Pi(m)$, which are obtained from the received word, are identical with the subarray u_a, $a \in \Pi(m)$, but the part u_a, $a \in \Pi \setminus \Pi(m)$ are unknown syndromes. On the other hand, among the functions defined on the curve, since X^a, $a \in \mathbf{N}^2 \setminus \Pi$ are linearly dependent on $\{X^b \mid b \in \Pi, o(X^b) \le o(X^a)\}$, the subarray u_a, $a \in 2\Pi(m)$ also is known, where $2\Pi(m) := \{a + b \mid a, b \in \Pi(m), o(X^{a+b}) \le m\}$. In the linear recurrence $f \circ u = 0$, i.e.

$$\sum_{a \in \mathrm{supp}(f)} c(f, a) u_{a+b} = 0,\ b \in \Pi,$$

not only the components u_a, $a \in \Pi(m)$ but also the components u_a, $a \in 2\Pi(m) \setminus \Pi(m)$ are concerned. Therefore, all the components u_a, $a \in 2\Pi(m)$ are necessary for decoding by using the BMS algorithm. Furthermore, treating only the known syndrome is not enough for decoding of this kind of codes up to half of the designed distance, which we will discuss below.

There have been several investigations on *designed distances* or *lower bounds for minimum distances* of codes from curves. We consider the Feng–Rao (1993) bound of dual Hermitian codes, which is equal to the so-called order bound (Høholdt et al. 1998; Geil 2009) as well as to the Goppa bound $d_G^{\perp}$ in case of $2g - 1 \le m < n$ for these codes. Although the Feng–Rao decoding algorithm based on Gaussian elimination and majority logic can decode up to $t_G^{\perp} = \lfloor \frac{d_G^{\perp} - 1}{2} \rfloor$ errors, it will turn out that the BMS algorithm with majority logic can do the same more efficiently (Sakata et al. 1995a). By using the BMS algorithm w.r.t. the term ordering corresponding to the pole order $o(X^a)$ as mentioned in the next paragraph, we can determine the unknown syndromes based on majority logic in its unique (basically, similar to the Feng–Rao algorithm) fashion so that we can find a minimal polynomial set of the array u which is a Gröbner basis of the error locator ideal $\mathbf{I}(\mathbf{e})$.

Let $\mathcal{O}$ be the set of pole orders $o(f)$ of functions f on the algebraic curve $\mathcal{X}$ over the closed extension (closure) $\tilde{\mathbb{F}}_{q_1} := \bigcup_{i \ge 1} \mathbb{F}_{q_1^i}$ of $\mathbb{F}_{q_1}$, and $\mathcal{O}(m) := \{l \in \mathcal{O} \mid l \le m\}$. Particularly, we denote the pole order $o(X^a)$ of the coordinate function X^a simply as $o(a)$, $a \in \mathbf{N}^2$, which determines the term ordering $<$ together with a certain lexicographic ordering $<_L$. Then, via $o(a)$, $a \in \mathbf{N}^2$, $\mathcal{O}$ and $\mathcal{O}(m)$ one-to-one correspond to Π and $\Pi(m)$, respectively. For $l \in \mathcal{O}$,

$$\nu(l) := \#\{(i, j) \in \mathcal{O}^2 \mid i + j = l\}$$

is introduced and the order bound of the code $C^{\perp}(m)$ is defined as

$$d(m) := \min\{\nu(l) \mid l \geq m+1\}.$$

On the other hand we sometimes have a couple of points $r \in \Pi$ and $r' = r \oplus 1$ (i.e. the next point after r w.r.t. the term ordering $<$) $\in 2\Pi \setminus \Pi$ s.t. $o(r) = o(r')$, and thus, $X^{r'} - X^{r} = \sum_{a:\, o(a)<o(r)} c_a X^a \bmod \mathbf{M}_{\mathcal{X}}$ and so it holds that the value $u_{r'}$ is determined from u_r via the values u_a, $a \in \Pi$ s.t. $o(a) < o(r)$, and vice versa, where r and r' are called *conjugate* to each other. We consider subsets $\Gamma_r := \{a \leq_P r \mid a \in \mathbf{N}^2\}$ and $\Gamma_{r'} := \{a \leq_P r' \mid a \in \mathbf{N}^2\}$. In our terminology, we have that if $o(r) = o(r') = l \in \mathcal{O}$,

$$\nu(l) = \#(\Gamma_r \cup \Gamma_{r'}) \cap \Pi,$$

where if such a couple does not exist, $\Gamma_r \cup \Gamma_{r'}$ should be regarded simply as Γ_r for r s.t. $o(r) = l$.

As we show below, in case of $t_G^{\perp}$ or less errors, we can find iteratively at each $a \in 2\Pi \setminus 2\Pi(m)$ the value of the unknown syndrome u_a and update a pair of minimal polynomial set F and auxiliary polynomial set G by using the modified BMS algorithm with majority voting among the candidate syndrome values, where a pair of conjugate points are treated simultaneously at each BMS iteration, i.e. F and G are updated at each pole order l s.t. $o(r) = o(r') = l$. Thus, we consider the syndrome subarray $u(l) := u^{r'}$ s.t. $o(r') = o(r) = l$, where $r' = r \oplus 1 \in 2\Pi \setminus \Pi$ (if it exists), for each $l > m$. First we remark that $\nu(l) > 2t_G$, $l \geq m+1$. From the known syndromes u_a, $a \in \Pi(m)$, we can get a minimal polynomial set F of the subarray $u(m) = (u_a)$, $a \in 2\Pi(m)$. Now, assume that we have got already the syndrome subarray $u(l)$ for some $l \geq m$ together with F and G of $u(l)$, which is accompanied with the stable subsets $\Sigma(F)$, $\Delta(F)$, and $\Delta(G)$ (see Sakata 2009). We stipulate the following as the *total number of votes* at l

$$v(l) := \#((\Gamma_r \cup \Gamma_{r'}) \cap \Pi \cap \Sigma(F)) \setminus ((r - \Delta(G)) \cup (r' - \Delta(G))),$$

where $r - \Delta(G) := \{r - a \in \Pi \mid a \in \Delta(G)\}$. Furthermore, for a subset $\bar{F} \subset F$ at l, we stipulate the following as the *number of votes for* $\bar{F}$ or *for the candidate values of the unknown syndromes determined by using* $f \in \bar{F}$ at l

$$v(\bar{F}) := \#((\Gamma_r \cup \Gamma_{r'}) \cap \Pi \cap \Sigma(\bar{F})) \setminus ((r - \Delta(G)) \cup (r' - \Delta(G))).$$

From the nature of iteration of BMS algorithm, we have the following:

Lemma 3 *If we have a minimal polynomial set $F^{\oplus}$ of $u(l+1)$ by updating F at the iteration at l, the difference $\#\Delta(F^{\oplus}) - \#\Delta(F)$ is identical with the number of votes for $F_{\text{fail}} := \{f \in F \mid f[u]_r \neq 0 \vee f[u]_{r'} \neq 0\}$ for the pair of conjugate points r and r' at l.*

Then, we have the following conclusion, which assures the validity of the BMS algorithm with majority voting for finding the correct values of the unknown syndrome in case of correctable number of errors.

