Fast Decoding of Algebraic-Geometric Codes up to the Designed Minimum Distance

Shajiro Sakata, *Senior Member, IEEE*, Jørn Justesen, Y. Madelung, Helhe Elbrønd Jensen, and Tom Høholdt, *Member, IEEE*

***Abstract*— We present a decoding algorithm for algebraic-geometric codes from regular plane curves, in particular the Hermitian curve, which corrects all error patternes of weight less than $d^*/2$ with low complexity. The algorithm is based on the majority scheme of Feng and Rao and uses a modified version of Sakata's generalization of the Berlekamp–Massey algorithm.**

***Index Terms*—Decoding, algebraic-geometric codes.**

I. Introduction

THE KNOWN algorithms for decoding codes from algebraic geometry [1]–[4] do not correct all errors with weight up to half the designed distance of the code, even though Pellikaan [5] showed that this could be done.

Recently Ehrhard [6], Feng and Rao [7], and Duursma [8] presented algorithms which correct all error patterns of weight less than $d^*/2$, where d^* is the designed distance of the code. These algorithms are based on Gaussian elimination and hence have complexity $O(n^3)$, where n is the length of the code.

In this paper we used a modified version of the algorithm of Sakata [9] combined with the idea of Feng and Rao, such that for algebraic-geometric codes from regular plane curves, all error patterns of weight less than $d^*/2$ are corrected with low complexity. In particular, we extend the algorithm of [4] such that for a class of codes from algebraic plane curves the complexity of the decoding algorithm is $O(n^{7/3})$.

The paper is organized as follows. In Section II we present the codes from Hermitian curves and discuss the decoding problem for those. Section III describes how Sakata's algorithm can be used to implement the idea of Feng and Rao and Section IV presents the new algorithm. In Section V we discuss the problem for general algebraic-geometric codes.

II. The Decoding Problem for a Class of Plane Curves

Before studying the Hermitian codes we briefly recall the setup from [4].

Manuscript received October 7, 1993. The material in this paper was presented at the 6th Joint Swedish–Russian International Workshop on Information Theory, Mölle, Sweden, Aug. 22–27, 1993.

S. Sakata is with the Department of Computer Science and Information Mathematics, Faculty of Electro-Communications, The University of Electro-Communications, Chofu-ga-oka 151, Chofu-shi, Tokyo 182, Japan.

J. Justesen and Y. Madelung are with the Institute of Circuit Theory and Telecommunication, The Technical University of Denmark, DK-2800 Lyngby, Denmark.

H. E. Jensen and T. Høholdt are with the Mathematical Institute, The Technical University of Denmark, DK-2800 Lyngby, Denmark.

IEEE Log Number 9414218.

Let $\mathbb{F}_q$ be a finite field with q elements and let $C(x, y)$ be a polynomial from $\mathbb{F}_q[x, y]$.

The set of points (x, y), where x and y are in the algebraic closure $\mathbb{F}$ of $\mathbb{F}_q$, for which $C(x, y) = 0$ is called an affine curve. The points on the curve with both coordinates in $\mathbb{F}_q$ are the *rational points*. The curve is *regular* if the projective closure is regular, in particular this implies that $C(x, y)$ is absolutely irreducible. If the curve is regular and $C(x, y)$ has degree m, then the *genus* g of the curve is given by $g = (m-1)(m-2)/2$.

Let $C(x, y) = 0$ be the equation of a regular curve, and let $P_1, P_2, \cdots, P_n$ be rational points on the curve. Let j be a natural number

$$m - 2 \le j \le \left\lfloor \frac{n-1}{m} \right\rfloor$$

and let $\varphi_0(x, y), \varphi_1(x, y), \cdots, \varphi_\mu(x, y)$ denote the monomials $x^a y^b$, ordered with respect to the graduated total degree order $\le_T$ where $(1, 0) <_T (0, 1)$, such that $(a, b) \le_T (0, j)$. The code $C^*(j)$ is then given by the parity check matrix $\boldsymbol{H}$

$$\boldsymbol{H} = \begin{bmatrix} \varphi_0(P_1) & \cdots & \varphi_0(P_n) \\ \varphi_1(P_1) & \cdots & \varphi_1(P_n) \\ \vdots & & \vdots \\ \varphi_\mu(P_1) & \cdots & \varphi_\mu(P_n) \end{bmatrix}. \tag{1}$$

It now follows from [1], that the code $C^*(j)$ has dimension $k = n - (mj - g + 1)$ and

$$d_{\min} \ge d^* = mj - 2g + 2.$$

The number d^* is the *designed distance* of the code.

