Title	FAST PARALLEL DECODING ON SYSTOLIC ARRAY ARCHITECTURE FOR CODES ON A CLASS OF ALGEBRAIC CURVES (Algebraic Aspects of Coding Theory and Cryptography)
Author(s)	Matsui, Hajime; Sakata, Shojiro; Kurihara, Masazumi
Citation	数理解析研究所講究録 (2005), 1420: 193-205
Issue Date	2005-04
URL	http://hdl.handle.net/2433/47176
Right	
Type	Departmental Bulletin Paper
Textversion	publisher

FAST PARALLEL DECODING ON SYSTOLIC ARRAY ARCHITECTURE FOR CODES ON A CLASS OF ALGEBRAIC CURVES

松井 一　　阪田 省二郎　　栗原 正純
HAJIME MATSUI　SHOJIRO SAKATA　MASAZUMI KURIHARA

ABSTRACT. We construct a two-dimensional systolic array implementing the Berlekamp–Massey–Sakata algorithm to provide error-locator polynomials for codes on selected algebraic curves. This array is constructed by introducing some new polynomials in order to increase the parallelism of the algorithm. The introduced polynomials are used in the majority logic scheme by Sakata *et al.* to correct errors up to the designed minimum distance without affecting its high-speed. The arrangement of the nearest local connection of processing units in the systolic array is obtained for the general case. Furthermore, shortened systolic arrays that reduce the circuit scale and have the same function are constructed with only a slight modification of the connections and controls; this enables the adjustment of the circuit scale for different types of systems.

1. PRELIMINARIES

Let $\mathbb{Z}_0$ be the set of non-negative integers. In this paper, we consider a one-point algebraic-geometric code on Miura's C_a^b curve $\mathcal{X}$ over a finite field $K := \mathbb{F}_q$. For positive integers a and b such that $a < b$ and $\gcd(a,b) = 1$, a C_a^b curve is defined by the polynomial equation

$$(1)\qquad D(x,y) := y^a + ex^b + \sum_{(n_1,n_2)\in\mathbb{Z}_0^2,\, n_1a+n_2b<ab} \chi_{(n_1,n_2)} x^{n_1} y^{n_2} = 0, \quad e \neq 0$$

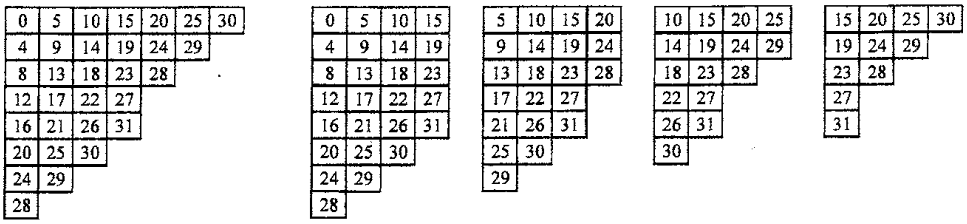
over K. It is known [9] that $\mathcal{X}$ is always absolutely irreducible and has no singular point except at a single infinite point P_∞. For simplicity, we consider a non-singular C_a^b curve although it is possible to argue singular cases similarly [9]. Then, the genus g of $\mathcal{X}$ is given by $g = (a-1)(b-1)/2$; moreover, the residue class ring $K[\mathcal{X}] := K[x,y]/(D(x,y))$ consists of all the algebraic functions having no poles except at P_∞.

Let $\{P_j\}_{1\le j\le n}$ be a set of n K-rational points except P_∞; we denote the pole order of $F \in K[\mathcal{X}]$ at P_∞ as $o(F)$. For $m \in \mathbb{Z}_0$, the K-linear subspace $L(mP_\infty) := \{F \in K[\mathcal{X}] | o(F) \le m\} \cup \{0\}$ has dimension $m - g + 1$, provided $m > 2g - 2$ by Riemann-Roch Theorem. In this paper, we assume that $m > 2g-2$ for simplicity. Our code $\mathcal{C}(m)$ is defined as $\mathcal{C}(m) := \left\{ (c_j) \in K^n \,\middle|\, \sum_{j=1}^n c_j F(P_j) = 0,\ F \in L(mP_\infty) \right\}$.

Given a received word $(r_j) = (c_j) + (e_j)$, where $e_j \neq 0$ only for $j \in \{j_1, \cdots, j_t\}$ corresponding to $\mathcal{E} = \{P_{j_\gamma}\}_{1\le\gamma\le t}$, we want to find a Gröbner basis of the error-locator ideal $I(\mathcal{E}) := \{F \in K[\mathcal{X}] \,|\, F(P_{j_\gamma}) = 0,\ P_{j_\gamma} \in \mathcal{E}\}$. Then, the set of common zeros of all the elements in the Gröbner basis agrees with $\mathcal{E}$, and the error values $\{e_{j_\gamma}\}_{1\le\gamma\le t}$ are obtained by O'Sullivan's formula in [10].

In this paper, we do not use any special fonts to represent vectors. For any element $n \in \mathbb{Z}_0^2$, n_1 and n_2 denote the first and second components of vector n. Let $\Phi(A) := \{n \in \mathbb{Z}_0^2 \,|\, n_2 < A\}$ for $A \in \mathbb{Z}_0$. Then, an element of $K[\mathcal{X}]$ is uniquely expressed as $F(x,y) = \sum_{n\in\Phi(a)} F_n x^{n_1} y^{n_2}$. We denote $x^{n_1}y^{n_2}$ by z^n; furthermore, we define $o(n) := o(z^n) = n_1 a + n_2 b$ for $n \in \mathbb{Z}_0^2$, where $o(\cdot)$ is defined on both $\mathbb{Z}_0^2$ and $K[\mathcal{X}]$, and we remember that $o(F) = \max\{o(n) |\, F_n \neq 0\}$ if $F = \sum_{n\in\Phi(a)} F_n z^n \in K[\mathcal{X}]$.

For A, $A' \in \mathbb{Z}_0$, we denote $\Phi(A, A') := \{n \in \Phi(A) | o(n) \le A'\}$, where Figure shows an example of $\Phi(2a-1, A')$ for $A' = 31$ and $(a,b) = (4,5)$. From a given received word (r_j), we can calculate the syndrome $\{u_l\}$ for $l \in \Phi(2a-1, m)$ by $u_l = \sum_{j=1}^n r_j z^l(P_j)$, where $u_l = \sum_{\gamma=1}^t e_{j_\gamma} z^l(P_{j_\gamma})$



0	5	10	15	20	25	30
4	9	14	19	24	29	
8	13	18	23	28		
12	17	22	27			
16	21	26	31			
20	25	30				
24	29					
28						

0	5	10	15
4	9	14	19
8	13	18	23
12	17	22	27
16	21	26	31
20	25	30	
24	29		
28			

5	10	15	20
9	14	19	24
13	18	23	28
17	22	27	
21	26	31	
25	30		
29			

10	15	20	25
14	19	24	29
18	23	28	
22	27		
26	31		
30			

15	20	25	30
19	24	29	
23	28		
27			
31			

Figure. Pole orders on $\Phi(7,31)$ and $\Phi^{(i)}(4,31)$ $(0 \le i \le 3)$

according to the definition of $C(m)$. For $\{u_n\}$ with $n \in \Phi(2a-1,m)\backslash\Phi(a,m)$, we may decide syndromes by the linear dependency among the elements of $K[\mathcal{X}]$ induced by the curve defining equation (1). More precisely, if $n \in \Phi(2a-1,m)\backslash\Phi(a,m)$ and $l \in \Phi(a,m)$ with $o(n) = o(l)$, we see that $n' := n - (0,a)$ satisfies $n' \in \Phi(a-1, m-ab)$ and $l = (b,0) + n'$; we then have $u_n + eu_l + \sum_{r \in \Phi(a,ab-1)} \chi_r u_{r+n'} = 0$.

For $\Phi^{(i)}(a) := (0,i) + \Phi(a) = \{(n_1,n_2) \in \mathbb{Z}_0^2 \,|\, i \le n_2 \le i+a-1\}$ with $0 \le i \le a-1$, we have $\Phi(2a-1) = \bigcup_{i=0}^{a-1} \Phi^{(i)}(a)$ (non-disjoint union). Furthermore, it should be noted that $o(n) \neq o(n')$ if and only if $n \neq n'$ for n, $n' \in \Phi^{(i)}(a)$. Similarly, for $\Phi^{(i)}(a,A') := \{n \in \Phi^{(i)}(a) | o(n) \le A'\}$, we have $\Phi(2a-1,A') = \bigcup_{i=0}^{a-1} \Phi^{(i)}(a,A')$. Note that $\Phi^{(0)}(a) = \Phi(a)$ and $\Phi^{(0)}(a,A') = \Phi(a,A')$. Figure shows an example of $\Phi^{(i)}(a,A')$ for $A' = 31$ and $(a,b) = (4,5)$.

The standard partial order $\le$ on $\mathbb{Z}_0^2$ is defined as follows: for $n = (n_1,n_2)$, $n' = (n_1',n_2') \in \mathbb{Z}_0^2$, $n \le n'$ if and only if $n_1 \le n_1'$ and $n_2 \le n_2'$. Let $l^{(i)} \in \Phi^{(i)}(a,A')$ be $o(l^{(i)}) = o(l)$ for $l \in \Phi(a,A')$ if there exists such an $l^{(i)}$ for l and i. Then, $l^{(i)}$ is uniquely determined for each l and i if it exists. Note that $l^{(0)} = l$ from its definition.

