ERROR CORRECTING SEQUENCE AND PROJECTIVE DE BRUIJN GRAPH

MARIKO HAGITA, MAKOTO MATSUMOTO, FUMIO NATSU, AND YUKI OHTSUKA

ABSTRACT. Let X be a finite set of q elements, and n, K, d be integers. A subset $C \subset X^n$ is an (n, K, d) error-correcting code, if $\#(C) = K$ and its minimum distance is d. We define an (n, K, d) error-correcting sequence over X as a periodic sequence $\{a_i\}_{i=0,1,\ldots}$ $(a_i \in X)$ with period K, such that the set of all consecutive n-tuples of this sequence form an (n, K, d) error-correcting code over X. Under a moderate conjecture on the existence of some type of primitive polynomials, we prove that there is a $(\frac{q^m-1}{q-1}, q^{\frac{q^m-1}{q-1}-m}-1, 3)$ error correcting sequence, such that its code-set is the q-ary Hamming code $[\frac{q^m-1}{q-1}, \frac{q^m-1}{q-1}-m, 3]$ with 0 removed, for $q > 2$ being a prime power. For the case $q = 2$, under a similar conjecture, we prove that there is a $(2^m - 2, 2^{2^m-m-2} - 1, 3)$ error-correcting sequence, such that its code-set supplemented with 0 is the subset of the binary Hamming code $[2^m - 1, 2^m - 1 - m, 3]$ obtained by requiring one specified coordinate being 0.

Keywords: error-correcting code, Hamming code, m-sequence, de Bruijn graph, projective de Bruijn graph.

1. INTRODUCTION

Let X be a q-element set. Let us consider the problem of synchronization through a noisy channel. The sender is sending a periodic sequence $S := a_0, a_1, \ldots \in X$ of period K, one element per unit time. A receiver starts to receive the sequence from some time, say, $a_s, a_{s+1}, \ldots$. Assume that the receiver received n consecutive elements. If no errors occur, then the received word is $(a_s, a_{s+1}, \ldots, a_{s+n-1})$ for some s, but through the noisy channel, there may be some errors. The receiver wants to recover the original n-tuple from the received n-tuple with some possible errors, similarly to the error-correcting codes.

We use standard terminologies for the error correcting codes, see [8] [1]. Hamming distance $d_H(c, c')$ for $c, c' \in X^n$ is defined as the number of positions for which the corresponding components of c and c' are different. A subset $C \subset X^n$ is called an (n, K, d) error-correcting code, if $\#(C) = K$ and

Dedicated to Professor Hikoe Enomoto on the occasion of his sixtieth birthday. This study is supported by JSPS/MEXT Grant-in-Aid for Scientific Research (No. 18654021, 18740044, 16204002, and 19204002), and JSPS Core-to-Core Program No. 18005.

its minimum distance defined by

$$\delta(C) := \min\{d_H(c, c') | c, c' \in C, c \neq c'\}$$

is d. It is convenient to define $\delta(C) = 0$ if C is a multi-set having some element with multiplicity. In the case of a linear code with $X = \mathbb{F}_q$, the common notation of $[n, k, d]$ linear codes is an (n, q^k, d) code in the notation here.

For the above sequence S, we define its multi-set of consecutive n-tuples in one period by

$$S^{(n)} := \{(a_i, a_{i+1}, \ldots, a_{i+n-1}) | i = 0, 1, \ldots, K-1\}. \quad (1)$$

Often, we consider $S^{(n)}$ as a cyclic sequence of elements in X^n, not merely as a set.

Let d be $\delta(S^{(n)})$. We call S *an* (n, K, d) *error-correcting sequence over* X. Thus, $d \geq 1$ is equivalent to that $S^{(n)}$ has no multiple elements. If $d \geq 2e + 1$, then one can correct up to e errors in a k-tuple, so the sequence is said to be e-error correcting.