Lemma 4 *Provided the number of errors is $t' \le t_G^{\perp}$, the polynomials f in F which give the correct syndrome values u_r or $u_{r'}$ have the majority of votes among F.*

Proof It is shown that $\#((r - \Delta(G)) \cup (r' - \Delta(G))) \cap \Pi = \#\Delta(G)$, and thus if the subset F_{fail} of f which does not give the correct syndrome values u_r or $u_{r'}$ at l has the majority of votes, in view of Lemma 3 and $\#\Delta(F) \setminus \Delta = \#\Delta(G)$, we should have $\#\Delta(F^{\oplus}) \setminus \Delta > \#\Delta(F) \setminus \Delta + \frac{1}{2}v(l) = \#\Delta(F) \setminus \Delta + \frac{1}{2}(2t_G^{\perp} - \#\Delta(F) \setminus \Delta - \#\Delta(G)) = t_G^{\perp}$, which contradicts the fact that for the eventual minimal polynomial set F and auxiliary polynomial set G, we have $\#\Delta(F) \setminus \Delta (= \#\Delta(G)) = t'$, where $t' = \#\mathcal{E}$ for the zero variety $V(\mathbf{M}(\mathbf{e})) = \mathcal{E}$ of the error locator submodule $\mathbf{M}(\mathbf{e})$. □

Our syndrome decoding method for Hermitian codes of codelength n has computational complexity $\mathcal{O}(n^{\frac{7}{3}})$ compared with $\mathcal{O}(n^3)$ of the method based on Gaussian elimination. This method can be applied to not only any one-point codes from algebraic curves but also codes from order domains (Høholdt et al. 1998; Geil 2009) at lease when the transcendence degree is one.

3 Multivariate Polynomial Interpolation and List Decoding of Primal Codes

A univariate polynomial interpolation is given by the well-known *Lagrange interpolating polynomial*, i.e. given a set of M points $\{(x^{(l)}, y^{(l)}) \in \mathbb{F}_q^2 \mid 1 \le l \le M\}$ in the 2-D space $\mathbb{F}_q^2$, where $x^{(j)} \ne x^{(l)}$, $j \ne l$, $1 \le j, l \le M$, a polynomial with minimum degree satisfying the interpolation condition $f(x^{(l)}) = y^{(l)}$, $1 \le l \le M$ is

$$f(x) = \sum_{l=1}^{M} y_l \frac{\prod_{j \ne l}(x - x^{(j)})}{\prod_{j \ne l}(x^{(l)} - x^{(j)})}.$$

We can consider any field, provided exact computation without numerical errors is done. However, we restrict to finite fields $\mathbb{F}_q$ with sufficiently large q to concern ourselves with decoding of algebraic geometry codes and to make our discussions simpler.

In the general case of multivariate interpolation, we cannot always have such an explicit interpolating polynomial as above. This is the following problem. Given a set of M points $\{(X^{(l)}, y^{(l)}) \in (\mathbb{F}_q)^{N+1} \mid 1 \le l \le M\}$ in the $(N+1)$-dimensional space $\mathbb{F}_q^{N+1}$ over $\mathbb{F}_q$, where $X^{(l)} = (x_1^{(l)}, \ldots, x_N^{(l)}) \in \mathbb{F}_q^N$, $y^{(l)} \in \mathbb{F}_q$, $1 \le l \le M$ and we assume $X^{(j)} \ne X^{(l)}$, $j \ne l$, $1 \le j, l \le M$, we want to find a N-variate polynomial f, which is *simplest* in some sense, satisfying the following condition:

$$f(X^{(l)}) = y^{(l)}, \quad 1 \le l \le M. \tag{2}$$

Since this is a system of linear equations for the unknown coefficients of f, its solution is not always unique (if it exists), which is given as a sum of a (special) solution of (2) and a general solution f of the following homogeneous system which is derived from (2) by putting $y^{(l)} = 0$, $1 \le l \le M$:

$$f(X^{(l)}) = 0, \quad X^{(l)} \in V, \tag{3}$$

where $V := \{X^{(l)} \mid 1 \le l \le M\} \subset \mathbb{F}_q^N$. The set of solutions f of (3)

$$\mathbf{I}(V) := \{f \in \mathcal{P} \mid f(X^{(l)}) = 0, \quad X^{(l)} \in V\}$$

is an ideal of the ring $\mathcal{P} = \mathbb{F}_q[x_1, \dots, x_N]$. Thus, provided 'simplicity' is interpreted as 'minimality' as in Gröbner basis theory, the interpolation problem (2) can be divided into two subproblems, i.e. finding a Gröbner basis of the ideal corresponding to the homogeneous system (3) and obtaining a special (*minimal*) solution of the non-homogeneous system (2).

Now, for the arrays $u^{(l)} = (u_a^{(l)})$, $v^{(l)} = (v_a^{(l)})$, $a \in \mathbf{N}^N$, $1 \le l \le M$ and $u = (u_a)$, $v = (v_a)$, $a \in \mathbf{N}^N$ defined by

$$\begin{aligned} u_a^{(l)} &:= (X^{(l)})^a, \qquad v_a^{(l)} := y^{(l)}(X^{(l)})^a, \quad a \in \mathbf{N}^N, \ 1 \le l \le M; \\ u_a &:= \sum_{1 \le l \le M} u_a^{(l)}, \qquad v_a := \sum_{1 \le l \le M} v_a^{(l)}, \quad a \in \mathbf{N}^N, \end{aligned}$$

it holds that

Lemma 5 *A polynomial $f = \sum_{a \in \mathrm{supp}(f)} c(f,a)X^a$ satisfies the interpolation condition (2) iff $f \circ u = v$, i.e.*

$$f\langle u \rangle_b =: \sum_{a \in \mathrm{supp}(f)} c(f,a) u_{a+b} = v_b, \quad b \in \mathbf{N}^N. \tag{4}$$

Proof

$$\begin{aligned} &\sum_{a \in \mathrm{supp}(f)} c(f,a)(X^{(l)})^a = y^{(l)}, \quad 1 \le l \le M \quad \Leftrightarrow \\ &\sum_{a \in \mathrm{supp}(f)} c(f,a)(X^{(l)})^{a+b} = y^{(l)}(X^{(l)})^b, \quad b \in \mathbf{N}^N, \ 1 \le l \le M \quad \Leftrightarrow \\ &\sum_{a \in \mathrm{supp}(f)} c(f,a)u_{a+b}^{(l)} = v_b^{(l)}, \quad b \in \mathbf{N}^N, \ 1 \le l \le M \quad \Leftrightarrow \\ &\sum_{a \in \mathrm{supp}(f)} c(f,a)u_{a+b} = v_b, \quad b \in \mathbf{N}^N, \end{aligned}$$

where the equivalence between the third and fourth conditions comes from the linear independence of the arrays $u^{(l)}$, $1 \le l \le M$ (Remark: we assume that q is sufficiently large). □

The linear recurrence corresponding to the homogeneous system (3) is just the homogeneous linear recurrence which is derived from (4) by letting the right-hand array $v := 0$, and it is easy to see that the characteristic ideal $\mathbf{I}(u)$ of the left-hand array u is identical with $\mathbf{I}(V)$.