In the decoding situation we receive a word $\boldsymbol{r}$, which is the sum of a codeword $\boldsymbol{c}$ and an error vector $\boldsymbol{e}$. We calculate the syndrome $\boldsymbol{H}\boldsymbol{r}^T$. If we number the coordinates of the syndrome vector, as we numbered the rows of $\boldsymbol{H}$ and the errors occurred in the points with coordinates (x_i, y_i) $i \in I$, $I \subseteq \{1, 2, \cdots, n\}$, with values e_i, it follows from (1) that

$$S_{ab} = \sum_{i \in I} e_i x_i^a y_i^b. \tag{2}$$

We shall refer to the S_{ab}'s as defined by (2) as a *syndrome* for any $a, b < q - 1$, even if it is only possible to calculate those directly from the parity check matrix if $a + b \le j$.

It now follows from [4, Section V] that if all syndromes S_{ab} $a, b < q-1$ are known then the error values can be found by a fast transformation using of most $(C_1 mq \log q + C_2 m^2 q)$

additions and multiplications in $\mathbb{F}_q$. The problem therefore is to determine the syndromes S_{ab} for $a+b>j$.

We recall that a polynomial

$$f(x, y)=\sum_{i, j} f_{ij} x^i y^j$$

is said to give recursions among the S_{ab}'s if

$$\sum_{i, j} f_{ij} S_{a+ib+j}=0$$

for all a, b, where the indices are calculated modulo $q-1$.

It is easy to see that the curve polynomial $C(x, y)$ gives recursions but usually we need more. We will use [4, Theorem 5] which we state here as

Theorem 1: Suppose that the curve polynomial is of the form

$$C(x, y)=\sum_{l+k\leq m-1} C_{lk} x^l y^k + x^m$$

and that a polynomial

$$\sigma(x, y)=\sum_{l+k\leq h} \sigma_{lk} x^l y^k$$

where $\sigma_{oh}\neq 0$ gives recursions among the S_{ab}'s.

If $C(x, y)$ and $\sigma(x, y)$ do not have a common factor then all S_{ab}'s can be determined from $S_{ab} a+b\leq j$, using at most $A\cdot m^2 q^2$ additions and multiplications in $\mathbb{F}_q$.

The problem is then to find a polynomial $\sigma(x, y)$; this is actually an error locator polynomial. In [4, Theorem 3] we showed how a modified version of Sakata's algorithm [9] could be used to find such a $\sigma(x, y)$ provided that the number of errors was bounded by $d^*/2-m^2/2$. Moreover, it also follows from [4, Theorem 3] that if all syndromes $S_{a, b}$, where $a+b\leq j+m$, could be used as input to the algorithm, then a polynomial $\sigma(x, y)$ of the proper form could be determined, provided that the number of errors were less than $d^*/2$. Therefore, what remains to be done is, given the number of errors is less than $d^*/2$, to find a method for finding the syndromes $S_{a, b}$ $j<a+b\leq j+m$, from the syndromes $S_{a, b}$ $a+b\leq j$. That this indeed is possible is the main result of Feng and Rao [7], but their method has complexity $O(n^3)$. In the next section we show how the algorithm of [4] can be used to implement the idea of Feng and Rao with lower complexity. In particular, we treat the codes $C^*(j)$ coming from the Hermitian curves, that is where

$$C(x, y)=x^{r+1}-y^r-y \tag{3}$$

where r is a power of a prime and $q=r^2$. It is well known [10] that this curve is regular and has r^3 rational points.

The equation of this curve has the form used in Theorem 1 with $m=r+1$ and the corresponding recursion therefore is

$$S_{a+m, b}=S_{a, b+m-1}+S_{a, b+1} \tag{4}$$

which in turn means that the syndromes we need to find are the S_{ab}'s where

$$j<a+b\leq j+m, \qquad 0\leq a<m.$$

III. Finding the Needed Unknown Syndromes

In order to describe the method, we have to explain the algorithm of Sakata in some detail. The algorithm was developed to find recursions consistent with a given two-dimensional array. More precisely, let

$$U=\{u_{p_1, p_2}\} \qquad (p_1, p_2)\leq_T (q_1, q_2)$$

be an array of elements from some field $\mathbb{F}$. We are then interested in the set $\mathcal{S}$ of polynomials

$$f(x, y)=\sum_{l, k} f_{lk} x^l y^k \tag{5}$$

which give a linear recursion among the elements of the array U, that is

$$\sum_{l, k} f_{l, k} u_{l+\alpha, k+\beta}=0 \tag{6}$$

for all (α, β) where $(\alpha+a, \beta+b)\leq_T (q_1, q_2)$ and $x^a y^b$ is the *leading term* of $f(x, y)$ which means that

$$f(x, y)=\sum_{(l, k)\leq_T (a, b)} f_{lk} x^l y^k$$

and $f_{ab}\neq 0$.