Example 1. *For a cyclic* (v, k, λ) *difference set* D*, the binary (i.e.* $X = \{0, 1\}$*) sequence* $a_0 a_1 \cdots$ *defined by*

$$i \in D \Leftrightarrow a_j = 1 \text{ for } j = i \bmod v$$

is a binary $(v, v, 2k - 2\lambda)$ *error-correcting sequence.*

If $n' \geq n$, then an (n, K, d) error-correcting sequence is an (n', K, d') error-correcting sequence for some $d' \geq d$. We desire larger K, larger d, and smaller n, similarly to the error-correcting codes.

2. De Bruijn graph and de Bruijn sequence

Let S be an $(n, K, 1)$-error-correcting sequence. This means that $S^{(n)}$ has no multiplicity. The q-ary de Bruijn graph $D(q, n)$ of degree n is a directed graph (with loops and multiple arcs allowed) whose vertex set is X^n and a vertex $(x_1, \ldots, x_n)$ is joined by an arrow to $(x_2, \ldots, x_n, y)$ for every $y \in X$ [2]. A sequence S of period K gives a closed walk whose vertices are $S^{(n)}$ in $D(q, n)$, by taking consecutive n tuples in S for one period. By definition, S is an $(n, K, 1)$ error-correcting sequence if and only if $S^{(n)}$ is a cycle (i.e. no vertices appear more than once).

For fixed q and n, the period K is bounded by $K \leq q^n$, since the cycle length is bounded by the number of the vertices. If the equality holds, then S is called a q-ary de Bruijn sequence of degree n. This is equivalent to that $S^{(n)}$ gives a Hamiltonian cycle of $D(q, k)$.

The number of de Bruijn sequences is known ([2] for binary case, and [5] for the general case).

Theorem 1. *There exist* $(q!)^{q^{n-1}} q^{-n}$ *de Bruijn sequences of degree* k *on a* q*-element set.*

3. LINEAR RECURRING SEQUENCE WITH $d \geq 3$

We study when a linear recurring sequence is an error correcting sequence with $d \geq 3$. From now on, we assume that X is a finite field $\mathbb{F}_q$. Let k be an integer, and $c_0, c_1, \dots c_{k-1}, c_k \in \mathbb{F}_q$ are constant with $c_k = 1$. Consider the following linear recurrence

$$a_{j+k} = -\sum_{0 \leq i \leq k-1} c_i a_{i+j} \quad (j = 0, 1, \dots), \tag{2}$$

which is denoted by $L(c_0, c_1, \dots, c_{k-1})$ or $L_k(\mathbf{c})$ where $\mathbf{c} = (c_0, c_1, \dots, c_{k-1})$. If $\mathbf{c}$ is clear from the context, we denote simply L_k. There is a unique solution for given initial vector $(a_0, a_1, \dots, a_{k-1})$. We always assume $c_0 \neq 0$. Then, the sequence defined by (2) is purely periodic. The characteristic polynomial of the recurrence (2) is

$$\chi_{\mathbf{c}}(t) = \sum_{0 \leq i \leq k} c_i t^i.$$

It is known that the maximum period of (2) is $q^k - 1$. Such a sequence exists for any prime power q and any positive integer k, and it is called an *m-sequence of degree k* over $\mathbb{F}_q$ [3]. The characteristic polynomial of an m-sequence is called a primitive polynomial.

Let $S_0, S_1, \dots, S_{r-1}$ be the set of all possible cyclic sequences generated by the linear recursion L_k. Here, we do not distinguish the starting point of the cyclic sequences. These give a partition of the vertices of $D(q, n)$ into cycles $S_0^{(n)}, S_1^{(n)}, \dots, S_{r-1}^{(n)}$. Since $\{0\}$ is a solution of (2), we may assume that $S_0^{(n)} = \{(0, 0, \dots, 0)\}$. The m-sequence property is equivalent to the condition $r = 2$.