We define *degree* $\deg(F) \in \Phi(a)$ of $F \in K[\mathcal{X}]$ by $o(\deg(F)) = o(F)$, and let $s := \deg(F)$. From now on, $\Phi(a,o(s))$ is abbreviated as $\Phi(a,s)$. Defining $dF_l := \sum_{n \in \Phi(a,s)} F_n u_{n+l^{(s_2)}-s}$ if $s \le l^{(s_2)}$, and $dF_l := 0$ otherwise, we call dF_l *discrepancy* of $F \in K[\mathcal{X}]$ at $l \in \Phi(a)$. Let $V(u,A')$ be the set of bivariate polynomials whose discrepancies are zero at every $l \in \Phi(a,A')$, and let $V(u,-1) := K[\mathcal{X}]$. In order to obtain the Gröbner basis [1] of $I(\mathcal{E})$, we compute the set of minimal elements in $V(u,B)$ in the meaning of $\deg(\cdot)$ concerning $\le$ for a sufficiently large $B \in \mathbb{Z}_0$. It is shown that $B = 2t + 4g - 2 + a$ is sufficient for correcting t errors from the facts that $F \in I(\mathcal{E})$ if $\sum_{n \in \Phi(a,s)} F_n u_{n+l} = 0$ for all $l \in \Phi(a)$ with $o(l) \le t + 2g - 1$ ([12], proof of Lemma 2) and that the pole orders of the minimal elements in $I(\mathcal{E})$ are less than or equal to $t + 2g - 1 + a$ ([3], proof of Lemma 5). From now on, we set $B := 2t + 4g - 2 + a$.

If we design a code that can correct up to t errors, the minimum distance d_{min} of the code must be greater than or equal to $2t+1$. It is well-known that the Goppa designed distance d_{G} of $C(m)$, which is the lower bound of d_{min} and agrees with the Feng–Rao designed distance d_{FR} if $m \ge 4g-2$, is equal to $m - 2g + 2$. Thus, we can set $m = 2t + 2g - 1$ and obtain $V(u,m)$ by using $\{u_l\}_{l \in \Phi(a,m)}$. Therefore, to obtain $I(\mathcal{E})$, $2g - 1 + a$ syndromes of $\{u_l\}_{l \in \Phi(a)}$ for $2t + 2g - 1 < o(l) \le 2t + 4g - 2 + a$ are required. These are called *unknown syndromes.*

2. BMS Algorithm via Kamiya–Miura for Codes on C_a^b Curves

Before stating Berlekamp–Massey–Sakata (BMS) algorithm, we introduce certain important quantities such as $\bar{\imath}$ for $0 \le i \le a-1$ to the updating of BMS algorithm and the construction of systolic array in this paper. By the assumption $\gcd(a,b) = 1$, we have an integer b^{-1} such that $0 < b^{-1} \le a-1$, $bb^{-1} \equiv 1 \pmod{a}$. For $0 \le N \le B$, we define a unique integer $\bar{\imath}$ in $\{0,1,\cdots,a-1\}$ by $\bar{\imath} \equiv b^{-1}N - i \pmod{a}$, which depends on not only i but also N; however, N is not clearly indicated. If there exists $l^{(i)} = (l_1^{(i)}, l_2^{(i)}) \in \Phi^{(i)}(a,B)$ with $N = o(l^{(i)})$, then $\bar{\imath} = l_2^{(i)} - i$ since $l_2^{(i)} \equiv b^{-1}N \pmod{a}$. Note that $\bar{\bar{\imath}} = i$, and that, if $l^{(i)}$ exists, then $l^{(\bar{\imath})}$ also exists and we have $l^{(i)} = l^{(\bar{\imath})}$ since $l_2^{(i)} = l_2^{(\bar{\imath})}$ by $0 \le l_2^{(i)} - \bar{\imath} = i \le a-1$.

Next, we explain the quantities $s_N^{(i)} = (s_{N,1}^{(i)}, i) \in \Phi(a)$ and $c_N^{(i)} = (c_{N,1}^{(i)}, i) \in \Phi(a) \cup \{(-1,i)\}$ for $0 \leq i \leq a-1$. At the first stage of BMS algorithm, N, $s_N^{(i)}$, and $c_N^{(i)}$ are initialized as 0, $(0,i)$, and $(-1,i)$, respectively. Let $l \in \Phi(a,B)$ and $l^{(i)} \in \Phi^{(i)}(a,B)$ be $N = o(l) = o(l^{(i)})$ if such l and $l^{(i)}$ exist. Then, we define $d_N^{(i)} := d(F_N^{(i)})_l$ for $F_N^{(i)} \in K[\mathcal{X}]$. In N-updating of BMS algorithm, $s_N^{(i)}$ and $c_N^{(\bar{i})}$ are updated to $s_{N+1}^{(i)}$ and $c_{N+1}^{(\bar{i})}$ as follows:

$$s_{N+1}^{(i)} : = \begin{cases} s_N^{(i)} & \text{if } d_N^{(i)} = 0 \text{ or } s_N^{(i)} \geq l^{(i)} - c_N^{(\bar{i})}, \\ l^{(i)} - c_N^{(\bar{i})} & \text{otherwise,} \end{cases} \tag{2}$$

$$c_{N+1}^{(\bar{i})} : = \begin{cases} c_N^{(\bar{i})} & \text{if } d_N^{(i)} = 0 \text{ or } s_N^{(i)} \geq l^{(i)} - c_N^{(\bar{i})}, \\ l^{(i)} - s_N^{(i)} & \text{otherwise.} \end{cases} \tag{3}$$

If $l^{(i)}$ exists, then $s_N^{(i)} \geq l^{(i)} - c_N^{(\bar{i})}$ is equivalent to $s_{N,1}^{(i)} \geq l_1^{(i)} - c_{N,1}^{(\bar{i})}$ since $i = l_2^{(i)} - \bar{i}$. For simplicity, we define the preserved condition (P) of $s_N^{(i)}$ and $c_N^{(\bar{i})}$ as follows:

$$\text{(P)} \ \Leftrightarrow \ d_N^{(i)} = 0 \text{ or } s_N^{(i)} \geq l^{(i)} - c_N^{(\bar{i})}.$$

Then the above condition "otherwise" indicates that $d_N^{(i)} \neq 0$ and $s_{N,1}^{(i)} < l_1^{(i)} - c_{N,1}^{(\bar{i})}$.

In [7][8], the BMS algorithm starts from $(0,0) \in \Phi(a,B)$, and is performed along with each element of $\Phi(a,B)$ in the total order $o(\cdot)$ as ordering. For later use, we describe here the algorithm performed not along with the pole order in the pole order sequence $o\,(\Phi(a,B))$ but along with $0 \leq N \leq B$ including gap-numbers.

BMS Algorithm:

Input: $\{u_l\}$ for $l \in \Phi(2a-1, m)$.

Output: $F_{m+1}^{(i)}$ and $G_{m+1}^{(i)}$ for all $0 \leq i \leq a-1$.

In each step, the indicated procedures are carried out for all $0 \leq i \leq a-1$.

Step 0: (initializing) $N := 0$, $s_N^{(i)} := (0,i)$ $c_N^{(i)} := (-1,i)$, $F_N^{(i)} := y^i$, $G_N^{(i)} := 0$.

Step 1: (computing discrepancy) If $l^{(i)}$ exists and $s_N^{(i)} \leq l^{(i)}$, $d_N^{(i)} := \sum_{n \in \Phi(a, s_N^{(i)})} F_{N,n}^{(i)} u_{n+l^{(i)}-s_N^{(i)}}$; otherwise, $d_N^{(i)} := 0$.

Step 2: (N-updating) $s_{N+1}^{(i)}$ and $c_{N+1}^{(\bar{i})}$ as described above,

$$F_{N+1}^{(i)} := z^{s_{N+1}^{(i)} - s_N^{(i)}} F_N^{(i)} - d_N^{(i)} z^{s_{N+1}^{(i)} - l^{(i)} + c_N^{(\bar{i})}} G_N^{(\bar{i})}, \tag{4}$$

$$G_{N+1}^{(\bar{i})} := \begin{cases} G_N^{(\bar{i})} & \text{if (P),} \\ (d_N^{(i)})^{-1} F_N^{(i)} & \text{otherwise.} \end{cases} \tag{5}$$

Step 3: If $N < m$, change N to $N+1$ and go to Step 1; otherwise, stop algorithm. □

In (4), if $l^{(i)}$ does not exist, we define $F_{N+1}^{(i)} := z^{s_{N+1}^{(i)} - s_N^{(i)}} F_N^{(i)}$.

The present form of the BMS algorithm, which is performed along with pole orders for the syndromes from codes on C_a^b curves, by Kamiya–Miura [2] is the reduced version of Sakata's algorithm [11]. As previously stated, the unknown syndromes must be determined to perform Step 1–2 for $m < N \leq B$; the BMS algorithm including the determination of unknown syndromes is described in a later section. From now on, N is called a processor number, which corresponds to processor's number in the two-dimensional systolic array described later in section 4. The following theorem confirms that $\{F_N^{(i)}\}_{0 \leq i \leq a-1}$ is a system of minimal polynomials.