A *minimal set* for U is a set F of polynomials from $\mathcal{S}$

$$F=\{f^{(1)}, \cdots, f^{(\nu)}\}$$

with leading terms $x^{s_1^{(i)}} y^{s_2^{(i)}}$, such that

$$s_1^{(1)}>s_1^{(2)}>\cdots>s_1^{(\nu)}=0 \quad \text{and}$$

$$0=s_2^{(1)}<s_2^{(2)}<\cdots<s_2^{(\nu)} \tag{7}$$

and, if we define

$$\Delta=\{(h, r) | h<s_1^{(i)} \text{ and } r<s_2^{(i+1)} \text{ for some } i \text{ where } 0<i<\nu\} \tag{8}$$

then no proper polynomial in $\mathcal{S}$ has leading term with exponent in Δ.

Sakata's algorithm generates a minimal set F for a given array U. A step in the algorithm consists reading the next element of the array, with respect to the total order $<_T$ and then finding a minimal set for the array of elements read so far.

At each step, the current set of polynomials in F are tested on the new element $u_{a, b}$, and if some $f^{(j)}$ is *not consistent*, that is if

$$\sum_{l, k} f_{l, k}^{(j)} u_{l+\alpha, k+\beta}\neq 0, \quad \text{where} \quad (s_1^{(j)}+\alpha, s_2^{(j)}+\beta)=(a, b) \tag{9}$$

then the set F is updated.

The details of the updating may be found in [9]. The important fact here is the increase of the size of Δ set. We denote the minimal set for the array

$$U=\{u_{p_1, p_2}\} \qquad (p_1, p_2)\leq_T (a, b)$$

as $F_{a, b}$ and the corresponding Δ set as defined by (8) as $\Delta_{a, b}$.

The crucial fact is [9, Lemma 4] which we formulate here as

Lemma 2: Suppose $f^{(j)}$ is not consistent with $u_{a,b}$ then every consistent f with leading term $x^{t_1}y^{t_2}$ satisfies $t_1 \geq a - s_1^{(j)} + 1$ or $t_2 \geq b - s_2^{(j)} + 1$.

This implies that if we put

$$\Delta(j) = \{(t_1, t_2) | t_1 \leq a - s_1^{(j)} \quad \text{and} \quad t_2 \leq b - s_2^{(j)}\} \backslash \Delta_{a,b} \tag{10}$$

then the increase of the size of the Δ set is at least $|\Delta(j)|$.

In the decoding case it follows from [4, Theorem 1], that the Δ set for the full array of syndromes $S_{a,b}$ $0 \leq a, b < q-1$ is equal to the number t of errors that have occurred. This fact, combined with the bound on the increase of the size of the Δ set at a given stage in the algorithm, puts restrictions on the number of polynomials in $F_{a,b}$ that are not consistent. This, as will be made precise below, enables us to determine the syndromes $S_{a,b}$ $a + b \leq j + m$. This observation is the main idea of [7], translated into the language of the present setup.

Let us again consider the codes from the Hermitian curve. We have already noted that the syndromes satisfy

$$S_{a+m,b} + S_{a,b+m-1} + S_{a,b+1} \tag{11}$$

or

$$S_{a+m,b-m+1} = S_{a,b} + S_{a,b-m+2}, \quad \text{if} \quad b \geq m-1. \tag{12}$$

Now suppose we have all the syndromes $S_{a,b}$

$$(0, j) \leq_T (a, b) <_T (q_1, q_2) \leq_T (0, j+m).$$

We will then show how S_{q_1,q_2} can be determined. We first note that if $q_1 \geq m$, then S_{q_1,q_2} can be calculated using (11) so we only need to consider the case where $q_1 < m$. Let us consider the polynomials in $F_{q_1,q_2} = \{f^{(1)}, \cdots, f^{(\nu)}\}$ where we can assume without loss of generality the coefficients of the leading terms are all 1. Suppose that for some $1 \leq i \leq \nu$ we can find $\alpha \geq 0$ and $\beta \geq 0$ such that $\alpha + s_1^{(i)} = q_1$ and $\beta + s_2^{(i)} = q_2$. We can then form the sum

$$\sum_{(l,k) <_T (s_1^{(i)}, s_2^{(i)})} f_{lk}^{(i)} S_{l+\alpha, k+\beta} = -v_i \tag{13}$$

and if by chance $f^{(i)}$ is consistent with S_{q_1,q_2} the value of v_i is exactly S_{q_1,q_2}.

We will also consider the case where it is possible to find $\alpha \geq 0$ and $\beta \geq 0$ such that

$$\alpha + s_1^{(i)} = q_1 + m \quad \text{and} \quad \beta + s_2^{(i)} = q_2 - m + 1$$

and then form the sum

$$\sum_{(l,k) <_T (s_1^{(i)}, s_2^{(i)})} f_{lk}^{(i)} S_{l+\alpha, k+\beta} - S_{q_1, q_2-m+2} = -w_i. \tag{14}$$

Here if by chance $f^{(i)}$ is consistent with S_{q_1+m, q_2-m+1} then it follows from (12) that the value of w_i is S_{q_1,q_2}.