Fix an integer $n > k$. The *n-dimensional parity check matrix* $P_n(L_k)$ of the recursion $L_k = L_k(\mathbf{c})$ is an $(n-k) \times n$ matrix defined by:

$$P_n(L_k) := \begin{pmatrix} c_0 & c_1 & c_2 & \dots & \dots & \dots & c_k & 0 & 0 & \dots & 0 \\ 0 & c_0 & c_1 & c_2 & \dots & \dots & \dots & c_k & 0 & \dots & 0 \\ 0 & 0 & c_0 & c_1 & c_2 & \dots & \dots & \dots & c_k & \dots & 0 \\ \vdots & & \ddots & & & & & \dots & \ddots & & \vdots \\ 0 & 0 & \dots & 0 & c_0 & c_1 & c_2 & \dots & \dots & \dots & c_k \end{pmatrix}.$$

Its top row is $c_0, \dots, c_k$ with $n-k$ zeros added at the right. By the definition of S_i, we have

$$\ker P_n(L_k(\mathbf{c})) = \coprod_{i=0}^{r-1} S_i^{(n)}. \tag{3}$$

We call this *the linear code of length n associated with the recursion L_k*, and denote $C_n(L_k)$.

Lemma 2. *Let L_k be a linear recursion (2). Its associated linear code $C_n(L_k)$ is an $(n, 2^k, d)$ code with $d \geq 3$ if and only if every pair of columns*

in $P_n(L_k)$ is linearly independent. In this case, every solution S_i of the linear recursion is an $(n, \#(S_i), d_i)$ error correcting sequence with $d_i \geq 3$.

Proof. It is easy to check that the condition on $P_n(L_k)$ is equivalent to that $\delta(\ker P_n(L_k)) \geq 3$ (see Theorem 1.31 in [1]). Thus, the lemma follows from (3). □

4. Projective version of de Bruijn graph

Again consider the linear recursion L_k as in (2). We would like to show that there is a linear recursion L_k whose associated code is a Hamming code, by graph theoretic arguments.

For a given $n > k$, let $T_n(L_k)$ be a periodic sequence with period n obtained by repeating the bottom row $(0, 0, \ldots, 0, c_0, c_1, \ldots, c_{k-1}, 1)$ of P_n. We call $T_n(L_k)$ the *associated sequence of period n* to L_k. Lemma 2 says that $\delta(C(L_k)) \geq 3$ holds if and only if the vectors in $T_n(L_k)^{(n-k)}$ are all non-zero and distinct each other in the $(n-k-1)$-dimensional projective space $P^{n-k-1}(\mathbb{F}_q)$.

This leads us to define a projective version of de Bruijn graphs.

Definition 3. *Suppose $X = \mathbb{F}_q$ and let m be a positive integer. The q-ary projective de Bruijn graph $PD(q, m)$ of degree m is a directed graph with loops and multiple edges allowed, whose vertex set consists of the points in the $(m-1)$-dimensional projective space*

$$P^m(\mathbb{F}_q) := \{[x_1 : \cdots : x_m] | x_i \in \mathbb{F}_q, (x_1, \ldots, x_m) \neq (0, \ldots, 0)\}$$

with a formal element $O_m = [0 : 0 : \cdots : 0]$ supplemented. Here, $[x_1 : \cdots : X_m]$ denotes the ratio of m elements. The arc set A_m consists of the points of m-dimensional projective space with $O_{m+1} = [0 : \cdots : 0]$ supplemented. The origin (the target) of an arc $[x_1 : \cdots : x_{m+1}]$ is the vertex $[x_1 : \cdots : x_m]$ ($[x_2 : \cdots : x_{m+1}]$, respectively).

The following is immediate.