Theorem 1. *We have* $F_N^{(i)} \in V(u, N-1)$, $\deg(F_N^{(i)}) = s_N^{(i)}$, *and* $F^{(i)}_{N,s_N^{(i)}} = 1$*; moreover,*

$$\min\left\{\zeta_{N,1}^{(i)} \,\middle|\, F \in V(u, N-1),\ \deg(F) = \left(\zeta_{N,1}^{(i)}, i\right)\right\} = s_{N,1}^{(i)}, \tag{6}$$

$$s_{N,1}^{(0)} \geq s_{N,1}^{(1)} \geq \cdots \geq s_{N,1}^{(a-1)}. \quad \square \tag{7}$$

The proof of Theorem 1 is referred to [2][11] or Appendix A, in which $s_{N,1}^{(i)} = c_{N,1}^{(i)} + 1$ is also proved for all N, i.

For later use, we describe a variant of the above algorithm. We associate $F(z)$ with a reciprocal univariate polynomial $\overline{F}(Z) := \sum_{n \in \Phi(a,s)} F_n Z^{o(s)-o(n)}$, where $s = \deg(F)$. Note that the degree of F must be presented together with $\overline{F}$ to reconstruct $F(z)$ from $\overline{F}(Z)$. For example, $Z^2 + 1$ corresponds to $1 + x$ if $(a, b) = (2, 3)$ and $s = (1, 0)$, and also corresponds to $x + x^2$ if $s = (2, 0)$. Setting

$$\overline{F}_N^{(i)}(Z) := \overline{F_N^{(i)}}(Z) \quad \text{and} \quad \overline{G}_N^{(\bar{i})}(Z) := Z^{N-M}\overline{G_N^{(\bar{i})}}(Z),$$

where M is the processor number at which the updating $G_N^{(\bar{i})} := (d_M^{(j)})^{-1} F_M^{(j)}$ occurs, or $M := 0$ if $G_N^{(\bar{i})} = 0$; note that $\overline{G}_N^{(\bar{i})} = Z^{N-M}(d_M^{(j)})^{-1}\overline{F}_M^{(j)}$ holds. Thus, we obtain the univariate version of the BMS algorithm by initializing $\overline{F}_0^{(i)} := 1$, $\overline{G}_0^{(i)} := 0$, and replacing (4)(5) to the followings:

$$\overline{F}_{N+1}^{(i)} := \overline{F}_N^{(i)} - d_N^{(i)} \overline{G}_N^{(\bar{i})}, \tag{8}$$

$$\overline{G}_{N+1}^{(\bar{i})} := \begin{cases} Z\overline{G}_N^{(\bar{i})} & \text{if (P)}, \\ Z(d_N^{(i)})^{-1}\overline{F}_N^{(i)} & \text{otherwise.} \end{cases} \tag{9}$$

This form in which the algorithm updates the reciprocal univariate polynomials corresponds to Kötter's algorithm [3]. Furthermore, we apply this mechanism for calculating "candidate value" of the unknown syndromes in later section.

3. Determination of Unknown Syndromes

The syndromes obtained with a received word are $\{u_n\}$ only for $n \in \Phi(2a-1, m)$, and therefore, the N-updating for $N > m$ needs the determination of unknown syndrome at Step 1 in the above algorithm to continue the loop until B. Through the restriction of curves and reduction of computation, an effective parallel algorithm can be constructed.

From now on, we impose the following restriction of algebraic curves.

Assumption. *In the defining equation* $D(z) = 0$, $D(z) := y^a - ex^b - \sum_{n \in \Phi(a, ab-1)} \chi_n z^n$ *of the curve* $\mathcal{X}$, *let* $m_D := \max\{o(n) \mid n \in \Phi(a, ab-1),\ \chi_n \neq 0\}$. *Then we only adopt the curve satisfying* $m_D \leq b$ *and* $e = 1$ *in the defining equation. This brings about the defining equation* $D(z) = y^a - x^b - \sum_{n \in \Phi(1,b)} \chi_n z^n$.

For example, the condition is satisfied for the elliptic curves having a defining equation of the form $y^2 + a_2 y = a_5 x^3 + a_1 x + a_0$ since $(a, b) = (2, 3)$ in this case. The Hermitian curves are another example. Let r be the power of a prime number, then a Hermitian curve is defined by the equation $y^r + y = x^{r+1}$ over $K = \mathbb{F}_{r^2}$; this curve has $r^3 + 1$ K-rational points including a single infinite point, which attain the Hasse–Weil bound $q + 1 + 2g\sqrt{q}$.

This restriction leads to a useful property of linear dependency among $\{z^n\}$ and consequently the syndromes $\{u_n\}$. As previously stated, if $n \in \Phi(2a-1, B) \backslash \Phi(a, B)$ and $l \in \Phi(a, B)$ with $o(n) = o(l)$, then $n' := n - (0, a)$ satisfies $n' \in \Phi(a-1, B-ab)$ and $l = (b, 0) + n'$. By the above assumption, we have $u_n = \sum_{r \in \Phi(1,b)} \chi_r u_{r+n'} + u_l$, where the sum is computed at Step 0 (initializing) without the unknown syndromes in the algorithm since $r+n' \in \Phi(a,m)$. Therefore, for all $n \in \Phi(2a-1,B)$, u_n can be represented as $u_n = \wp_n + u_l$, where

$$\wp_n := \begin{cases} 0 & \text{if } n = l \in \Phi(2a-1,B) \cap \Phi(a,B), \\ \sum_{r \in \Phi(1,b)} \chi_r u_{r+n'} & \text{otherwise.} \end{cases}$$

If $l^{(i)} \in \Phi^{(i)}(a,B)$ with $o(l^{(i)}) = N$ exists and $s_N^{(i)} \leq l^{(i)}$, we define *candidate* $b_N^{(i)}$ of unknown syndrome as $b_N^{(i)} := \sum_{\substack{n \in \Phi(a,s_N^{(i)}) \\ n \neq s_N^{(i)}}} F_{N,n}^{(i)} u_{n+l^{(i)}-s_N^{(i)}} + \wp_{l^{(i)}}$. Note that $u_{n+l^{(i)}-s_N^{(i)}}$ is not an unknown syndrome since $o\left(n + l^{(i)} - s_N^{(i)}\right) \leq N-1$. After u_l is determined, it follows that $b_N^{(i)} = d_N^{(i)} - u_l$. It is worth to notice that, in [12][13], the candidate of unknown syndrome was defined by omitting $\wp_{l^{(i)}}$ from $b_N^{(i)}$, which agrees with $d_N^{(i)} - u_{l^{(i)}}$. In the following majority logic scheme ($\Diamond$), which is quoted from [12][13] with this modification, and which is similar to that of Kötter [3], our definition makes it possible to classify the set $\{b_N^{(i)}\}$ into equivalence classes according not to the linear dependency as in [12][13] but to the easier equality relation. Our technique is, under the restriction of curves, the combination of this modification and further $\overline{V}_N^{(i)}$, $\overline{W}_N^{(\bar{\imath})}$ to realize parallel computation of $b_N^{(i)}$ on systolic array.

($\Diamond$): Let Ξ be the set of $b_N^{(i)}$ for which $l^{(i)}$ exists and $s_N^{(i)} \leq l^{(i)}$, and let $\{B_\gamma\}$, $B_\gamma = \{b_N^{(i)}\}_{i \in I_\gamma}$ be the set of equivalence classes dividing Ξ by the equality relation. For each γ, define the number of votes h_γ as $h_\gamma := \sum_{i \in I_\gamma} \max\left\{0,\, l_1^{(i)} - c_{N,1}^{(\bar{\imath})} - s_{N,1}^{(i)}\right\}$. Then, there is a unique largest number of votes h_δ, and for $i \in I_\delta$, $u_l = -b_N^{(i)}$ and $d_N^{(i)} = 0$ hold.

It is shown in [13] that $h_\delta > \sum_{\gamma \neq \delta} h_\gamma$ for the largest number of votes h_δ, and thus, our variant of candidate $b_N^{(i)}$ from [13] also gives the correct unknown syndrome. To implement ($\Diamond$) on systolic array, the definition of $V_N^{(i)}(z)$ and $W_N^{(i)}(z)$ is adapted as follows:

$$(10) \quad V_N^{(i)}(z) := \sum_{n \in \Phi^{(i)}(a,B)} V_{N,\eta+s_N^{(i)}-n}^{(i)} z^{\eta+s_N^{(i)}-n}, \quad W_N^{(\bar{\imath})}(z) := \sum_{n' \in \Phi^{(j)}(a,B)} W_{N,\eta+s_M^{(j)}-n'}^{(\bar{\imath})} z^{\eta+s_M^{(j)}-n'},$$

$$(11) \quad V_{N,\eta+s_N^{(i)}-n}^{(i)} := \sum_{\substack{r \in \Phi(a,s_N^{(i)}) \\ o(r+n-s_N^{(i)}) \leq \max\{m,N-1\}}} F_{N,r}^{(i)} u_{r+n-s_N^{(i)}} + \sum_{\substack{r \in \Phi(a,s_N^{(i)}) \\ o(r+n-s_N^{(i)}) > \max\{m,N-1\}}} F_{N,r}^{(i)} \wp_{r+n-s_N^{(i)}},$$

$$(12) \quad W_{N,\eta+s_M^{(j)}-n'}^{(\bar{\imath})} := \sum_{\substack{r \in \Phi(a,s_M^{(j)}) \\ o(r+n'-s_M^{(j)}) \leq \max\{m,N-1\}}} G_{N,r}^{(\bar{\imath})} u_{r+n'-s_M^{(j)}} + \sum_{\substack{r \in \Phi(a,s_M^{(j)}) \\ o(r+n'-s_M^{(j)}) > \max\{m,N-1\}}} G_{N,r}^{(\bar{\imath})} \wp_{r+n'-s_M^{(j)}},$$

where η is a fixed element in $\Phi(2a-1)$ satisfying $\eta \geq n$ for all $n \in \Phi(2a-1,B)$. We regard as $\deg(V_N^{(i)}) := \eta + s_N^{(i)}$ and $\deg(W_N^{(\bar{\imath})}) := \eta + s_M^{(j)}$. Then we define

$$(13) \quad \overline{V}_N^{(i)}(Z) := \sum_{n \in \Phi^{(i)}(a,B)} V_{N,\eta+s_N^{(i)}-n}^{(i)} Z^{o(n)}, \quad \overline{W}_N^{(\bar{\imath})}(Z) := \sum_{n' \in \Phi^{(j)}(a,B)} W_{N,\eta+s_M^{(j)}-n'}^{(\bar{\imath})} Z^{o(n')+N-M}.$$