In order to use (14) one should argue that the syndromes that appear are all known, but this is the case since either

$$(l+\alpha, \beta+k) <_T (q_1, q_2)$$

or

$$(l+\alpha, \beta+k) <_T (q_1+m, q_2-m+1)$$

in which case the involved syndromes can be calculated by (11).

The remaining part of this section is devoted to estimate the number of cases where (13) and (14) can be calculated and compare this with the number of cases where the polynomials are consistent. This will finally yield a method for determining, under certain conditions, the correct values S_{q_1,q_2}.

Let (q_1, q_2) satisfy $q_1 < m$ and

$$(0, j) <_T \qquad (q_1, q_2) \leq_T (0, j+m).$$

It follows from the structure of Sakata's algorithm, that there exists an i, $1 \leq i \leq \nu$ such that (13) can be calculated. On the other hand, it can be shown that if $j \geq 2m-3$ then there exists an i, $1 \leq i \leq \nu$, such that (14) can be calculated.

Now let

$$K_1 = \{(x, y) | 0 \leq x \leq q_1 \wedge 0 \leq y \leq q_2\}$$
$$K_2 = \{(x, y) | 0 \leq x < m \wedge 0 \leq y \leq q_2 - m + 1\}$$

and put $K = K_1 \cup K_2$. K_2 can be empty ($q_2 < m-1$), but only in the case where $j < 2m-3$. Let

$$A_i = \{(x, y) \in K | x + s_1^{(i)} \leq q_1 \wedge y + s_2^{(i)} \leq q_2\}$$
$$B_i = \{(x, y) \in K | x + s_1^{(i)} \leq q_1 + m \wedge y + s_2^{(i)} \leq q_2 - m + 1\}$$

and let

$$K' = \left(\bigcup_{i=1}^{\nu} A_i \cup B_i \right) \Big\backslash \Delta_{q_1 q_2}.$$

Lemma 3: If $j < q_1 + q_2 \leq j + m$ and $q_1 < m$, then

$$|K| > 2 \left\lfloor \frac{d^* - 1}{2} \right\rfloor.$$

Proof: First, if $K_2 \neq \varnothing$

$$\begin{aligned} |K| &= (q_1+1)(q_2+1) + (m - q_1 - 1)(q_2 - m + 2) \\ &= m(q_1+q_2) - m^2 + 3m - q_1 - 1 \\ &\geq m(j+1) - m^2 + 3m - (q_1+1) \\ &\geq mj - m^2 + 3m = d^* > 2 \left\lfloor \frac{d^* - 1}{2} \right\rfloor. \end{aligned}$$

Second, if $K_2 = \varnothing$ then $q_2 \leq m-2$ so

$$\begin{aligned} |K| - (q_1+1)(q_2+1) &\geq (q_1+1)(q_2+1) \\ &\quad + (m - q_1 - 1)(q_2 - m + 2) > 2 \left\lfloor \frac{d^* - 1}{2} \right\rfloor \end{aligned}$$

as shown above. ■

Lemma 4: If $j < q_1 + q_2 \leq j + m$ and $q_1 < m$, then

$$|K'| \geq |K| - 2|\Delta_{q_1 q_2}|.$$

Proof: Suppose $(x, y) \in K$, $(x, y) \notin K'$, and $(x, y) \notin \Delta_{q_1 q_2}$, then for each $i = 1, \cdots, \nu$ we have

$$x + s_1^{(i)} > q_1 \quad \text{or} \quad y + s_2^{(i)} > q_2$$

and

$$x + s_1^{(i)} > q_1 + m \quad \text{or} \quad y + s_2^{(i)} > q_2 - m + 1.$$

If $(x, y) \in K_1$, then the inequality $x + s_1^{(i)} > q_1$ is satisfied for $i = 1$ but not for $i = \nu$, hence there exists a largest i such that $x + s_1^{(i)} > q_1$ and $x + s_1^{(i+1)} \leq q_1$ but then $y + s_2^{(i+1)} > q_2$, and therefore $(q_1 - x, q_2 - y) \in \Delta_{q_1 q_2}$.

If $(x, y) \in K_2 \backslash K_1$, then the inequality $x + s_1^{(i)} > q_1 + m$ is satisfied for $i = 1$ but not for $i = \nu$, so arguing as before we get

$$(q_1 + m - x, q_2 - m + 1 - y) \in \Delta_{q_1 q_2}.$$

In this manner we have established an injective mapping from $K \backslash (K' \cup \Delta_{q_1 q_2})$ into $\Delta_{q_1 q_2}$ and the lemma follows.

If we combine the two lemmas in the situation where the number t of errors, that has occurred, satisfy

$$t \leq \left\lfloor \frac{d^* - 1}{2} \right\rfloor$$

with the fact that $|\Delta_{q_1 q_2}| \leq t$ we get in particular that $|K'| \geq 1$.