Such a multivariate interpolation problem as above appears in the context of *list decoding* (Sudan 1997; Shokrollahi and Wasserman 1999; Guruswami and Sudan 1999), which is a generalization of conventional *bounded-distance decoding* (including syndrome decoding) of algebraic geometry codes. First, we give a simple sketch of list decoding of (primal) RS codes. We take a primal $(n = q - 1, k, d = q - k)$ RS code $C = \{\mathbf{c} = (f(\alpha^i))_{0\le i\le n-1} \mid f \in \mathbb{F}_q[x], \deg(f) \le k-1\}$ and an integer $\tau (< n)$ which is more than the number of correctable errors $t = \lfloor \frac{n-k}{2} \rfloor$. Given a received word $\mathbf{r} = (r_j)_{0\le j\le n-1} \in \mathbb{F}_q^n$, we want to find all the codewords $\mathbf{c} = (c_j)_{0\le j\le n-1} \in C$ whose components differ from $\mathbf{r}$ by at most τ components, i.e. for $\mathbf{r} = \mathbf{c} + \mathbf{e}$ with $\mathbf{e} = (e_j)_{0\le j\le n-1} \in \mathbb{F}_q^n$, we assume that the size $t' := \#\mathcal{E}$ of the error locators $\mathcal{E} = \{\alpha^j \mid e_j \ne 0, 0 \le j \le n-1\}$ is less than or equal to τ. Then, it is shown below that list decoding is reduced to an interpolation problem, where the *leading exponent* $\mathrm{le}(Q)(\in \mathbf{N}^2)$ of a bivariate polynomial $Q = Q(x, y)$ is introduced according to the term ordering $<$ defined by the weight $w = (1, k-1)$ (and the lexicographic ordering $<_L$ s.t. $x <_L y$).

Lemma 6 *Assume that a nonzero bivariate polynomial $Q(x, y)$ in $\mathbb{F}_q[x, y]$, $Q(x, y) = \sum_{(i,j)\in \mathrm{supp}(Q)} Q_{ij} x^i y^i$, satisfies the condition*

$$Q(\alpha^j, r_j) = 0, \quad 0 \le j \le n-1 \tag{5}$$

and that its leading exponent $\mathrm{le}(Q) < (n - \tau, 0)$. *Then, the polynomial f corresponding to a codeword* $\mathbf{c}$ *within the radius τ from the received word* $\mathbf{r}$ *satisfies* $y - f(x) \mid Q(x, y)$.

Proof By the condition $\mathrm{le}(Q) < (n - \tau, 0)$, the univariate polynomial $Q(x, f(x))$ has degree at most $n - \tau - 1$. On the other hand, since the identities $r_l = f(\alpha^l)$ hold except for at most τ integers l, $1 \le l \le n$, we have that $Q(\alpha^l, f(\alpha^l)) = 0$ for al least $n - \tau$ integers l, from which it follows that $Q(x, f(x)) = 0$ identically. Thus, $y - f(x) \mid Q(x, y)$ as univariate polynomials over the polynomial ring $\mathbb{F}_q[x]$. □

Therefore, by finding $Q(x, y)$ satisfying the interpolation condition (5) and furthermore finding its factors in the form of $y - f(x)$, we can obtain f which gives a candidate codeword. The 2-D linear recurrence derived from (5) is a special case of the homogeneous linear recurrence (4), where the right-hand side is 0. As a conclusion, we can obtain Q among a Gröbner basis of the characteristic ideal of the 2-D array $u = (u_a)$ defined by $u_a := \sum_{0\le j\le n-1} (X^{(j)})^a$, $a \in \mathbf{N}^2$ for $X^{(j)} = (\alpha^j, r_j)$, $0 \le j \le n-1$. Our method of finding the interpolation polynomial for list decoding of RS codes of codelength n and coding rate $\frac{k}{n} = R$ has computational complexity $\mathcal{O}(R^{-\frac{1}{2}} n^2)$, which is $\mathcal{O}(n^2)$ if the coding rate R is fixed as a constant when both values n and k become asymptotically larger, compared with $\mathcal{O}(n^3)$ of the method based simply on Gaussian elimination.

We do not discuss the existence condition of such an interpolation polynomial as above, although it is related with a practically important problem of how much list decoding can contribute to improvement of reliability in transmission. If it exists, it is the most convenient to have an interpolation polynomial Q with minimal leading exponent $\mathrm{le}(Q)$.

List decoding of codes from curves also is reduced to an interpolation problem. For simplicity, we consider only primal Hermitian codes $C := \{\mathbf{c} = (f(P_j))_{0\le j\le n-1} \mid f \in L(mP_\infty)(= \mathbb{F}_q[\Pi(m)])\}$. In this case, the *leading exponent* of a tri-variate polynomial $Q(x, y, z)$ with support $\mathrm{supp}(Q)$ $(\subset \Pi(m) \times \mathbf{N})$ is introduced over $\Pi(m) \times \mathbf{N}$ according to the term ordering $<$ defined by the weight $w = (q_1, q_1 + 1, m)$ (and the lexicographic ordering $<_L$ s.t. $x <_L y <_L z$). Then, we have:

Lemma 7 *We assume that a nonzero polynomial* (*or rather function*) $Q(P, z) = Q(x, y, z) = \sum_{(a,l)\in\mathrm{supp}(Q)} q_{a,l} P^a z^l$ $(\in \mathbb{F}_q[\Pi(m)][z])$ *satisfies the condition*

$$Q(P_j, r_j) = 0, \quad 0 \le j \le n-1 \tag{6}$$

and has leading exponent $\mathrm{le}(Q) < (\lfloor \frac{n-\tau}{q_1} \rfloor, 0, 0)$, *where the components of* $P = (x, y)$ *are viewed not only as the coordinates of* P *but also as functions on the curve* $\mathcal{X}$. *Then, the function* $f(x, y) \in \Pi(m)$ *corresponding to a codeword* $\mathbf{c}$ *within the radius* τ *from the received word* $\mathbf{r}$ *satisfies* $z - f(x, y) \mid Q(x, y, z)$.