Note that, in (11), the coefficient of $z^{\eta+s_N^{(i)}-n}$ with $o(n) = N > m$, i.e., the coefficient of $Z^{o(n)} = Z^N$, equals the candidate $b_N^{(i)}$ of unknown syndrome. Then we obtain the following theorem.

Theorem 2. *If $N \leq m$, then we have*

$$\overline{V}^{(i)}_{N+1} = \overline{V}^{(i)}_{N} - d^{(i)}_{N}\overline{W}^{(\bar{\imath})}_{N}, \tag{14}$$

$$\overline{W}^{(\bar{\imath})}_{N+1} = \begin{cases} Z\left(d^{(i)}_{N}\right)^{-1}\overline{V}^{(i)}_{N} & \text{if (P)}, \\ Z\overline{W}^{(\bar{\imath})}_{N} & \text{otherwise.} \end{cases} \tag{15}$$

If $N > m$, then we have

$$\overline{V}^{(i)}_{N+1} = \overline{V}^{(i)}_{N} + u_l Z^N \overline{F}^{(i)}_{N} - d^{(i)}_{N}\left(\overline{W}^{(\bar{\imath})}_{N} + u_l Z^N \overline{G}^{(\bar{\imath})}_{N}\right), \tag{16}$$

$$\overline{W}^{(\bar{\imath})}_{N+1} = \begin{cases} Z\left(d^{(i)}_{N}\right)^{-1}\left(\overline{V}^{(i)}_{N} + u_l Z^N \overline{F}^{(i)}_{N}\right) & \text{if (P)}, \\ Z\left(\overline{W}^{(\bar{\imath})}_{N} + u_l Z^N \overline{G}^{(\bar{\imath})}_{N}\right) & \text{otherwise.} \end{cases} \tag{17}$$

We postpone the proof of Theorem 2 until Appendix B.

Thus, we obtain the following version of BMS algorithm including the determination of unknown syndromes, employing the majority logic scheme [12][13], where the candidates of unknown syndromes are computed parallelly by polynomials $\overline{V}^{(i)}_{N}$ and $\overline{W}^{(i)}_{N}$ introduced above.

Parallel Version of BMS Algorithm (Complete Form):
Input: $\{u_l\}$ for $l \in \Phi(2a-1, m)$.
Output: $F^{(i)}_{B+1}$ and $G^{(i)}_{B+1}$ for all $0 \leq i \leq a-1$.
In each step, the indicated procedures are carried out for all $0 \leq i \leq a-1$.

Step 0: (initializing) $N := 0$, $s^{(i)}_{N}$, $c^{(i)}_{N}$, $\overline{F}^{(i)}_{N} := 1$, $\overline{G}^{(i)}_{N} := 0$, $\overline{W}^{(i)}_{N} := 0$, and $\overline{V}^{(i)}_{N} := \sum_{n\in\Phi^{(i)}(a,m)} u_n Z^{o(n)} + \sum_{n\in\Phi^{(i)}(a,B),\, m<o(n)} \wp_n Z^{o(n)}$ as above.

Step 1: (determining unknown syndrome, checking discrepancy) While $0 \leq N \leq m$, $d^{(i)}_{N} := \overline{V}^{(i)}_{N,N}$ if $l^{(i)}$ exists and $s^{(i)}_{N} \leq l^{(i)}$; $d^{(i)}_{N} := 0$ otherwise. While $N > m$, $(\Diamond)$ is carried out, and $d^{(i)}_{N} := \overline{V}^{(i)}_{N,N} + u_l$ if $l^{(i)}$ exists and $s^{(i)}_{N} \leq l^{(i)}$; $d^{(i)}_{N} := 0$ otherwise.

Step 2: (N-updating) $s^{(i)}_{N+1}$, $c^{(i)}_{N+1}$, $\overline{F}^{(i)}_{N+1}$, $\overline{G}^{(i)}_{N+1}$ are the same as above. While $0 \leq N \leq m$, $\overline{V}^{(i)}_{N}$ and $\overline{W}^{(i)}_{N}$ are updated by (14) and (15). While $m < N$, $\overline{V}^{(i)}_{N}$ and $\overline{W}^{(i)}_{N}$ are updated by (16) and (17).

Step 3: If $N < B$, change N to $N+1$ and go to Step 1; otherwise, stop algorithm. □

4. Systolic Array for Parallel BMS Algorithm

In this section, we describe two-dimensional systolic array for the algorithm. The two-dimensional systolic array is constructed by the following rules.

(i): it is organized by connected processors P_N $(0 \leq N \leq B)$ in a series
(ii): each P_N contains a cells $\{\mathrm{C}^{(i)}_{N}\}_{0\leq i<a}$
(iii): all $\{\mathrm{C}^{(i)}_{N}\}$ have input and output terminals
(iv): $\mathrm{C}^{(i)}_{N}$ is connected to $\mathrm{C}^{(i)}_{N+1}$
(v): $\mathrm{C}^{(i)}_{N}$ is connected to $\mathrm{C}^{(i^*)}_{N+1}$, where i^* is uniquely defined by $i^* \equiv b^{-1} + i \pmod{a}$

It should be noted that $i^* \equiv b^{-1} + i \pmod{a}$ is equivalent to $\bar{\imath} \equiv b^{-1}(N+1) - i^* \pmod{a}$, which implies that $\bar{\imath}$ agrees with $\overline{i^*}$ at $N+1$. The cell $\mathrm{C}^{(i)}_{N}$ calculates the right-hand sides of the updating formulas, and transmits the resulting values $s^{(i)}_{N+1}$, $\overline{F}^{(i)}_{N+1}$, $\overline{V}^{(i)}_{N+1}$ to $\mathrm{C}^{(i)}_{N+1}$ through the connection (iv), and $c^{(\bar{\imath})}_{N+1}$, $\overline{G}^{(\bar{\imath})}_{N+1}$, $\overline{W}^{(\bar{\imath})}_{N+1}$ to $\mathrm{C}^{(i^*)}_{N+1}$ through the connection (v). All calculations of the values and the coefficients of the polynomials in the cells are synchronized at each clock signal, and in the next section, we show the scheduling, that is, the calculations that are done at each clock signal.

It is strongly desirable that the connection between cells satisfies local condition in the sense that only the adjoining cells are connected; this is precisely defined as follows. Let $\{(j,N)\}_{0\le j<a,0\le N\le B}$ be a set of lattice points. For each N, the lattice points $(0,N)$, $(1,N)$, $\cdots$, $(a-1,N)$ are regarded as the positions of a cells $\{\mathrm{C}_N^{(i)}\}_{0\le i<a}$ in one processor P_N, although cell $\mathrm{C}_N^{(j)}$ is not generally situated at (j,N). Two cells in P_N and P_{N+1} situated at lattice points (j,N) and $(j^+,N+1)$ are said to be in neighborhood if $|j-j^+|\le 1$. The systolic array is said to satisfy *local condition* if all the pairs of cells connected by rules (iv) and (v) are in neighborhood.

We first argue on the arrangement of cells for the decoding of codes on C_a^b curves with $b\equiv 1\,(\mathrm{mod}\,a)$; we then solve the general case including a, b with $b\not\equiv 1\,(\mathrm{mod}\,a)$. Let $b\equiv 1\,(\mathrm{mod}\,a)$, then we define

$$\phi_N(j):\equiv\begin{cases} a-\dfrac{j-N}{2} & j+N\text{ is even},\\ \dfrac{j+N+1}{2} & j+N\text{ is odd},\end{cases}\tag{18}$$

$$\psi_N(j):\equiv\begin{cases} \dfrac{j+N}{2} & j+N\text{ is even},\\ a-\dfrac{j-N+1}{2} & j+N\text{ is odd},\end{cases}\tag{19}$$

where $:\equiv$ indicates that $\phi_N(j)$, $\psi_N(j)$ are chosen in the range $0\le\phi_N(j),\psi_N(j)\le a-1$ by $\mathrm{mod}\,a$. Then $\psi_N(j)\equiv N-\phi_N(j)\,(\mathrm{mod}\,a)$ is easily checked. If $\phi_N(j)=i$, then $\psi_N(j)=\bar{\imath}$ holds since $\bar{\imath}\equiv N-i\,(\mathrm{mod}\,a)$ by $b\equiv 1\,(\mathrm{mod}\,a)$.