Now let $a_1, a_2, \cdots, a_\rho$ be the different values obtained by either using (13) or (14) and let

$$K_j = \left(\bigcup_{v_i = a_j} A_i \cup \bigcup_{w_i = a_j} B_i \right) \Big\backslash \Delta_{q_1 q_2}, \qquad j = 1, 2, \cdots, \rho.$$

We then have

$$K' = \bigcup_{j=1}^{\rho} K_j.$$

If for all j, $1 \leq j \leq \rho$, we had $a_j \neq S_{q_1 q_2}$ then the next Δ set, Δ', would be increased with K' by Lemma 2. But then

$$|\Delta'| \geq |\Delta_{q_1 q_2}| + |K'| \geq |\Delta_{q_1 q_2}| + |K| - 2|\Delta_{q_1 q_2}|$$

by Lemma 4, and therefore

$$|\Delta'| \geq |K| - |\Delta_{q_1 q_2}| \geq d^* - t > t$$

in contradiction with the fact that $|\Delta'| \leq t$.

This means that at least one of the a_j's, say a_1, is equal to $S_{q_1 q_2}$. Moreover, we have that the Δ set is increased with

$$\overline{K}_1 = \bigcup_{j=2}^{\rho} K_j$$

and therefore $|\Delta_{q_1 q_2}| + |\overline{K}_1| \leq t$, so

$$|\overline{K}_1| \leq t - |\Delta_{q_1 q_2}| < \frac{d^*}{2} - |\Delta_{q_1 q_2}| \leq \frac{1}{2}|K'|$$

by Lemmas 3 and 4, so

$$|K_1| > \frac{1}{2}|K'|.$$

This in general implies that if we put

$$\overline{K}_\gamma = \bigcup_{j \neq \gamma} K_j$$

then for the correct values $S_{q_1 q_2}$ we have $|\overline{K}_\gamma| < \frac{1}{2}|K'|$ and for all the other values we have $|\overline{K}_{\gamma_1}| > \frac{1}{2}|K'|$ since $\overline{K}_{\gamma_1} \supseteq K_\gamma$, so the correct value have the minimal $|\overline{K}_\gamma|$ or equivalently the maximal $|K_\gamma|$.

These arguments show that the syndrome $S_{q_1 q_2}$ can be determined by the following procedure: use (13) or (14) to obtain the different values $a_1, \cdots, a_\rho$. Put

$$K_j = \left(\bigcup_{v_i = a_j} A_i \cup \bigcup_{w_i = a_j} B_i \right) \Big\backslash \Delta_{q_1 q_2}.$$

Let γ be the value for which $|K_\gamma|$ is maximal. We then have that $S_{q_1 q_2} = a_\gamma$.

On calculating (13) or (14) we often have freedom in selecting $f^{(i)}$. However, it can be shown that if

$$(A_1 \cap A_j) \backslash \Delta_{q_1 q_2} \neq \varnothing$$

$f^{(i)}$ and $f^{(j)}$ give the same a_i. This fact is useful in the implementation of the algorithm.

We also note that the procedure described above can be continued beyond the point $(0, j+m)$ in order to obtain all the syndromes $S_{a,b}$ a, $b < q-1$. In this case, the corresponding F set is a Gröbner basis of the ideal of error locator polynomials, whose common zeros just coincide with the error locations.

IV. The Improved Algorithm

Let $C^*(j)$ be the code over $\mathbb{F}_q$, defined in Section II from the Hermitian curve.

$$x^{r+1} - y^r - y = 0$$

where r is a power of a prime and $q = r^2$. We also suppose that

$$2r - 1 < j < \left\lfloor \frac{n-1}{r+1} \right\rfloor.$$

1) Calculate the syndromes S_{ab} $a + b \leq j$.

2) Calculate the syndromes S_{ab} $a + b \leq j + m$ by using either the procedure described in Section III or the equation of the curve. The syndromes are calculated one at a time, according to the total order, and after each calculation Sakata's algorithm is used to update the minimal set.

3) From the minimal set $\{f^{(1)}, \cdots, f^{(\nu)}\}$ corresponding to the array S_{ab} $a+b \leq j+m$, the polynomial $f^{(v)}$ by (7) has the form needed to get, together with $C(x, y)$, and using Theorem 1, all the syndromes S_{ab} $0 \leq a < q-1$, $0 \leq b < q-1$.

4) Use a two-dimensional Fourier transform to obtain the error values, as described in [4].

The step that determines the complexity of the algorithm is step 2). It follows from the calculations in [4, p. 116] with $j + m$ substituted for j that the total number of $\mathbb{F}_q$ multiplications and additions is bounded above by $A \cdot r^3 j^2$. In the interesting case where $n \sim r^3$ we get $A \cdot n \cdot n^{4/3} = A \cdot n^{7/3}$.