Lemma 4. *Let S be a sequence $\{a_i\}_{i=0,1,\ldots}$ $(a_i \in \mathbb{F}_q)$ with period K. Define a sequence of vertices of $PD(q, m)$ by*

$$S^{[m]} := \{[a_i : a_{i+1} : \ldots : a_{i+m-1}] \in P^{m-1}(\mathbb{F}_q) | i = 0, 1, \ldots, P-1\}.$$

This gives a closed walk in $PD(q, m)$ of length K, where $[a_i : a_{i+1} : \ldots : a_{i+m}]$ are the set of arcs of this walk.

The observation at the beginning of this section now gives the following.

Theorem 5. *Let L_k be a linear recurrence as in (2), with $c_0 \neq 0$, $c_k = 1$. Let $T_n(L_k)$ be the sequence of period n obtained by repeating the length-n sequence $(0, 0, \ldots, 0, c_0, c_1, \ldots, c_k)$, as above. Then, $\delta(C_n(L_k)) \geq 3$ holds if and only if $T_n(L_k)^{[n-k]}$ is a cycle (i.e. passes every vertex at most once).*

We introduce three special vertices of $PD(q, m)$: $O := [0 : \cdots : 0]$, $O1 := [0 : \cdots : 0 : 1]$, and $1O := [1 : 0 : \cdots : 0]$.

Theorem 6. *Let n, k be integers. The above correspondence $(c_0, \dots, c_k) \mapsto T_n(L_k)^{[n-k]}$ gives a bijection from the set of linear recurring sequences L_k over $\mathbb{F}_q$ of degree k with $\delta(C(L_k)) \geq 3$ to the set of length-n cycles of $PD(q, n-k)$ which passes $1O$ but avoids O.*

Proof. It suffices to construct the inverse mapping. Namely, let C be such a cycle. We form a sequence $\{c_i\}$ of period n from such a cycle, such that its associated T_n satisfies $T_n^{[n-k]} = C$. By the assumption, C has the vertex $1O = [1 : 0 : 0 : \cdots : 0] \in PD(q, n-k)$. The previous vertex in this directed cycle should have the form $[x : 1 : 0 : \cdots : 0]$, for uniquely determined x'. We define c_{k-1} to be x. Then, its previous vertex should have the form $[x' : c_{k-1} : 1 : 0 : \cdots : 0]$. The unique solution x' gives c_{k-1}. We can determine inductively $c_{k-1}, c_{k-2}, \dots, c_0, c_{-1}, c_{-2}, c_{-3}, \dots$, until we have $n-k-1$ consecutive zeroes. However, since the cycle contains one unique $1O$ in one period and avoids O, we will not reach to such consecutive zeroes before one period. Since the length of the cycle is n, we notice that $[c_{-n+k} : \cdots : c_{-2} : c_{-1}] = [c_k : 0 : \cdots : 0]$. This forces $c_{-1} = c_{-2} = \cdots = c_{-n+k-1} = 0$. Since $c_k = 1$, the solution c_{-n+k} of this equation is an arbitrary nonzero elements. We choose $c_{-n+k} = 1$, and proceed in the same way again. Now we have a periodic sequence T_n with $T_n^{[n-k]}$ being the original cycle. □

Projective de Bruijn graphs have rather different properties from de Bruijn graphs (except for the case $q = 2$ where they are isomorphic), as remarked in the following.

Remark 7.

- *It is not generally true that a cycle of $PD(q, m)$ of length n is realized as $S^{[m]}$ for S with period n. In the above proof, the solution c_{-n+k} may be different from c_k if we do not start from $1O \in C$.*
- *$PD(q, m)$ is nearly regular, but not exactly, for $q > 2$. Every vertices have q incoming arcs and q outgoing arcs, except that O has two incoming arcs and two outgoing arcs (it has one loop).*
- *The line digraph of $PD(q, m)$ is nearly isomorphic, but not exactly, to $PD(q, m+1)$. Clearly, the arc set of the former coincides with the vertex set of the latter. Two connecting arcs $[x_1 : \cdots : x_m]$, $[x_2 : \cdots : x_{m+1}]$ in the former gives an arc $[x_1 : \cdots : x_{m+1}]$. This arc is unique except for the case of $x_2 = x_3 = \cdots = x_m = 0$. In this exception, we have $q-1$ different arcs $[1 : 0 : \cdots : 0 : x]$ $(x \in {\mathbb{F}_q}^\times)$ in $PD(q, m+1)$, for the one arc of the line digraph of $PD(q, m)$. Thus, $PD(q, m+1)$ is obtained by splitting this one arc to $(q-1)$ parallel arcs in the line digraph.*

However, the following holds.