Situating the cell $\mathrm{C}_N^{(\phi_N(j))}$ at position (j,N), we see that connection (iv) implies that $\mathrm{C}_N^{(\phi_N(j))}$ is connected to $\mathrm{C}_{N+1}^{(\phi_{N+1}(j'))}$ if $\phi_N(j)=\phi_{N+1}(j')$, and connection (v) implies that $\mathrm{C}_N^{(\phi_N(j))}$ is connected to $\mathrm{C}_{N+1}^{(\phi_{N+1}(j''))}$ if $\psi_N(j)=\psi_{N+1}(j'')$. It can then be shown that the local condition is satisfied. More precisely, the following relations hold:

$$\phi_N(j)=\begin{cases}\phi_{N-1}(a-1) & j=a-1,\ j+N\text{ is odd}\\ \phi_{N-1}(j+1) & j\ne a-1,\ j+N\text{ is odd}\\ \phi_{N-1}(0) & j=0,\ N\text{ is even}\\ \phi_{N-1}(j-1) & j\ne 0,\ j+N\text{ is even},\end{cases}\tag{20}$$

$$\psi_N(j)=\begin{cases}\psi_{N-1}(a-1) & j=a-1,\ j+N\text{ is even}\\ \psi_{N-1}(j+1) & j\ne a-1,\ j+N\text{ is even}\\ \psi_{N-1}(0) & j=0,\ N\text{ is odd}\\ \psi_{N-1}(j-1) & j\ne 0,\ j+N\text{ is odd}.\end{cases}\tag{21}$$

Thus, we can design the arrangement of cells to satisfy the local condition in the special case $b\equiv 1\,(\mathrm{mod}\,a)$. In the general case, instead of $\phi_N(j)$ and $\psi_N(j)$, we take

$$\phi_N(j;b):\equiv b^{-1}\phi_N(j),\ \psi_N(j;b):\equiv b^{-1}\psi_N(j).\tag{22}$$

If $\phi_N(j;b)=i$, then $\psi_N(j;b)=\bar{\imath}$ holds since $\bar{\imath}\equiv b^{-1}N-i\,(\mathrm{mod}\,a)$. Moreover, we claim that (20) and (21) are still valid for $\phi_N(j;b)$ and $\psi_N(j;b)$. By connecting the cells as described above with $\phi_N(j;b)$ and $\psi_N(j;b)$ in place of $\phi_N(j)$ and $\psi_N(j)$, the arrangement of cells for the local condition is obtained.

$\phi_N(j;b)$ and $\psi_N(j;b)$ have notable properties. They have a period of $2a$: $\phi_{N+2a}(j;b)=\phi_N(j;b)$ and $\psi_{N+2a}(j;b)=\psi_N(j;b)$. Furthermore, they have a kind of symmetry with respect to j in the sense that $\phi_{N+a}(j;b)=\phi_N(j^\star;b)$ and $\psi_{N+a}(j;b)=\psi_N(j^\star;b)$ with $j+j^\star=a-1$.

Table. Values of $\phi_N(j;b)$ and $\psi_N(j;b)$ with $b \equiv 3 \pmod 4$

$\phi_N(j;b)$									
$j \backslash N$	0	1	2	3	4	5	6	7	8
0	0	3	3	2	2	1	1	0	0
1	3	0	2	3	1	2	0	1	3
2	1	2	0	1	3	0	2	3	1
3	2	1	1	0	0	3	3	2	2

$\psi_N(j;b)$									
$j \backslash N$	0	1	2	3	4	5	6	7	8
0	0	0	3	3	2	2	1	1	0
1	1	3	0	2	3	1	2	0	1
2	3	1	2	0	1	3	0	2	3
3	2	2	1	1	0	0	3	3	2

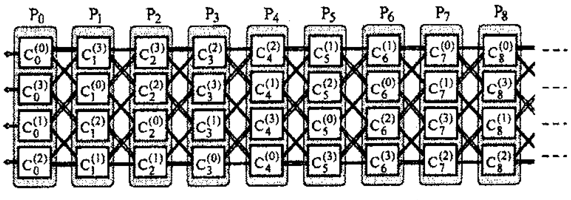


Figure. Systolic array for codes on $C_4{}^{11}$ curves

These properties are utilized in [5] to reduce the scale of the systolic array. We can interchange $\phi_N(j;b)$ and $\psi_N(j;b)$ in order that the resulting systolic array still satisfies the local condition.

Table lists the values of $\phi_N(j;b)$ and $\psi_N(j;b)$ with $b \equiv 3\,(\mathrm{mod}\,4)$. An example of the C_a^b curve with $b \equiv 3\,(\mathrm{mod}\,a)$ that attains the Hasse–Weil bound is $y^4 + y = x^{11}$ over $\mathbb{F}_{2^{10}}$, which is in Miura's list [9] of C_a^b curves having many K-rational points. In Figure, we show the cell arrangement and their connection in the systolic array constructed as above according to the values $\phi_N(j;11)$ and $\psi_N(j;11)$ in Table, where the solid and double lines express the connection according to $\phi_N(j;11)$ and $\psi_N(j;11)$, respectively.

We have applied the arrangement of cells on the three-dimensional systolic array described in [14] to our two-dimensional systolic array, as in [7][8], and extended it to the general case for b.

5. Scheduling

In this section, we describe the scheduling of data in the algorithm on the systolic array. As a result, the circuit scale of the systolic array in this section will be reduced to almost half the scale with the same running time as in [5]. Although, in [7][8], g gap-numbers $\mathbb{Z}_0 \backslash o(\Phi(a))$ were excluded from the processor numbers, we now include them in the processor numbers $0 \leq N \leq B$ in order to regularize the arrangement of cells.

We define that, for $0 \leq N \leq B$, $f_{N+1,h}^{(i)}$ and $v_{N+1,h}^{(i)}$ (resp. $g_{N+1,h}^{(i)}$ and $w_{N+1,h}^{(i)}$) are the values in K received by cell $\mathrm{C}_{N+1}^{(i)}$ from $\mathrm{C}_N^{(i)}$ (resp. $\mathrm{C}_{N+1}^{(i^*)}$ from $\mathrm{C}_N^{(i)}$) at clock $h \in \mathbb{Z}_0$. We also define that, for $N = 0$, $f_{0,h}^{(i)}$, $v_{0,h}^{(i)}$, $g_{0,h}^{(i)}$, and $w_{0,h}^{(i)}$ are the values in K inputted to cell $\mathrm{C}_0^{(i)}$ at clock $h \in \mathbb{Z}_0$.

Next, we define the coefficients $\overline{V}_{N,h}^{(i)}$, $\overline{W}_{N,h}^{(\bar{i})}$, $\overline{F}_{N,h}^{(i)}$, and $\overline{G}_{N,h}^{(\bar{i})}$ in $\overline{V}_N^{(i)}$, $\overline{W}_N^{(\bar{i})}$, $\overline{F}_N^{(i)}$, and $\overline{G}_N^{(\bar{i})}$, respectively, by

(23)

$$\overline{V}_N^{(i)} = \sum_{h=N}^{B} \overline{V}_{N,h}^{(i)} Z^h,\ \overline{W}_N^{(\bar{i})} = \sum_{h=N}^{B} \overline{W}_{N,h}^{(\bar{i})} Z^h,\ \overline{F}_N^{(i)} = \sum_{h=0}^{o(s_N^{(i)})} \overline{F}_{N,h}^{(i)} Z^h,\ \overline{G}_N^{(\bar{i})} = \sum_{h=N-M}^{o(s_M^{(j)})+N-M} \overline{G}_{N,h}^{(\bar{i})} Z^h.$$

Note that the coefficient of Z^h for $h < N$ in $\overline{V}_N^{(i)}$ has been omitted since it is not necessary in the algorithm; then, it follows from $\overline{W}_N^{(\bar{i})} = Z^{N-M}(d_M^{(j)})^{-1}\overline{V}_M^{(j)}$ that the lowest degree of Z^h in $\overline{W}_N^{(\bar{i})}$ equals N. Then, we give the scheduling for the computation of the coefficients $\overline{V}_{N,h}^{(i)}$, $\overline{W}_{N,h}^{(\bar{i})}$, $\overline{F}_{N,h}^{(i)}$, and $\overline{G}_{N,h}^{(\bar{i})}$ as follows:

$$\text{(24)} \qquad \overline{V}_{N,h}^{(i)} = v_{N,N+h}^{(i)},\ \overline{W}_{N,h}^{(\bar{i})} = w_{N,N+h}^{(\bar{i})},\ \overline{F}_{N,h}^{(i)} = f_{N,2N+h}^{(i)},\ \overline{G}_{N,h}^{(\bar{i})} = g_{N,2N+h}^{(\bar{i})}.$$

These imply that, for example, $\overline{V}_{N,h}^{(i)}$ is obtained at clock $N + h$ in $\mathrm{C}_N^{(i)}$. The validity of this scheduling follows from the recurrence formulas (25)–(30) given below and the range of h for $v_{N,h}^{(i)}$, $w_{N,h}^{(\bar{i})}$, $f_{N,h}^{(i)}$, and $g_{N,h}^{(\bar{i})}$ given later.