Proof Since $\mathrm{le}(Q) < (\lfloor \frac{n-\tau}{q_1} \rfloor, 0, 0)$, the algebraic function $Q(x, y, f(x, y))$ has pole order less than $n - \tau$ (at the pole P_∞). On the other hand, since $r_j = f(P_j)$ except for at most τ integers j, we have that $Q(P_j, f(P_j)) = 0$ for at least $n - \tau$ integers j, from which it follows that $Q(P, f(P))$ has the total zero order of $n - \tau$ or more. Since it does not have any other pole except for P_∞, we have that $Q(P, f(P)) = 0$ identically, which implies that $z - f(x, y) \mid Q(x, y, z)$ when $Q(x, y, z) = Q(P, z)$ is viewed as a univariate polynomial w.r.t. the main variable z over the ring $\mathbb{F}_q[\Pi]$. $\square$

Also in this situation, the interpolation condition (6) is reduced to a homogeneous linear recurrence. Consequently, we can obtain Q among a Gröbner basis of the characteristic ideal of the 3-D array $u = (u_a)$ defined by $u_a := \sum_{0\le j\le n-1} (X^{(j)})^a$, $a \in \mathbf{N}^3$ for $X^{(j)} = (P_j, r_j)$, $0 \le j \le n-1$.

From the viewpoint of linear algebra, the linear recurrence (4) is nothing but a system of linear equations for unknowns $c(f, a)$, $a \in \mathrm{supp}(f)$. Particularly, in the 2-D case, it is just a 2-D block-Hankel or 2-D block-Toeplitz system of linear equations, where the extent $\mathrm{supp}(f)$ of a solution f is also unknown in our situation, distinctly from solving the ordinary system of linear equations. For the purpose of multivariate interpolation or decoding of codes, our method is unique and distinct from the known fast methods of solving block-Hankel systems or other interpolation methods.

Soon after Sudan (1997) proposed his list decoding method, Guruswami and Sudan (1999) gave an improvement called the *GS list decoding* method, which can be effective even for higher coding rate, while the original Sudan list decoding works only for coding rate $\leq\frac{1}{3}$. It is based on the notion of *zeros with multiplicity* defined as follows. Here we consider RS codes as in Lemma 6 for simplicity. A point $X^{(l)} = (x^{(l)}, y^{(l)}) \in (\mathbb{F}_q)^2$ is called a *zero with multiplicity* s *or more* of a polynomial $Q(x, y) = \sum_{(i,j)\in\mathrm{supp}(Q)} Q_{ij}x^i y^i = \sum_{a\in\mathrm{supp}(Q)} c(Q, a)X^a \in \mathbb{F}_q[x, y]$ iff in the expansion

$$Q^{(l)}(x, y) = \sum_{a\in\mathbf{N}^2} c(Q^{(l)}, a)X^a \tag{7}$$

of the polynomial $Q^{(l)}(x, y) := Q(x + x^{(l)}, y + y^{(l)})$, all the terms $c(Q^{(l)}, a)X^a$ vanish, i.e. $c(Q^{(l)}, a) = 0$, for $\forall a = (a_1, a_2) \in \mathbf{N}^2$ s.t. $a_1 + a_2 < s$. Then, we have a modification of Lemma 6:

Lemma 8 *Assume that a nonzero bivariate polynomial* $Q(x, y) = \sum_{(i,j)\in\mathrm{supp}(Q)} Q_{ij}x^i y^i$ $(\in \mathbb{F}_q[x, y])$ *has zeros* (α^j, r_j), $0 \leq j \leq n-1$, *each with multiplicity* s *or more and that it has* $\deg(Q) <_T (s(n-\tau), 0)$. *Then, the polynomial* f *corresponding to a codeword within the radius* τ *from* $\mathbf{r}$ *satisfies* $y - f(x) \mid Q(x, y)$.

Neglecting discussions on the error correction performance of GS list decoding, we will show that one can apply the BMS algorithm to find such an interpolation polynomial with minimal degree. First we remark the following facts.

Lemma 9 *For a finite subset* $V = \{X^{(l)} = (x^{(l)}, y^{(l)}) \mid 0 \leq l \leq n-1\} \subset \mathbb{F}_q^2$, *any integer* s, *and any point* $c \in \mathbf{N}^2$, *each of the following sets is an ideal of* $\mathbb{F}_q[x, y]$, *the former of which we call the ideal of the zero variety* V *with multiplicity* s.

$$\begin{aligned}\mathbf{I}(V; s) &:= \{Q(x, y) \in \mathbb{F}_q[x, y] \mid c(Q^{(l)}, a) = 0, a = (a_1.a_2) \in \mathbf{N}^2,\\ &\qquad a_1 + a_2 < s, 0 \leq l \leq n-1\},\\ \mathbf{I}(V; c) &:= \{Q(x, y) \in \mathbb{F}_q[x, y] \mid c(Q^{(l)}, a) = 0, a = (a_1.a_2) \in \mathbf{N}^2,\\ &\qquad a \leq_P c, 0 \leq l \leq n-1\}.\end{aligned}$$

Next, for two points $a = (a_1, a_2)$, $b = (b_1, b_2) \in \mathbf{N}^2$, we introduce the 2-D binomial coefficients

$$\binom{b}{a} := \binom{b_1}{a_1}\binom{b_2}{a_2},$$

where if it does not hold that $a \leq_P b$, $\binom{b}{a} = 0$. Then, the coefficients $c(Q^{(l)}, a)$ of the expansion of (7) are written as

$$c(Q^{(l)}, a) = \sum_{b\in\mathrm{supp}(Q):\, b\geq_P a} \binom{b}{a} c(Q, b)(X^{(l)})^{b-a}.$$

Therefore,

Lemma 10 $Q = \sum_{a \in \mathrm{supp}(Q)} c(Q,a)X^a \in \mathbf{I}(V,c) \Leftrightarrow$

$$\sum_{b \in \mathrm{supp}(Q): b \geq_P a} \binom{b}{a} c(Q,b)(X^{(l)})^{b-a} = 0, \quad a \in \Gamma_c,\ 0 \leq l \leq n-1.$$

For a point $c \in \mathbf{N}^2$, we introduce a 2-D array $u = (u_b)$ as follows:

$$u_b := \sum_{0 \leq l \leq n-1} \binom{b}{c} (X^{(l)})^{b-c}, \quad b \in \mathbf{N}^2.$$

Then,

Lemma 11 $Q = \sum_{a \in \mathrm{supp}(Q)} c(Q,a)X^a \in \mathbf{I}(V,c) \Leftrightarrow Q \circ u = 0$, *i.e.*

$$\sum_{a \in \mathrm{supp}(Q)} c(Q,a)u_{a+b} = 0, \quad b \in \mathbf{N}^2.$$

For the ideal $\mathbf{I}(V,s)$, we introduce s 2-D arrays $u^{(i)} = (u_b^{(i)})$, $1 \leq i \leq s$ as follows:

$$u_b^{(i)} := \sum_{0 \leq l \leq n-1} \binom{b}{c^{(i)}} (X^{(l)})^{b-c^{(i)}}, \quad b \in \mathbf{N}^2, \tag{8}$$

where $c^{(i)} := (i-1, s-i) \in \mathbf{N}^2$, $1 \leq i \leq s$. Then, in view of $\{a = (a_1, a_2) \in \mathbf{N}^2 \mid a_1 + a_2 < s\} = \cup_{1 \leq i \leq s} \Gamma_{c^{(i)}}$, we have