The algorithm is implemented in the case $r = 16$, $j = 57$ which gives a $(4096, 3146, 731)$ code over $\mathbb{F}_{28}$. The details

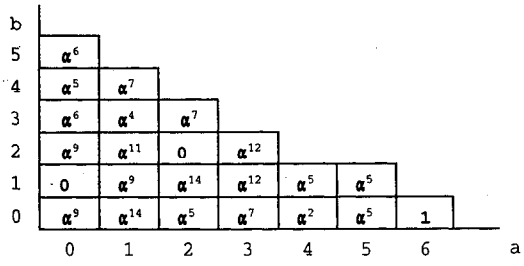

Fig. 1. Syndromes S_{ab} used as input.

can be found in [11]. We illustrate the algorithm here in the example below.

Example: We consider the code $C^*(5)$ from the Hermitian curve $x^5 + y^4 + y = 0$ over $\mathbb{F}_{16}$. It has 64 points of the form (α^i, α^j), where α is a primitive element of $\mathbb{F}_{16}$, $\alpha^4+\alpha+1 = 0$, so we get a (64, 44, 15) code over $\mathbb{F}_{16}$.

Let us consider a seven-error pattern where the errors are located at the points

$$P_1 = (x_1, y_1) = (1, \alpha)$$
$$P_2 = (x_2, y_2) = (\alpha^8, \alpha^3)$$
$$P_3 = (x_3, y_3) = (\alpha, \alpha^7)$$
$$P_4 = (x_4, y_4) = (\alpha^2, \alpha^3)$$
$$P_5 = (x_5, y_5) = (\alpha^{11}, \alpha^3)$$
$$P_6 = (x_6, y_6) = (\alpha^5, \alpha^3)$$

and

$$P_7 = (x_7, y_7) = (\alpha^{14}, \alpha^3).$$

The corresponding error values are $e_1 = \alpha^6$, $e_2 = \alpha^8$, $e_3 = \alpha^7$, $e_4 = \alpha$, $e_5 + 1$, $e_6 = \alpha^6$, and $e_7 = \alpha^{10}$.

The known part of the two-dimensional syndrome array is shown in Fig. 1. Here $S_{6,0}$ and $S_{5,1}$ are calculated by using the equation of the curve. When Sakata's algorithm is used on this array the output is

$$F = \{\alpha + \alpha x + \alpha^{11} y + \alpha^4 x^2 + xy + \alpha^3 x^3 + \alpha^9 x^2 y + x^4,$$
$$\alpha^4 + \alpha^7 x + \alpha y + \alpha^3 x^2 + \alpha^4 xy + x^2 y,$$
$$\alpha^{11} + \alpha^{13} x + \alpha^{13} y + \alpha^{10} xy + y^2\}$$

so $|\Delta| = 6$.

This first unknown syndrome is $S_{4,2}$. For this, estimates can be obtained from all the polynomials in F and these yield the same value α^6, which then is the correct value. It turns out that for all syndromes until $S_{3,4}$ there is only one possibility. One obtains $S_{3,3} = \alpha^3, S_{2,4} = \alpha^6, S_{1,5} = \alpha^4, S_{0,6} = \alpha^{11}, S_{7,0} = S_{2,4} + S_{2,1} = \alpha^8, S_{6,1} = S_{1,5} + S_{1,2} = \alpha^{13}, S_{5,2} = S_{0,6} + S_{0,3} = \alpha$, and $S_{4,3} = \alpha^{10}$. For $S_{3,4}$ one gets $a_1 = \alpha$, obtained from $f^{(2)}$ and $f^{(3)}$ using (13) with $|K_1| = 8$ and $a_2 = \alpha^9$ with $|K_2| = 1$ obtained from $f^{(1)}$ using (14).

The value for $S_{3,4}$ is therefore $S_{3,4} = \alpha$. The F set, which now is updated, becomes

$$F = \{y + y^4 + x^5, \alpha^4 + \alpha^7 x + \alpha y + \alpha^3 x^2 + \alpha^4 xy + x^2 y,$$
$$\alpha^{11} + \alpha^{13} x + \alpha^{13} y + \alpha^{10} xy + y^2\}$$

and now $|\Delta| = 7$.

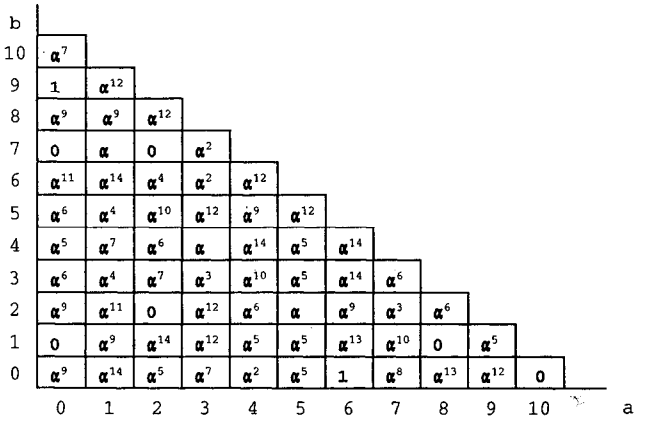

Fig. 2. Syndromes after step 2).