Thus, the updating formulas (8), (9), (14), (15), (16), and (17) are changed to the following (25), (26), (27), (28), (29) and (30), respectively.

Parallel Version of BMS Algorithm (Scheduling):
Input: $\{u_l\}$ for $l \in \Phi(2a-1, m)$.
Output: $F^{(i)}_{B+1}$ and $G^{(i)}_{B+1}$ for all $0 \le i \le a-1$.
In each step, the indicated procedures are carried out for all $0 \le i \le a-1$.

Step 0: (initializing) $N := 0$, $s^{(i)}_N := (0, i)$, $c^{(i)}_N := (-1, i)$, $f^{(i)}_{N,0} := 1$, $g^{(i)}_{N,0} := 0$, $w^{(i)}_{N,h} := 0$ $(0 \le h \le B)$;

$$v^{(i)}_{N,h} := \begin{cases} 0 & h \notin o\left(\Phi^{(i)}(a,B)\right), \\ u_{n^{(i)}} & h \in o\left(\Phi^{(i)}(a,B)\right) \text{ and } 0 \le h \le m, \\ \wp_{n^{(i)}} & h \in o\left(\Phi^{(i)}(a,B)\right) \text{ and } m < h \le B, \end{cases}$$

where $n^{(i)}$ is in $\Phi^{(i)}(a, B)$ with $h = o(n^{(i)})$, and we have $u_{n^{(i)}} = \wp_{n^{(i)}} + u_n$ for $o(n^{(i)}) = o(n)$ with $n \in \Phi(a, B)$.

Step 1: (determining the unknown syndrome, checking discrepancy) While $0 \le N \le m$, $d^{(i)}_N := v^{(i)}_{N,2N}$ if $l^{(i)}$ exists and $s^{(i)}_N \le l^{(i)}$; $d^{(i)}_N := 0$ otherwise. While $N > m$, $(\Diamond)$ is carried out for $b^{(i)}_N = v^{(i)}_{N,2N}$ and u_l is obtained. Then, $d^{(i)}_N := v^{(i)}_{N,2N} + u_l$ if $l^{(i)}$ exists and $s^{(i)}_N \le l^{(i)}$; $d^{(i)}_N := 0$ otherwise.

Step 2: (N-updating) $s^{(i)}_{N+1}$, $c^{(i)}_{N+1}$ are the same as in (2).

(25) $$f^{(i)}_{N+1,h+2} := f^{(i)}_{N,h} - d^{(i)}_N g^{(\bar{\imath})}_{N,h},$$

(26) $$g^{(\bar{\imath})}_{N+1,h+3} := \begin{cases} g^{(\bar{\imath})}_{N,h} & \text{if (P)}, \\ (d^{(i)}_N)^{-1} f^{(i)}_{N,h} & \text{otherwise :} \end{cases}$$

while $0 \le N \le m$,

(27) $$v^{(i)}_{N+1,h+1} := v^{(i)}_{N,h} - d^{(i)}_N w^{(\bar{\imath})}_{N,h},$$

(28) $$w^{(\bar{\imath})}_{N+1,h+2} := \begin{cases} w^{(\bar{\imath})}_{N,h} & \text{if (P)}, \\ (d^{(i)}_N)^{-1} v^{(i)}_{N,h} & \text{otherwise :} \end{cases}$$

while $m < N$,

(29) $$v^{(i)}_{N+1,h+1} := v^{(i)}_{N,h} + u_l f^{(i)}_{N,h} - d^{(i)}_N \left(w^{(\bar{\imath})}_{N,h} + u_l g^{(\bar{\imath})}_{N,h}\right),$$

(30) $$w^{(\bar{\imath})}_{N+1,h+2} := \begin{cases} \left(w^{(\bar{\imath})}_{N,h} + u_l g^{(\bar{\imath})}_{N,h}\right) & \text{if (P)}, \\ (d^{(i)}_N)^{-1}\left(v^{(i)}_{N,h} + u_l f^{(i)}_{N,h}\right) & \text{otherwise.} \end{cases}$$

Step 3: If $N < B$, change N to $N+1$ and go to Step 1; otherwise, stop algorithm. □

In view of the left-hand side of (25)–(30), we see that the number of registers for $v^{(i)}_{N,h}$, $w^{(i)}_{N,h}$, $f^{(i)}_{N,h}$, and $g^{(i)}_{N,h}$ in $\mathrm{C}^{(i)}_N$ must be set to one, two, two, and three, respectively. In order to complete the construction of the array, the range of h for $v^{(i)}_{N,h}$, $w^{(\bar{\imath})}_{N,h}$, $f^{(i)}_{N,h}$, and $g^{(\bar{\imath})}_{N,h}$ must be indicated. This is given from (23) as follows:

(31) $$2N \le h \le N + B \ \text{ for } v^{(i)}_{N,h} \text{ and } w^{(\bar{\imath})}_{N,h},$$

(32) $$2N \le h \le 2N + o(s^{(i)}_N) \ \text{ for } f^{(i)}_{N,h},$$

(33) $$2N + N - M \le h \le 2N + N - M + o(s^{(j)}_M) \ \text{ for } g^{(\bar{\imath})}_{N,h}.$$

The validity of the scheduling follows from the observation that the values in the right-hand side of (25)–(30) are obtained at clock h except for u_l and $d^{(i)}_N$, which are obtained at clock

$2N \leq h$, while the values in the left-hand side are obtained at clock $> h$. Thus, the systolic array consisting of $B+1$ processors has been constructed.

Appendix A. Proof of Theorem 1

Theorem 1 is proved by the following three lemmas.

Lemma 1. *Suppose that $G(z) \in V(u, M-1)$, $G_t = 1$, $dG_k \neq 0$, and $t \leq k$ with $t = \deg(G)$, $k \in \Phi^{(t_2)}(a, B)$, and $o(k) = M$. Moreover, suppose that $F(z) \in V(u, M)$ and $F_s = 1$ with $s = \deg(F)$. Then, it holds that at least one condition of $s_1 \geq k_1 - t_1 + 1$ and $s_2 \neq k_2 - t_2$.* □

Proof of Lemma 1. We suppose that $s_1 \leq k_1 - t_1$ and $s_2 = k_2 - t_2$. Since $G \in V(u, M-1)$ and $F \in V(u, M)$, we have

$$- \sum_{n \in \Phi(a,t) \setminus \{t\}} G_n u_{n+l-t} = u_l \quad \text{for} \quad l \in \Phi^{(t_2)}(a, M-1),\ t \leq l,$$
$$- \sum_{r \in \Phi(a,s) \setminus \{s\}} F_r u_{r+l-s} = u_l \quad \text{for} \quad l \in \Phi^{(s_2)}(a, M),\ s \leq l.$$

Since $n_2 + k_2 - t_2 \leq a - 1 + s_2$ and $n + k - t \geq n + s \geq s$ for $n \in \Phi(a,t)$, we have $n + k - t \in \Phi^{(s_2)}(a, M)$ and $s \leq n + k - t$ for $n \in \Phi(a, t)$, and moreover,

$$\begin{aligned} - \sum_{n \in \Phi(a,t) \setminus \{t\}} G_n u_{n+k-t} &= \sum_{n \in \Phi(a,t) \setminus \{t\}} G_n \left\{ \sum_{r \in \Phi(a,s) \setminus \{s\}} F_r u_{r+(n+k-t)-s} \right\} \\ &= \sum_{r \in \Phi(a,s) \setminus \{s\}} F_r \sum_{n \in \Phi(a,t) \setminus \{t\}} G_n u_{n+(r+k-s)-t} \\ &= - \sum_{r \in \Phi(a,s) \setminus \{s\}} F_r u_{r+k-s}, \end{aligned}$$

where the last equality follows from $r+k-s \in \Phi^{(t_2)}(a, M-1)$ and $t \leq r+k-s$ for $r \in \Phi(a,s) \setminus \{s\}$ since $r_2 + k_2 - s_2 \leq a - 1 + t_2$ and $r + k - s \geq r + t \geq t$ for $r \in \Phi(a, s)$, and the last sum agrees with u_k since $s_2 \leq k_2 = s_2 + t_2 \leq s_2 + a - 1$ and $k \in \Phi^{(s_2)}(a, M)$. This contradicts $dG_k \neq 0$. □

Lemma 2. *We have $s_{N,1}^{(i)} = c_{N,1}^{(i)} + 1$.* □

Proof of Lemma 2. We prove it by induction. The case of $N = 0$ follows from the initializing. Assuming $s_{N,1}^{(i)} = c_{N,1}^{(i)} + 1$ for all i, we prove $s_{N+1,1}^{(i)} = c_{N+1,1}^{(i)} + 1$. If there is no $l^{(i)}$, then also no $l^{(\bar{\imath})}$, and therefore, we may assume that there is $l^{(i)} = l^{(\bar{\imath})}$. It follows from the assumption of the induction that $s_{N,1}^{(i)} \geq l_1^{(i)} - c_{N,1}^{(\bar{\imath})}$ if and only if $s_{N,1}^{(\bar{\imath})} \geq l_1^{(\bar{\imath})} - c_{N,1}^{(i)}$. Thus, we may assume that $s_{N,1}^{(i)} < l_1^{(i)} - c_{N,1}^{(\bar{\imath})}$, $s_{N,1}^{(\bar{\imath})} < l_1^{(\bar{\imath})} - c_{N,1}^{(i)}$, and $d_N^{(i)} \neq 0$ without loss of generality. If $d_N^{(\bar{\imath})} = 0$, then it contradicts Lemma 1 since $F_N^{(i)} \in V(u, N-1)$, $F_N^{(\bar{\imath})} \in V(u, N)$, $s_{N,1}^{(\bar{\imath})} \leq l_1^{(i)} - s_{N,1}^{(i)}$, and $\bar{\imath} = l_2^{(i)} - i$. Thus, we obtain $d_N^{(\bar{\imath})} \neq 0$ and $s_{N+1,1}^{(i)} - c_{N+1,1}^{(i)} = s_{N,1}^{(\bar{\imath})} - c_{N,1}^{(\bar{\imath})}$. □

It follows from Lemma 2 that $\max\limits_{\leq} \left\{ s_N^{(i)}, l^{(i)} - c_N^{(\bar{\imath})} \right\} = \left(\max \left\{ s_{N,1}^{(i)}, l_1^{(i)} - s_{N,1}^{(\bar{\imath})} + 1 \right\}, i \right)$.