Theorem 8. *A circuit of $PD(q, m)$ (i.e. a closed walk that passes any arc at most once) is in one-to-one correspondence with the set of cycles of*

$PD(q, m+1)$. The correspondence is given through the identification of the arc set of $PD(q, m)$ and the vertex set of $PD(q, m+1)$.

Here, we do not distinguish two cycles with same ordering of the same vertices, which may arise because of the multiple arcs.

Proof. Since the set of arrows of $PD(q, m)$ is the set of arcs of $PD(q, m+1)$, we only need to prove that the adjacency condition as arcs in $PD(q, m)$ is equivalent to that of vertices in $PD(q, m+1)$, but this was seen in Remark 7, in the comparison with the line digraph. □

Theorem 9. *There is a cycle of $PD(q, m)$ that passes all the vertices of $PD(q, m)$ except O.*

Proof. By Theorem 8, it suffices to show that there is a circuit that passes all the arcs of $PD(q, m-1)$ (i.e. Eulerian circuit), because then it corresponds to a cycle in $PD(q, m)$ that passes all the vertices. We can skip O, by changing the length two subpath $1O, O, O1$ of the circuit into a shortcut arc $1O, O1$.

Now, each vertex has the same number of the incoming arcs and the outgoing arcs. Clearly $PD(q, m-1)$ is connected, so there is an Eulerian cycle of $PD(q, m-1)$ by the standard theorem. □

5. Construction a la Hamming Code

Consider the linear recursion $L_k = L_k(\mathbf{c})$ as in (2).

Theorem 10. *The linear code $C_n(L_k)$ is a q-ary $[n, k, d]$ Hamming code if and only if $T_n^{[n-k]}$ is a cycle passing all the vertices of $PD(q, n-k)$ except O (and automatically, $(q^{n-k}-1)/(q-1) = n$ must hold). By using a new parameter $m = n-k$, this is a q-ary $[(q^m-1)/(q-1), (q^m-1)/(q-1)-m, 3]$ Hamming code. For any $\mathbb{F}_q$ and m, such a linear recursion exists. The number of such recursions is the number of Hamiltonian cycles in $PD(q, (q^m-1)/(q-1))$.*

Proof. By the definition of the Hamming code, $C_n(L_k) = \ker P_n(L_k)$ is a Hamming code if and only if the columns of $P_n(L_k)$ gives a complete representing system of the points of projective space. By Theorem 5, this is equivalent to that $T_n(L_k)^{[n-k]}$ is a Hamiltonian cycle of $PD(q, n-k)$ with O removed, which proves the first statement. Since the cycle length is the number of points $(q^{n-k}-1)/(q-1)$ in the projective space, by putting $m := n-k$, we have the second statement. The number of such recurrences is same with the number of Hamiltonian cycles by Theorem 8 (note that for any Hamiltonian cycle of $PD(q, m)$, one can remove O by a short cut, as remarked above). The existence is shown by Theorem 9. □

Corollary 11. *The number of linear recursions satisfying the condition in the above theorem is $2^{2^{n-1}-n}$ if $q = 2$. It is at least $((q-1)!)^{(q^{m-1}-1)/(q-1)}$ for general q.*

Proof. For the case $q = 2$, the projective de Bruijn graph is same with the de Bruijn graph, and the statement follows from Theorem 1. For the general case, the second statement follows from the next theorem. □