Corollary 1 $Q \in \mathbf{I}(V,s) \Leftrightarrow Q \circ u^{(i)} = 0$, $1 \leq i \leq s$, *i.e.*

$$\sum_{a \in \mathrm{supp}(Q)} c(Q,a)u_{a+b}^{(i)} = 0, \quad b \in \mathbf{N}^2,\ 1 \leq i \leq s.$$

Consequently, it turns out that GS list decoding of primal RS codes can be solved by the multiple-array BMS algorithm (Sakata 1989), which is a modification of the BMS algorithm for finding a minimal polynomial set of a finite set of 2-D arrays $u^{(i)}$, $1 \leq i \leq s$ as in (8) with $X^{(l)} = (\alpha^l, r_l) \in \mathbb{F}_q^2$, $0 \leq l \leq n-1$.

Compared with $\mathcal{O}(n^3 s^6)$ of the method based simply on Gaussian elimination, our method (Numakami et al. 2000) of finding the interpolation function for GS list decoding with multiplicity s of RS codes of codelength n and coding rate R has the same computational complexity $\mathcal{O}(R^{-\frac{1}{2}} n^2 s^4)$ as other efficient algorithms, e.g. Koetter–Vardy (2003), O'Kieffe–Fitzpatrick (2002), Lee–O'Sullivan (2006), but our method is unique in the sense that it uses (syndrome-like) arrays which contain in the condensed form all the information necessary for decoding. For GS list decoding of algebraic geometry codes, there have been several approaches (Sakata 2001; O'Keeffe and Fitzpatrick 2007; Lee and O'Sullivan 2008), etc., which we do not treat here because we need more involved discussions for that purpose. For general multivariate interpolation the Buchberger–Möller (1982, 2009a) and the Marinani–Möller–Mora (1993) algorithm are alternatives, in comparison with which the BMS algorithm is conjectured to have less computational complexity, depending on the situations, although the exact estimations remain to be investigated.

4 Other Relevant Decoding Methods of Primal/Dual Codes

In this section, we consider a special case of Sudan list decoding, i.e. the case of list size 1. In this case, we treat nothing but polynomials of degree 1 w.r.t. the main variable and bounded-distance decoding of primal codes up to half the correction bound.[3]

Again we take a primal $(n = q - 1, k, d = q - k)$ RS code, and we assume that the number τ of errors is less than $\frac{d}{2}$ as in Sect. 2. As a corollary of Lemma 6, we have

Lemma 12[4] *If a bivariate polynomial of the form*

$$Q(x, y) = Q_0(x) - yQ_1(x) \quad (\neq 0) \quad (\in \mathbb{F}_q[x, y])$$

satisfies the conditions

$$\begin{aligned} &(1) \quad \deg(Q_0(x)) < n - \tau,\ \deg(Q_1(x)) < n - \tau - (k - 1); \\ &(2) \quad Q(\alpha^j, r_j) = 0, \quad 0 \le j \le n - 1, \end{aligned} \tag{9}$$

then $Q_1(x)$ is an error locator polynomial which has $\mathcal{E}$ as its zeros, i.e. $Q_1(\alpha^j) = 0$ for $\alpha^j \in \mathcal{E}$, and $Q_1(x) \mid Q_0(x)$ so that the quotient $f(x) = \frac{Q_0(x)}{Q_1(x)}$ is the message polynomial corresponding to the sent codeword $\mathbf{c} = (c_j)$, i.e. $c_j = f(\alpha^j)$.

In fact, such a polynomial $Q(x, y)$ exists as shown in the following lemma so that we can obtain it by applying the BMS algorithm to the 2-D array $u = (u_a)$ defined by $u_a := \sum_{0 \le j \le n-1} (X^{(j)})^a$, $a \in \mathbf{N}^2$ for $X^{(j)} = (\alpha^j, r_j)$, $0 \le j \le n - 1$ similarly to list decoding, where in this case we do not need to be worried about factorization of $Q(x, y)$.

[3] Of course, a primal code can be decoded as a dual code of its dual by using syndrome decoding. But, sometimes from both the practical and theoretical points of view it is required to have some direct decoding method as a primal code itself.

[4] This lemma is given in Justesen and Høholdt (2004).

Lemma 13 *There exists at least one nonzero polynomial $Q(x, y)$ as in Lemma 12.*

Sine we assume that τ is less than or equal to the number of correctable errors $t = \lfloor \frac{d-1}{2} \rfloor$, there exists only a single codeword $\mathbf{c}$ s.t. $\mathrm{dis}(\mathbf{c}, \mathbf{r}) \le \tau$ and thus the above method gives us the ordinary bounded-distance decoding of primal RS codes. By the way, the above method based on the 2-D BMS algorithm can be replaced by the vectorial BM algorithm, which is the 1-D vectorial BMS algorithm. First, we take n pairs of 1-D arrays $v^{(j)} = (v_i^{(j)})$, $w^{(j)} = (w_i^{(j)})$, $i \in \mathbf{N}$, $0 \le j \le n-1$ defined by

$$v_i^{(j)} := (\alpha^j)^i, \qquad w_i^{(j)} := -r_j(\alpha^j)^i, \quad i \in \mathbf{N},$$

from which we have a pair of 1-D arrays $v = (v_i)$, $w = (w_i)$ defined by

$$v_i := \sum_{j=1}^{n} v_i^{(j)}, \qquad w_i := \sum_{j=1}^{n} w_i^{(j)}, \quad i \in \mathbf{N}.$$

Then, we have

Lemma 14 *The condition (9) is equivalent to the compound linear recurrence*

$$\sum_{i=0}^{d_0} c(Q_0, i) v_{i+j} + \sum_{i=0}^{d_1} c(Q_1, i) w_{i+j} = 0, \quad j \in \mathbf{N}. \tag{10}$$

Thus, we can apply the vectorial BM algorithm (Sakata 1991, 2009) to the pair (v, w) of 1-D arrays so that we can have a Gröbner basis of the module defined by the pair of arrays as a minimal polynomial vector set, in which the desired solution (Q_0, Q_1) is contained. Thus, we have another method of the ordinary bounded-distance decoding of primal RS codes.[5] In form, this method is similar to the decoding method (Sakata 2006) based on the vectorial BM algorithm which we gave as an alternative to the Welch–Berlekamp (1986) decoding algorithm of the dual RS code, where we have instead of the condition (9)

$$Q\left(\alpha^j, \frac{r_j}{p_j \alpha^j}\right) = 0, \quad 0 \le j \le d-2, \tag{11}$$

where p_j, $0 \le j \le d-2$ are defined by

$$p(x) = \prod_{i=1}^{d-2} (x - \alpha^i) = \sum_{j=0}^{d-2} p_j x^j. \tag{12}$$

[5]The vectorial BMS algorithm (Sakata 1991, 2009) for any dimension N is given in 1991. Fitzpatrick (1995) gave a similar method, which may be considered to be equivalent to a version of the vectorial BM algorithm according to Blackburn–Chambers' (1996) explanation, where the swapping based on the special term ordering $<_r$ used in the Fitzpatrick algorithm corresponds to the degree change in the (vectorial) BM algorithm.