Lemma 3. *Let $F(z) \in V(u, N-1)$, $s \leq l$ with $s = \deg(F)$ for $l \in \Phi^{(s_2)}(a, B)$, and let $G(z) \in V(u, M-1)$, $t \leq k$ with $t = \deg(G)$ for $k \in \Phi^{(t_2)}(a, B)$. Moreover, suppose that $G \neq 0$, $dG_k = 1$, $M = o(k) < N = o(l)$ and $k_2 - t_2 = l_2 - s_2$. Then,*

$$H(z) := z^{r-s} F - dF_l z^{r-l+k-t} G \ \in V(u, N)$$

and $\deg(H) = r$*, where* $r := s$ *if* $dF_l = 0$*, and* $r := \max\limits_{\leq}\{s, l-k+t\} = (\max\{s_1, l_1 - k_1 + t_1\}, s_2)$ *otherwise.* □

Proof of Lemma 3. Since

$$o\left(z^{r-s}F\right) - o\left(z^{r-l+k-t}G\right) = r_1a + s_2b - (r_1 - l_1 + k_1)a - t_2b \tag{34}$$
$$= o(l) - o(k) > 0,$$

we obtain $\deg(H) = r$. Next, since $F \in V(u, N-1)$ and $G \in V(u, M-1)$, we have

$$\sum_{n\in\Phi(a,s)} F_n u_{n+p-s} = \begin{cases} 0 & p \in \Phi^{(s_2)}(a, N-1),\ s \leq p \\ dF_l & p = l, \end{cases}$$
$$\sum_{n\in\Phi(a,t)} G_n u_{n+p-t} = \begin{cases} 0 & p \in \Phi^{(t_2)}(a, M-1),\ t \leq p \\ 1 & p = k. \end{cases}$$

We may assume $dF_l \neq 0$. If $p \in \Phi^{(s_2)}(a, N-1)$ and $r \leq p$, then we have $p-l+k \in \Phi^{(t_2)}(a, M-1)$ and $t \leq p - l + k$, and moreover,

$$\sum_{n\in\Phi(a,r)} H_n u_{n+p-r} = \sum_{n\in\Phi(a,s)} F_n u_{n+(r-s)+p-r} - dF_l \sum_{n\in\Phi(a,t)} G_n u_{n+(r-l+k-t)+p-r}$$
$$= \sum_{n\in\Phi(a,s)} F_n u_{n+p-s} - dF_l \sum_{n\in\Phi(a,t)} G_n u_{n+(p-l+k)-t}$$
$$= \begin{cases} 0 & p \in \Phi^{(s_2)}(a, N-1),\ r \leq p \\ dF_l - dF_l \cdot 1 = 0 & p = l. \end{cases} \qquad \square$$

Proof of Theorem 1. If $d_N^{(i)} \neq 0$ and $G_N^{(\bar\imath)} = 0$, then $s_{N+1,1}^{(i)} := l_1^{(i)} + 1$ and $F_{N+1}^{(i)} := x^{l_1^{(i)}+1} F_N^{(i)}$. Thus $d_{N+1}^{(i)} = 0$ and $\deg(F_{N+1}^{(i)}) = s_{N+1}^{(i)}$ hold. Supposing that $G_N^{(\bar\imath)} \neq 0$, let M be the processor number most recently satisfying $G_N^{(\bar\imath)} := \left(d_M^{(j)}\right)^{-1} F_M^{(j)}$, $o(k^{(j)}) = M$, and $\bar\imath = k_2^{(j)} - j$, then we have $c_N^{(\bar\imath)} = k^{(j)} - s_M^{(j)}$. Thus we can prove the theorem except for (6) and (7) by using Lemma 3 since $l^{(i)} - k^{(j)} + s_M^{(j)} = l^{(i)} - c_N^{(\bar\imath)}$. The minimality (6) is proved by induction. (6) at $N := 0$ holds trivially. Supposing that the equality is true for $s_{N,1}^{(i)}$, we prove it for $s_{N+1,1}^{(i)}$. Let $\varsigma_{N,1}^{(i)}$ be the minimum of $\zeta_{N,1}^{(i)}$ in (6). If $d_N^{(i)} = 0$ or $s_N^{(i)} \leq l^{(i)} - c_N^{(\bar\imath)}$, then $s_{N,1}^{(i)} = \varsigma_{N,1}^{(i)} \leq \varsigma_{N+1,1}^{(i)} \leq s_{N+1,1}^{(i)} = s_{N,1}^{(i)}$, thus $\varsigma_{N+1,1}^{(i)} = s_{N+1,1}^{(i)}$ holds. If $d_N^{(i)} \neq 0$ and $s_N^{(i)} > l^{(i)} - c_N^{(\bar\imath)}$, we have $\varsigma_{N+1,1}^{(i)} \leq s_{N+1,1}^{(i)} = l_1^{(i)} - s_{N,1}^{(\bar\imath)} + 1$, and moreover, $d_N^{(\bar\imath)} \neq 0$ as in the proof of Lemma 2. Assuming $\varsigma_{N+1,1}^{(i)} \leq l_1^{(i)} - s_{N,1}^{(\bar\imath)}$, Lemma 1 is again applied for $F_N^{(\bar\imath)} \in V(u, N-1)$, $F \in V(u, N)$ with $\deg(F) = (\varsigma_{N+1,1}^{(i)}, i)$. Then this leads contradiction and prove $\varsigma_{N+1,1}^{(i)} = s_{N+1,1}^{(i)}$. Lastly for the proof of (7), supposing $s_{N,1}^{(i)} < s_{N,1}^{(j)}$ with $0 \leq i < j \leq a-1$, $y^{j-i}F_N^{(i)}$ is still in $V(u, N-1)$ and $\deg(y^{j-i}F_N^{(i)}) = (s_{N,1}^{(i)}, j)$, which contradicts the minimality of $s_{N,1}^{(j)}$. $\square$

We have proved Kamiya-Miura's version with no use of figures shaped by $s_N^{(i)}$ and $c_N^{(i)}$ and along with the line of the proof in [4] of Berlekamp–Massey algorithm for one-dimensional case more analogously than the original one.

Appendix B. Proof of Theorem 2

Before proving Theorem 2 for the present $\overline{V}_N^{(i)}$ and $\overline{W}_N^{(\bar{\imath})}$, we change (11) and (12) by setting $\pi := r + n - s_N^{(i)}$ and $\pi := r + n' - s_M^{(j)}$, respectively, as follows:

(35)

$$\overline{V}_N^{(i)}(Z) := \sum_{n\in\Phi^{(i)}(a,B)} \left\{ \sum_{\substack{\pi\in\Phi^{(n_2-i)}(a,n)\\ o(\pi)\le\max\{m,N-1\}}} F^{(i)}_{N.\pi-n+s_N^{(i)}} u_\pi + \sum_{\substack{m\in\Phi^{(n_2-i)}(a,n)\\ o(\pi)>\max\{m,N-1\}}} F^{(i)}_{N,\pi-n+s_N^{(i)}} \wp_\pi \right\} Z^{o(n)},$$

(36)

$$\overline{W}_N^{(\bar{\imath})}(Z) := \sum_{n'\in\Phi^{(j)}(a,B)} \left\{ \sum_{\substack{\pi\in\Phi^{(n'_2-j)}(a,n')\\ o(\pi)\le\max\{m,N-1\}}} G^{(\bar{\imath})}_{N,\pi-n'+s_M^{(j)}} u_\pi + \sum_{\substack{\pi\in\Phi^{(n'_2-j)}(a,n')\\ o(\pi)>\max\{m,N-1\}}} G^{(\bar{\imath})}_{N,\pi-n'+s_M^{(j)}} \wp_\pi \right\} Z^{o(n')+N-M}.$$

Note that, if $c_{N,1}^{(\bar{\imath})} \neq -1$ and $n := n' + l^{(i)} - k^{(j)} \in \Phi^{(i)}(a,B)$ with $o(l^{(i)}) = N$ and $o(k^{(j)}) = M$ in (36), the coefficient of $Z^{o(n')+N-M} = Z^{o(n)}$ equals

(37)
$$\sum_{\substack{\pi\in\Phi^{(n_2-i)}(a,n)\\ o(\pi)\le\max\{m,N-1\}}} G^{(\bar{\imath})}_{N,\pi-n+l^{(i)}-c_N^{(\bar{\imath})}} u_\pi + \sum_{\substack{\pi\in\Phi^{(n_2-i)}(a,n)\\ o(\pi)>\max\{m,N-1\}}} G^{(\bar{\imath})}_{N,\pi-n+l^{(i)}-c_N^{(\bar{\imath})}} \wp_\pi$$

since $c_N^{(\bar{\imath})} = k^{(j)} - s_M^{(j)}$, $n'_2 - j = n_2 - l_2^{(i)} + k_2^{(j)} - j = n_2 - i$, and $G^{(\bar{\imath})}_{N,\pi-n+l^{(i)}-c_N^{(\bar{\imath})}} := 0$ for $\pi \in \Phi^{(n_2-i)}(a,n)$ with $o(\pi) > o(n')$.