For $S_{2,5} \cdots S_{0,10}$ it turns out that these three polynomials give the same value, so when step 2) of the algorithm is finished we have the syndrome array shown in Fig. 2.

Step 3) in the algorithm now uses the polynomial $C(x, y)$, i.e., $y + y^4 + x^5$ together with $f^{(2)} = \alpha^{11} + \alpha^{13} x + \alpha^{13} y + \alpha^{10} xy + y^2$ to get the full array as shown in Fig. 3.

To illustrate step 4) in the algorithm we calculate the error value at the point $(1, \alpha)$. This is found as

$$\sum_{a,b=0}^{14} S_{ab}(1)^{-a}(\alpha)^{-b} = \sum_{b=0}^{14}\alpha^{-b}\sum_{a=0}^{14} S_{ab}$$
$$= \alpha^{-0}\cdot\alpha^6 + \alpha^{-1}\cdot\alpha^7 + \alpha^{-2}\cdot\alpha^8 + \alpha^{-3}\cdot\alpha^9$$
$$+ \alpha^{-4}\alpha^{10} + \alpha^{-5}\cdot\alpha^{11} + \alpha^{-6}\cdot\alpha^{12} + \alpha^{-7}\cdot\alpha^{13}$$
$$+ \alpha^{-8}\alpha^{14} + \alpha^{-9}\cdot 1 + \alpha^{-10}\cdot\alpha + \alpha^{-11}\cdot\alpha^2$$
$$+ \alpha^{-12}\alpha^3 + \alpha^{-13}\cdot\alpha^4 + \alpha^{-14}\cdot\alpha^5 = \alpha^6.$$

V. General Algebraic Geometry Codes

Feng and Rao consider codes $C_\Omega(D, G)$ from a general nonsingular curve χ over $\mathbb{F}_q$, where the divisor D is $D = P_1 + P_2 + \cdots + P_n$ with the P_i's are rational points on χ and $G = a \cdot Q$, where Q is another rational point. We have only treated the corresponding codes from the Hermitian curve of degree $r+1$, with $Q = P_\infty$ and $a = (r+1)j$. The restriction on the number a is not important, the algorithm is easily modified to cover all a's. However, in order to use the two-dimensional version of Sakata's algorithm it is crucial that the space $L(aQ)$ has a basis of the form $\varphi^l\psi^k$, where the orders of φ and ψ at their pole Q are coprime integers (c, d). This is indeed the case for the Hermitian curve. Other cases as considered in [13] and [14] can also be handled by our algorithm if one chooses the total order defined by (c, d) instead of the graduated total degree order, the details of this can be found in [15]. We also note that the method can be extended to decode up to half the Feng and Rao distance, see [16], which is better then the estimate given here when $j < 3/2m$. Furthermore, it is shown in [3] that the space $L(aQ)$ always has a basis of the form $\varphi_1^{l_1} \cdots \varphi_N^{l_N}$ (with $N \leq g$), and hence any one-point AG code can be decoded by the N-dimensional version of Sakata's algorithm (but with higher complexity than in the

b															
14	0	α^2	α	α^{11}	1	α^5	α^9	α^{13}	α^4	α^4	0	α^3	α^{14}	α^7	α^2
13	α^{13}	α^{14}	α^2	α^{13}	α^8	α^9	α^9	α	1	α^{13}	α^2	0	α^8	α^{12}	α^7
12	α^{14}	α^6	0	α^7	0	α^{13}	α^4	α^{13}	α	α^4	α^6	α^{10}	α^8	1	α^7
11	α^6	α^4	α^9	α^7	α^6	α^4	α^8	α^5	0	α^2	α^7	α	α^3	α^{12}	α^6
10	α^7	α^9	1	α^2	α^3	α^6	α^{10}	α^3	α^6	α^{13}	α^8	α^{12}	α^7	α^4	α^{10}
9	1	α^{12}	α^{11}	α^6	α^6	α^5	α^4	α^8	α^{14}	α^{13}	α^5	α^{13}	α^9	α^2	0
8	α^9	α^9	α^{12}	α^8	α^7	α^3	α^4	α^{11}	α^{10}	α^6	α^7	0	α^3	α^7	α^{11}
7	0	α	0	α^2	α	α^5	α^{14}	α^8	α^{11}	α^{10}	α^7	α^5	α^3	α^{10}	α^3
6	α^{11}	α^{14}	α^4	α^2	α^{12}	α^7	α^3	1	0	α^9	α^9	α^{11}	α^{13}	α^7	α^9
5	α^6	α^4	α^{10}	α^{12}	α^9	α^{12}	α^5	α^{13}	α^3	α^4	α^{13}	α^7	α^2	α^{14}	α^{10}
4	α^5	α^7	α^6	α	α^{14}	α^5	α^{14}	α^3	α^9	1	α^{10}	α^8	α^4	α^{12}	α^{12}
3	α^6	α^4	α^7	α^3	α^{10}	α^5	α^{14}	α^6	α^5	α^7	0	0	α^{13}	α^2	α^5
2	α^9	α^{11}	0	α^{12}	α^6	α	α^9	α^3	α^6	α^3	α^{13}	1	α^{13}	α^5	1
1	0	α^9	α^{14}	α^{12}	α^5	α^5	α^{13}	α^{10}	0	α^5	α^{13}	α^6	α^8	α^2	α^7
0	α^9	α^{14}	α^5	α^7	α^2	α^5	1	α^8	α^{13}	α^{12}	0	α^2	α^{12}	α^9	α^{10}
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14 a