Theorem 12. *Let D be a digraph with p vertices. Assume that each vertex i $(1 \leq i \leq p)$ has the same number d_i of incoming arcs and outgoing arcs. Assume that D is strongly connected. Then, there are at least $\prod_{i=1}^{p}((d_i-1)!)$ different Eulerian circuits in D.*

Proof. We observe that, if we specify a bijection from incoming arcs to the outgoing arcs at every vertex, then we specify a decomposition of the arc set into disjoint circuits. Conversely, if we have such a decomposition, we can specify a bijection at every vertex, which we call the switching specified the circuit decomposition.

Since it is strongly connected and the incoming degree equals the outgoing degree, there is a Eulerian circuit C. It specifies a bijection at every vertex, as above. On the other hand, C specifies a bijection from the outgoing arcs to the incoming arcs at every vertex: for an outgoing arc from the vertex 1, we proceed along C, until returning to the same vertex 1 at the first time. This specifies a bijection from the outgoing arcs to the incoming arcs. By the Eulerian property, this bijection composed with the bijection specified by C at 1 gives a cyclic permutation. If we change the switching of C at the vertex 1 so that the composition is again a cyclic permutation, then it results in another (different) Eulerian circuit.

At the vertex 1, we have $(d_1 - 1)!$ different switchings that gives different Eulerian circuits. For each of these, we have $(d_2 - 1)!$ different switching at 2, each of which gives different Eulerian circuits. By continuing this process, we will have the desired number of distinct Eulerian circuits. □

Remark 13. *The number of Eulerian circuits in the line digraph is studied in* [5] [4]*, and it is plausible that one can get a closed formula for the number of such circuits for projective de Bruijn graphs.*

6. Error-correcting m-sequence

We consider the case where the linear recursion L_k gives an m-sequence, namely, its period is the maximum possible value $q^k - 1$. It is well known that the number of primitive polynomials of degree k is $\varphi(q^k - 1)/k$ (see for example [7]).

Conjecture 1. *Let $\mathbb{F}_q$ be a finite field with $q \geq 3$, and $m \geq 2$ be an integer. Then, there exists a linear recursion L_k of degree $k := (q^m - 1)/(q - 1) - m$, whose characteristic polynomial is primitive and $T_n(L_k)^{[n-k]}$ is Hamiltonian in $PD(q, n - k)$ minus O for $n := (q^m - 1)/(q - 1)$.*

This conjecture comes from our heuristic expectation that "the Hamiltonian property is independent of the primitivity," so the number of such

linear recursion is approximately the number of Hamiltonian cycles times $\frac{\varphi(q^k-1)/k}{q^{k-1}}$, which quickly increases by Corollary 11.

Now Theorem 10 and Lemma 2 imply the following.

Theorem 14. *If Conjecture 1 is true, then there is a* $(\frac{q^m-1}{q-1}, q^{\frac{q^m-1}{q-1}-m}-1, 3)$ *error correcting sequence, such that it is an* m*-sequence of degree* $\frac{q^m-1}{q-1}-m$ *and its code-set is the* q*-ary Hamming code* $[\frac{q^m-1}{q-1}, \frac{q^m-1}{q-1}-m, 3]$ *with* 0 *removed.*

In the case of $q = 2$, the above conjecture is not true. The number of 1's in a de Bruijn sequence is even, and this implies that if $T_n(L_k)^{[n-k]}$ is a Hamiltonian cycle, then the characteristic polynomial of L_k is divisible by $t-1$, and thus it can not be primitive. Instead, we have the following conjecture.