For the primal Hermitian code $C(m)$ we have a corollary of Lemma 7.

Lemma 15 *If a trivariate polynomial*

$$Q(x,y,z) = Q_0(x,y) - zQ_1(x,y) \in \mathbb{F}_q[\Pi(m)][z]$$

satisfies the conditions

$$\begin{aligned} &(1) \quad o(Q_0) \le m + \tau + g, \quad o(Q_1) \le \tau + g; \\ &(2) \quad Q(x_l, y_l, r_l) = 0, \quad 0 \le l \le n-1, \end{aligned} \tag{13}$$

then $Q_1(x,y)$ is an error locator function which has $\mathcal{E}$ as its zeros, i.e. $Q_1(P_j) = 0$ for $P_j \in \mathcal{E}$, and $Q_1(x,y) \mid Q_0(x,y)$ so that the quotient $f(x,y) := \frac{Q_0(x,y)}{Q_1(x,y)}$ is the message function corresponding to the sent codeword $\mathbf{c}$, *i.e. $c_j = f(P_j)$, $0 \le j \le n-1$.*

In fact, such a function $Q(x,y,z)$ exists as shown in the following lemma so that we can obtain it by applying the 3-D BMS algorithm to the 3-D array $u = (u_a)$ defined by $u_a := \sum_{0 \le j \le n-1} (X^{(j)})^a$, $a \in \mathbf{N}^3$ for $X^{(j)} = (P_j, r_j)$, $0 \le j \le n-1$ similarly to the list decoding, where in this case we do not need to be worried about factorization of $Q(x,y,z)$.

Lemma 16 *There exists at least one nonzero function $Q(x,y,z)$ as in Lemma 15.*

If τ is less than or equal to $\hat{t} = \lfloor \frac{d_G - g - 1}{2} \rfloor$ $(< t_G)$, then there exists only a single codeword $\mathbf{c}$ s.t. $\mathrm{dis}(\mathbf{c}, \mathbf{r}) \le \tau$ and thus this method (Fujisawa and Sakata 2005) gives us the ordinary bounded-distance decoding of primal Hermitian codes up to $\hat{t}$. By the way, the method based on the 3-D BMS algorithm can be replaced by the vectorial 2-D BMS algorithm. Instead of the 3D array u as above, we take a pair of 2D arrays $v = (v_a)$, $w = (w_a)$, $a = (a_1, a_2) \in \Pi$ defined by

$$v_a := \sum_{0 \le l \le n-1} P_l^a = \sum_{0 \le l \le n-1} (\alpha_l)^{a_1} (\beta_l)^{a_2}, \tag{14}$$

$$w_a := -\sum_{0 \le l \le n-1} r_l P_l^a = -\sum_{0 \le l \le n-1} r_l (\alpha_l)^{a_1} (\beta_l)^{a_2}, \tag{15}$$

for which the following *compound* linear recurrence must hold:

$$\sum_{a \in \mathrm{supp}(g)} c(g,a) v_{a+b} + \sum_{a \in \mathrm{supp}(h)} c(h,a) w_{a+b} = 0, \quad b \in \Pi, \tag{16}$$

where $g (:= Q_0) = \sum_{a \in \mathrm{supp}(g)} c(g,a) X^a$ and $h (:= Q_1) = \sum_{a \in \mathrm{supp}(h)} c(h,a) X^a$. Thus, we can apply the vectorial BMS algorithm to the pair (v, w) of 2-D arrays so that we can have a Gröbner basis of the module defined by the pair of arrays as a minimal polynomial vector set, in which the desired solution $(g, h) = (Q_0, Q_1)$ is contained. Thus, we have another method of the ordinary bounded-distance decoding of primal Hermitian codes up to $\hat{t}$. Furthermore, it is shown in Fujisawa et al. (2006) that most of errors up to half the Goppa bound d_G of the code $C(m)$ over a large finite field $\mathbb{F}_q$ can be corrected by the decoding method, i.e. for $t := \lfloor \frac{d_G-1}{2} \rfloor$, $1 - \frac{1}{q}$ of t or less errors can be corrected.

We should not ignore the fact that the interpolation problems (9), (13) can be solved either by Buchberger–Möller (1982) algorithm or Mariani–Möller–Mora (1993) algorithm, both of which are a general method of multi-variate interpolation problem although our method based on the BMS algorithm discussed above also is a general method of multi-variate interpolation problem, or by the Farr–Gao (2005) algorithm which is explained as a generalization of Newton's interpolation for univariate polynomial. Our method seems to have less computational complexity than them, but the exact comparison remains to be investigated.

Recently a novel decoding algorithm of primal RS codes which is based on higher-dimensional interpolation has been published by Parvaresh and Vardy (2005). Its error correction performance is superior to GS list decoding, where the ratios of the number of correctable errors per the codelength are $\frac{\tau_{PV}}{n} = 1 - R^{\frac{N}{N+1}}$, if $(N+1)$-variate polynomial interpolation is used, for the Parvaresh–Vardy (PV) method and $\frac{\tau_{GS}}{n} = 1 - R^{\frac{1}{2}}$ for GS method, respectively. In fact, GS list decoding is a special case of $N = 1$ of the PV method. In case of $N = 2$, in encoding, the PV method gives not only the codeword of $\mathbf{c} = (c_j) = \mathrm{ev}(f) \in C$ for a message polynomial $f(x) = \sum_{i=0}^{k-1} f_i x^i \in \mathcal{K}[x]$ of the actual RS code C $(\subset \mathcal{K}^n)$ but also another codeword $\mathbf{c}' := \mathrm{ev}(g) \in C$ for $g(x) = (f(x))^a \bmod h(x)$, and then sends the pair of codewords $\mathbf{c}, \mathbf{c}' \in C$, where $h(x) \in \mathcal{K}[x]$ is an irreducible polynomial over $\mathcal{K}$ of degree k, and a is any integer satisfying a special condition. In decoding, given a pair of received words $\mathbf{y} = (y_j), \mathbf{z} = (z_j) \in \mathcal{K}^n$, one tries to find a Gröbner basis of the ideal

$$\mathbf{I}(\mathbf{y}, \mathbf{z}) := \{Q(x, y, z) \in \mathcal{K}[x, y, z] \mid Q(\alpha^j, y_j, z_j) = 0, 0 \le j \le n-1\}$$

w.r.t. the term order defined by the weight $(1, k-1, k-1)$. Then, from the minimum element $Q_m(x, y, z)$ of $\mathbf{I}(\mathbf{y}, \mathbf{z})$ one computes $P(y, z) = Q_m(x, y, z) \bmod h(x)$, interpreted as an element of $\tilde{\mathcal{K}}[y, z]$, where $\tilde{\mathcal{K}} \simeq \mathcal{K}[x]/\langle h(x)\rangle$ is the extension field of $\mathcal{K}$, and obtains the univariate polynomial $\tilde{P}(y) := P(y, y^a) \in \tilde{\mathcal{K}}[y]$, whose roots $\in \tilde{\mathcal{K}}$ can be candidates of the message polynomial $f(x) \in \mathcal{K}[x]$. Thus, the multivariate interpolation, which is a key step of the PV decoding method, can be solved by the BMS algorithm efficiently.