Fig. 3. The full syndrome array.

two-dimensional case). Such cases are treated in [17] and [18], and in general in [19].

REFERENCES

[1] J. Justesen, K. J. Larsen, A. Havemose, H. E. Jensen, and T. Høholdt, "Construction and decoding of a class of algebraic geometry codes," *IEEE Trans. Inform. Theory*, vol. 35, pp. 811–821, July 1989.

[2] A. N. Skorobogatov and S. G. Vlădut, "On the decoding of algebraic-geometric codes," *IEEE Trans. Inform. Theory*, vol. 36, pp. 1051–1061, Spet. 1990.

[3] S. C. Porter, B.-Z. Shen, and R. Pellikaan, "Decoding geometric Goppa codes using an extra place," *IEEE Trans. Inform. Theory*, vol. 38, pp. 1663–1677, Nov. 1992.

[4] J. Justesen, K. J. Larsen, H. E. Jensen, and T. Høholdt, "Fast decoding of codes from algebraic plane curves," *IEEE Trans. Inform. Theory*, vol. 38, pp. 111–121, Jan. 1992.

[5] R. Pellikaan, "On a decoding algorithm for codes on maximal curves," *IEEE Trans. Inform. Theory*, vol. 35, pp. 1228–1232, Nov. 1989.

[6] D. Erhard, "Decoding Hermitian codes over $\mathbb{F}_{q^2}$ up to designed error capability," to appear in *Proc. ACCT 1992* (Bulgaria).

[7] G. L. Feng and T. R. N. Rao, "Decoding algebraic geometric codes up to the designed minimum distance," *IEEE Trans. Inform. Theory*, vol. 39, pp. 37–46, Jan 1993.

[8] I. M. Duursma, "On the decoding procedure of Feng and Rao," to appear in *Proc. ACCT 1992* (Bulgaria).

[9] S. Sakata, "Finding a minimal set of linear recurring relations capable of generating a given finite two-dimensional array," *J. Symb. Comp.*, vol. 5, pp. 321–337, 1988.

[10] H. Stichtenoth, "A note on Hermitian codes over GF(a^2)," *IEEE Trans. Inform. Theory*, vol. 34, pp. 1345–1348, Sept. 1988.

[11] Y. Madelung, "Implementation of a decoding algorithm for AG-codes from the Hermitian curve," Rept. IT 93-137, Inst. Circuit Theory Telecom., Tech. Univ. of Denmark, Lyngby, Denmark, Apr. 1993.

[12] S. Sakata, "Extension of the Berlekamp–Massey algorithm to N dimension," *Inform. Comput.*, vol. 84, pp. 207–239, Feb. 1990.

[13] H. Stichtenoth, "Self-dual Goppa codes," *J. Pure Appl. Algebra*, vol. 55, pp. 199–211, 1988.

[14] N. Kamiya and S. Miura, "Geometric-Goppa codes on some maximal curves and their minimum distance," *Proc. ITW-93*, 1993, pp. 85–86.

[15] S. Sakata, J. Justesen, Y. Madelung, H. E. Jensen, and T. Høholdt, "A fast decoding method of AG codes from Mirua–Kamiya curves C_{ab} up to half the Feng–Rao bound," preprint, Toyohashi Univ. Technol., Aug. 1993. To appear in *Finite Fields and Applications*.

[16] G.-L. Feng and T. R. N. Rao, "A novel approach for construction of algebraic-geometric codes from affine plane curves," Univ. Southwestern Louisiana, preprint 1992.

[17] C. Dahl, "Fast decoding of codes from algebraic curves," *IEEE Trans. Inform. Theory*, vol. 40, pp. 223–230, Jan. 1994.

[18] J. P. Pedersen and A. B. Sørensen, "Codes from certain algebraic function fields with many rational places," Tech. Rep., Math. Inst., Tech. Univ. of Denmark, Lyngby, Denmark, 1990.

[19] S. Sakata, H. E. Jensen, and T. Høholdt, "Generalized Berlekamp–Massey decoding of algebraic geometric codes up to half the Feng–Rao bound," in *Proc. 1994 IEEE Int. Symp. on Information Theory*.