Proof of Theorem 2. The coefficient of $z^{\pi-n+s_{N+1}^{(i)}}$ in $F_{N+1}^{(i)}(z)$ equals

$$F^{(i)}_{N,\pi-n+s_N^{(i)}} - d_N^{(i)} G^{(\bar{\imath})}_{N,\pi-n+l^{(i)}-c_N^{(\bar{\imath})}},$$

which is regarded as $F^{(i)}_{N,\pi-n+s_N^{(i)}}$ if $l^{(i)}$ does not exist. Substituting this into (35) for $\overline{V}_{N+1}^{(i)}$, the contribution of $F^{(i)}_{N,\pi-n+s_N^{(i)}}$ equals

$$\sum_{\substack{\pi\in\Phi^{(n_2-i)}(a,n)\\ o(\pi)\le\max\{m,N\}}} F^{(i)}_{N,\pi-n+s_N^{(i)}} u_\pi + \sum_{\substack{\pi\in\Phi^{(n_2-i)}(a,n)\\ o(\pi)>\max\{m,N\}}} F^{(i)}_{N,\pi-n+s_N^{(i)}} \wp_\pi.$$

If $N \le m$, that is, $\max\{m,N\} = m$, then this agrees with the coefficient of $Z^{o(n)}$ in $\overline{V}_N^{(i)}$ at (35). If $N > m$, that is, $\max\{m,N\} = N$ and $\max\{m,N-1\} = N-1$, then this agrees with

$$\sum_{\substack{\pi\in\Phi^{(n_2-i)}(a,n)\\ o(\pi)\le N-1}} F^{(i)}_{N,\pi-n+s_N^{(i)}} u_\pi + \sum_{\substack{\pi\in\Phi^{(n_2-i)}(a,n)\\ o(\pi)>N-1}} F^{(i)}_{N,\pi-n+s_N^{(i)}} \wp_\pi + u_l F^{(i)}_{N,l^{(n_2-i)}-n+s_N^{(i)}},$$

where the last term is regarded as zero if there is no $l^{(n_2-i)} \in \Phi^{(n_2-i)}(a,n)$ with $o(l^{(n_2-i)}) = N$. Since $o\left(l^{(n_2-i)} - n + s_N^{(i)}\right) = N + o(s_N^{(i)}) - o(n)$, $u_l F^{(i)}_{N,l^{(n_2-i)}-n+s_N^{(i)}}$ is the coefficient of $Z^{o(n)}$ in $u_l Z^N \overline{F}_N^{(i)}$. Similarly, the contribution of $G^{(\bar{\imath})}_{N,\pi-n+l^{(i)}-c_N^{(\bar{\imath})}}$ equals

$$\sum_{\substack{\pi\in\Phi^{(n_2-i)}(a,n)\\ o(\pi)\le\max\{m,N\}}} G^{(\bar{\imath})}_{N,\pi-n+l^{(i)}-c_N^{(\bar{\imath})}} u_\pi + \sum_{\substack{\pi\in\Phi^{(n_2-i)}(a,n)\\ o(\pi)>\max\{m,N\}}} G^{(\bar{\imath})}_{N,\pi-n+l^{(i)}-c_N^{(\bar{\imath})}} \wp_\pi.$$

If $N \leq m$, then this agrees with the coefficient of $Z^{o(n)}$ in $\overline{W}_N^{(\bar{i})}$ at (36), as noted there. If $N > m$, then this agrees with

$$\sum_{\substack{\pi \in \Phi^{(n_2-i)}(a,n) \\ o(\pi) \leq N-1}} G^{(\bar{i})}_{N,\pi-n+l^{(i)}-c_N^{(\bar{i})}} u_\pi + \sum_{\substack{\pi \in \Phi^{(n_2-i)}(a,n) \\ o(\pi) > N-1}} G^{(\bar{i})}_{N,\pi-n+l^{(i)}-c_N^{(\bar{i})}} \wp_\pi + u_l G^{(\bar{i})}_{N,l^{(n_2-i)}-n+l^{(i)}-c_N^{(\bar{i})}}.$$

Since $o\left(l^{(n_2-i)} - n + l^{(i)} - c_N^{(\bar{i})}\right) = N + o(s_M^{(j)}) - o(n) + N - M$, $u_l G^{(\bar{i})}_{N,l^{(n_2-i)}-n+l^{(i)}-c_N^{(\bar{i})}}$ is the coefficient of $Z^{o(n)}$ in $u_l Z^N \overline{W}_N^{(\bar{i})}$; thus (14) and (16) are proved. (15) and (17) are verified in a similar manner. □

References

[1] D. Cox, J. Little, and D. O'Shea, *Ideals, varieties, and algorithms,* UTM Springer–Verlag, 1992.

[2] N. Kamiya, S. Miura, "On a recursive decoding algorithm for codes defined on algebraic curves with at most one higher order cusp," (Japanese) *Trans. IEICE,* J76–A, no. 3, pp.480–492, 1993.

[3] R. Kötter, "A fast parallel implementation of a Berlekamp–Massey algorithm for algebraic-geometric codes," *IEEE Trans. Inf. Theory,* vol.44–4, pp.1353–1368, 1998.

[4] J. L. Massey, "Shift-register synthesis and BCH decoding," *IEEE Trans. Inf. Theory,* vol.IT-15, pp.122–127, 1969.

[5] H. Matsui, "A method to reduce the circuit scale of systolic array for BMS algorithm," (Japanese) *Proc. The 26th Symposium on Information Theory and Its Applications,* pp.457–460, Dec. 17, 2003.

[6] H. Matsui, S. Sakata, S. Mita "Determination of unknown syndromes in parallel decoding of codes from algebraic curves with systolic array," (Japanese) *Trans. IEICE,* J85–A, no. 4, pp.460–470, 2002.

[7] H. Matsui, N. Matsunagi, S. Mita, "Construction of decoder for codes on algebraic curves and its performance estimation," *Proc. International Symposium on Information Theory and Its Applications,* pp.411–414, Xi'an, China, Oct. 9, 2002.

[8] H. Matsui, S. Mita "Parallel decoding of codes on a class of algebraic curves using two-dimensional systolic array," (Japanese) *Trans. IEICE,* J86–A, no. 9, pp.945–956, 2003.

[9] S. Miura, "Algebraic geometric codes on certain plane curves," (Japanese) *Trans. IEICE,* J75–A, no. 11, pp.1735–1745, 1992.

[10] M. E. O'Sullivan, "On Koetter's algorithm and the computation of error values," *Designs, Codes and Cryptography,* vol.31, pp.169–188, 2004.

[11] S. Sakata, "Finding a minimal set of linear recurring relations capable of generating a given finite two dimensional array," *Journal of Symbolic Computation,* No.5, pp.321–337, Nov. 1988.

[12] S. Sakata, "A vector version of the BMS algorithm for implementing fast erasure-and-error decoding of one-point AG codes," *Proc. AAECC-12, Lecture Notes in Computer Science,* vol.1255, pp.291–310, Springer Verlag, 1997.

[13] S. Sakata, H. Elbrønd Jensen, and T. Høholdt, "Generalized Berlekamp–Massey decoding of algebraic geometric code up to half the Feng–Rao bound," *IEEE Trans. Inf. Theory,* vol.41, No.6, Part I, pp.1762–1768, Nov. 1995.

[14] S. Sakata and M. Kurihara, "A systolic array architecture for fast decoding of one-point AG codes and scheduling of parallel processing on it," *Proc. AAECC-13, Lecture Notes in Computer Science,* vol. 1719, pp.302–313, Springer Verlag, 1999.

松井 一 (Hajime MATSUI)
豊田工業大学電子情報系 (Electronics and Information Science, Toyota Technological Institute)
468-8511 名古屋市天白区久方 2-12-1 (2-12-1 Hisakata, Tenpaku-ku, Nagoya 468-8511, Japan)
e-mail address: **hmatsui@toyota-ti.ac.jp**

阪田 省二郎 (Shojiro SAKATA), 栗原 正純 (Masazumi KURIHARA)
電気通信大学情報通信工学科 (Department of Information and Communication Engineering, The University of Electro-Communications)
182-8585 東京都調布市調布ヶ丘 1-5-1 (1-5-1 Chofugaoka, Chofu-shi, Tokyo 182-8585, Japan)