5 Conclusion

We have discussed how the BMS algorithm and its variations (Sakata 1988, 1989, 1990, 1991, 2009) are applied to various decoding methods of algebraic geometry codes and multivariate interpolation related to list decoding, and how these decoding methods are connected with Gröbner bases via multidimensional arrays and linear recurrences. Although we have explained our decoding methods mainly as regards Reed–Solomon codes and Hermitian codes, our methods work for one-point codes from any algebraic curves and codes from order domains. For example, primal and dual one-point codes which have an $\overline{\mathbb{F}}_q(f_\rho)$-module basis (see Sect. 7 of Leonard 2009a) can be decoded by the vectorial BMS algorithm. In the sequel, we have clarified that these problems are reduced to finding a set of minimal polynomials, which corresponds to a Gröbner basis, of a given (set of) multidimensional array(s).[6] We have given a basic set of algorithms for solving these problems, which constitute a unified system of unique methods in comparison with other various relevant methods related to Gröbner bases. In fact, there have been many other pioneering investigations (Justesen et al. 1989, 1992; Pellikaan 1989, 1993; Skorobogatov and Vlăduţ 1990; Porter et al. 1992; Shen 1992; Duursma 1993; Ehrhard 1993; Feng et al. 1994), etc.[7] on decoding algebraic geometry codes, but those are less efficient than our methods based on the Gröbner basis theory (Buchberger 1965, 1970, 1985, 1998, 2006) and the BMS algorithm (Sakata 1988, 1990). In Leonard (2009b), Guerrini and Rimoldi (2009) in this issue, other decoding methods from Gröbner basis perspectives are discussed. For encoding of AG codes, see Little (2009).

Acknowledgements Part of these results have been presented at Linz D1 2006, which was a workshop within the Special Semester on Gröbner Bases, February–July 2006, organized by RICAM, Austrian Academy of Sciences, and RISC, Johannes Kepler University, Linz, Austria.

References

D. Augot, *A parallel version of a special case of the Sudan list decoding algorithm*, Proc. of ISIT2002, 2002, pp. 86–86.

D. Augot, E. Betti, and E. Orsini, *An introduction to linear and cyclic codes*, this volume, 2009, pp. 47–68.

S. R. Blackburn and W. G. Chambers, *Some remarks on an algorithm of Fitzpatrick*, IEEE Trans. on Inf. Th. **42** (1996), no. 4, 1269–1271.

B. Buchberger, *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal*, Ph.D. thesis, Innsbruck, 1965.

B. Buchberger, *Ein algorithmisches Kriterium für die Lösbarkeit eines algebraischen Gleichungssystems*, Aequationes Math. **4** (1970), 374–383.

B. Buchberger, *Gröbner-bases: An algorithmic method in polynomial ideal theory*, Multidimensional systems theory, Reidel, Dordrecht, 1985, pp. 184–232.

B. Buchberger, *An algorithmical criterion for the solvability of algebraic systems of equations*, London Math. Soc. LNS **251** (1998), 535–545.

B. Buchberger, *Bruno Buchberger's PhD thesis 1965: An algorithm for finding the basis elements of the residue class ring of a zero dimensional polynomial ideal*, J. Symb. Comput. **41** (2006), nos. 3–4, 475–511.

[6] These facts are based on the well-known correspondence between ideals and varieties (zeros) (Cox et al. 1992), but a little bit distinct from the duality discussed by Mora (2009a) in this issue.

[7] See Høholdt et al. (1998).

D. Cox, J. Little, and D. O'Shea, *Ideals, varieties, and algorithms*, Springer, Berlin, 1992, An introduction to computational algebraic geometry and commutative algebra.
I. M. Duursma, *Majority coset decoding*, IEEE Trans. on Inf. Th. **39** (1993), no. 3, 1067–1070.
D. Ehrhard, *Achieving the designed error capacity in decoding algebraic-geometric codes*, IEEE Trans. on Inf. Th. **39** (1993), no. 3, 743–751.
J. B. Farr and S. Gao, *Gröbner bases, Padé approximation, and decoding of linear codes*, Contemp. Math. **381** (2005), 3–18.
G. L. Feng and T. R. N. Rao, *Decoding algebraic-geometric codes up to the designed minimum distance*, IEEE Trans. on Inf. Th. **39** (1993), no. 1, 37–45.
G. L. Feng, V. K. Wei, T. R. N. Rao, and K. Tzeng, *Simplified understanding and efficient decoding of algebraic geometric codes*, IEEE Trans. on Inf. Th. **40** (1994), no. 4, 981–1002.
P. Fitzpatrick, *On the key equation*, IEEE Trans. on Inf. Th. **41** (1995), no. 5, 1290–1302.
M. Fujisawa and S. Sakata, *On a fast method of bounded-distance decoding based on Sudan's algorithm for one-point algebraic geometry code*, Proc. of SITA2005, 2005, pp. 543–546.
M. Fujisawa, H. Matsui, M. Kurihara, and S. Sakata, *With a higher probability one can correct error up to the designed distance for primal codes from curves*, Proc. of SITA2006, 2006, pp. 101–104.
O. Geil, *Algebraic geometry codes from order domains*, this volume, 2009, pp. 121–141.
V. D. Goppa, *Codes on algebraic curves*, Soviet Math. Dokl. **24** (1981), no. 1, 170–172.
E. Guerrini and A. Rimoldi, *FGLM-like decoding: from Fitzpatrick's approach to recent developments*, this volume, 2009, pp. 197–218.
V. Guruswami and M. Sudan, *Improved decoding of Reed–Solomon and algebraic geometric codes*, IEEE Trans. on Inf. Th. **45** (1999), no. 6, 1757–1767.
T. Høholdt, J. H. van Lint, and R. Pellikaan, *Algebraic geometry of codes*, Handbook of coding theory, vols. I, II (V. S. Pless and W.C. Huffman, eds.), North-Holland, Amsterdam, 1998, pp. 871–961.
J. Justesen and T. Høholdt, *A course in error-correcting codes*, EMS textbooks in mathematics, EMS, 2004.
J. Justesen, Larsen K. J., Jensen H. E., A. Havemose, and T. Høholdt, *Construction and decoding of a class of algebraic geometry codes*, IEEE Trans. on Inf. Th. **35** (1989), no. 4, 811–821.
J. Justesen, K. J. Larsen, H. E. Jensen, and T. Høholdt, *Fast decoding of codes from algebraic plane curves*, IEEE Trans. on Inf. Th. **38** (1992), no. 1, 111–119.
R. Kötter, *On decoding of algebraic-geometric and cyclic codes*, Ph.D. thesis, Linköping University, 1996.
R. Kötter and A. Vardy, *Algebraic soft-decision decoding of Reed–Solomon codes*, Trans. on Inf. Th. **49** (2003), no. 11, 2809–2825.
K. Lee and M. E. O'Sullivan, *Sudan's list decoding of RS codes from a Gröbner basis perspective*, preprint, 2006, arXiv:math/0601022.
K. Lee and M. E. O'Sullivan, *List decoding of Reed–Solomon codes from a Gröbner basis perspective*, J. Symbolic Comput. **43** (2008), no. 9, 645–658.
D. A. Leonard, *A tutorial on AG code construction from a Gröbner basis perspective*, this volume, 2009a, pp. 93–106.
D. A. Leonard, *A tutorial on AG code decoding from a Gröbner basis perspective*, this volume, 2009b, pp. 187–196.
J. B. Little, *Automorphisms and encoding of AG and order domain codes*, this volume, 2009, pp. 107–120.
M. G. Marinari, H. M. Möller, and T. Mora, *Gröbner bases of ideals defined by functionals with an application to ideals of projective points*, AAECC **4** (1993), no. 2, 103–145.
H. M. Möller and B. Buchberger, *The construction of multivariate polynomials with preassigned zeros*, LNCS, vol. **144**, Springer, Berlin, 1982, pp. 24–31.
T. Mora, *The FGLM problem and Möller's algorithm on zero-dimensional ideals*, this volume, 2009a, pp. 27–45.
T. Mora, *Gröbner technology*, this volume, 2009b, pp. 11–25.
Y. Numakami, M. Fujisawa, and S. Sakata, *Fast interpolation methods for list decoding of RS codes*, IEICE Trans. Fundamentals **J83** (2000), 1309–1317.

H. O'Keeffe and P. Fitzpatrick, *Gröbner bases solutions of constrained interpolation problems*, Linear algebra and its applications **351–352** (2002), 533–551.

H. O'Keeffe and P. Fitzpatrick, *Gröbner basis approach to list decoding of algebraic geometry codes*, AAECC **18** (2007), no. 5, 445–466.

M. E. O'Sullivan, *Decoding of codes defined by a single point on a curve*, IEEE Trans. on Inf. Th. **41** (1995), no. 6, 1709–1719, part 1.

F. Parvaresh and A. Vardy, *Correcting errors beyond the Guruswami–Sudan radius in polynomial time*, Proc. of IEEE FOCS2005, IEEE Computer Society, 2005, pp. 285–294.

R. Pellikaan, *On a decoding algorithm for codes on maximal curves*, IEEE Trans. on Inf. Th. **35** (1989), no. 6, 1228–1232.

R. Pellikaan, *On the efficient decoding of algebraic-geometric codes*, Eurocode '92, CISM courses and lectures, vol. **339**, Springer, Berlin, 1993, pp. 231–253.

S. C. Porter, B. Z. Shen, and R. Pellikaan, *Decoding geometric Goppa codes using an extra place*, IEEE Trans. on Inf. Th. **38** (1992), no. 6, 1663–1676.

K. Saints and C. Heegard, *Algebraic-geometric codes and multidimensional cyclic codes: a unified theory and algorithms for decoding using Gröbner bases*, IEEE Trans. Inform. Theory **41** (1995), no. 6, 1733–1751.

S. Sakata, *Finding a minimal set of linear recurring relations capable of generating a given finite two-dimensional array*, J. Symbolic Comput. **5** (1988), no. 3, 321–337.

S. Sakata, *n-dimensional Berlekamp–Massey algorithm for multiple arrays and construction of multivariate polynomials with preassigned zeros*, LNCS, vol. **357**, Springer, Berlin, 1989, pp. 356–376.

S. Sakata, *Extension of the Berlekamp-Massey algorithm to N dimensions*, Inform. and Comput. **84** (1990), no. 2, 207–239.

S. Sakata, *Finding a minimal polynomial vector set of a vector of nD arrays*, LNCS, vol. **539**, Springer, Berlin, 1991, pp. 414–425.

S. Sakata, *On fast interpolation method for Guruswami–Sudan list decoding of one-point AG codes*, LNCS, vol. **2227**, Springer, Berlin, 2001, pp. 172–181.

S. Sakata, *Efficient factorization methods for list decoding of code from curves*, Proc. of ISIT2003, 2003, pp. 363–363.

S. Sakata, *A comparison between WB algorithm and BM algorithm*, Proc. of ISITA2006, 2006, pp. 244–247.

S. Sakata, *The BMS algorithm*, this volume, 2009, pp. 143–163.

S. Sakata and M. Fujisawa, *WB-like decoding algorithm of one-point codes from curves*, Proc. of SITA2006, 2006, pp. 93–96.

S. Sakata, H. E. Jensen, and T. Høholdt, *Generalized Berlekamp–Massey decoding of algebraic-geometric codes up to half the Feng–Rao bound*, IEEE Trans. on Inf. Th. **41** (1995a), no. 6, 1762–1768, part 1.

S. Sakata, J. Justesen, Y. Madelung, H. E. Jensen, and T. Høholdt, *A fast decoding method of AG codes from Miura–Kamiya curves C_{ab} up to half the Feng–Rao bound*, Finite Fields Appl. **1** (1995b), no. 1, 83–101.

S. Sakata, J. Justesen, Y. Madelung, H. E. Jensen, and T. Høholdt, *Fast decoding of algebraic-geometric codes up to the designed minimum distance*, IEEE Trans. on Inf. Th. **41** (1995c), no. 6, 1672–1677, part 1.

B. Z. Shen, *Algebraic-geometric codes and their decoding algorithm*, Ph.D. thesis, Eindhoven Univ. Tech., 1992.

M. A. Shokrollahi and H. Wasserman, *List decoding of algebraic-geometric codes*, IEEE Trans. on Inf. Th. **45** (1999), no. 2, 432–437.

A. N. Skorobogatov and S. G. Vlăduţ, *On the decoding of algebraic-geometric codes*, IEEE Trans. on Inf. Th. **36** (1990), no. 5, 1051–1060.

H. Stichtenoth, *A note on Hermitian codes over $GF(q^2)$*, IEEE Trans. on Inf. Th. **34** (1988), 1345–1348.

M. Sudan, *Decoding of Reed–Solomon codes beyond the error correction bound*, J. of Complexity **13** (1997), 180–193.

L. R. Welch and E. R. Berlekamp, *Error correction for algebraic block codes*, U.S. Patent No. 4633470, 1986.