Conjecture 2. *Let* $\mathbb{F}_2$ *be the two element field, and* $m \geq 2$ *be an integer. Then, there exists a linear recursion* L_k *of degree* $k := 2^m - 2 - m$*, whose characteristic polynomial is primitive and* $T_n(L_k)^{[n-k]}$ *is a Hamiltonian cycle in* $PD(q, n-k)$ *with* O *and* $[1:1:\cdots:1]$ *removed, for* $n := 2^m - 2$*.*

The motivation of this modification from Conjecture 1 is that we have to abandon the Hamiltonian property, and a cycle which is one shorter length can be obtained by only bypassing the vertex $[1:\cdots:1]$.

Now Theorem 10 and Lemma 2 imply the following.

Theorem 15. *If Conjecture 2 is true, then there is a* $(2^m-2, 2^{2^m-2-m}-1, 3)$ *error correcting sequence, such that it is an* m*-sequence of degree* 2^m-2-m*.*

Note that the set of columns of its parity check matrix P_{2^m-2} is the set of vectors in ${\mathbb{F}_2}^m$ with O and $(1, 1, \ldots, 1)$ removed. If we supplement the transposition of this vector as a column to P_{2^m-2}, we have a Hamming code. Thus, the code-set of such an error-correcting sequence is obtained by taking the subset of the Hamming code where the component corresponding to $(1, \ldots, 1)$ is zero.

Example 2 $(m = 3)$**:** $x^3 + x + 1$ is a primitive polynomial of degree $k = 2^3-2-3 = 3$ whose coefficients give an example of Theorem 15. This is because by supplying $m-1$ zeroes at the left, 001011 gives a Hamiltonian cycle of $D(2, 3)$ minus O and $(1, 1, 1)$. Consequently, the corresponding m-sequence 0010111 is a $(6, 7, 3)$ error-correcting sequence.

Example 3 $(m = 4)$ **:** 10011010111 is the coefficients of a primitive polynomial of degree $k = 2^4 - 2 - 4 = 10$, and by supplying $m-1$ zeroes at the left, we have an example of a Hamiltonian cycle of $D(2, 4)$ minus O and $(1, 1, 1, 1)$. Consequently, the corresponding m-sequence is a $(14, 1023, 3)$ error-correcting sequence.

Theorem 15 gives a recipe to find a one-error-correcting m-sequence as follows. First, find a de Bruijn sequence of degree m. Then, remove the pattern

of $(0, 0, \ldots, 0)$ consisting of m consecutive zeros, and remove one 1 from the m consecutive 1s in the de Bruijn sequence. This results in a bit sequence of length $2^m - 1 - m$, started from 1 and end at 1. This gives a polynomial of degree $2^m - 2 - m$. If this is primitive, then the corresponding m-sequence is one-error correcting with code length $n = 2^m - 2$.

We have the following computational results for $m = 5, 6, 7$.

Theorem 16. *($m = 5, 6, 7$) For $m = 5$, there are 2048 de Bruijn sequences, and 316 of them are primitive??? (i.e. satisfies the condition of Theorem 15).*

For $m = 6$, there are $2^{2^{6-1}-6} = 2^{26}$ de Bruijn sequences. Since it is difficult to obtain and check all these, we randomly generated 1000 such sequences, and checked that 34 of the first found 1000 were primitive.

For $n = 7$, there are $2^{2^{7-1}-7} = 2^{57}$ de Bruijn sequences. we randomly generated 3000, and 91 of them were primitive.

7. DECODING

To correct 1-error of n-tuples of m-sequences in Theorems 14 and 15, one may use the standard method based on the parity check matrix P_n. We compute the syndrome $P_n\mathbf{x}$ for the obtained word $\mathbf{x}$. If it is 0 we guess that there is no error. It it is not 0, then we need to find the column of P_n which coincides with the syndrome, then the position of that column among the n columns gives the place of the error. This might be non trivial if n is large, but in software we may construct a lookup table.

It seems difficult to obtain the place of the sequence, namely, to compute s such that $(a_s, a_{s+1}, \ldots, s_{s+n-1}) = \mathbf{x}$, since this is nothing but the discrete log problem. But for some application, it suffices to correct the error, such as synchronization.

Acknowledgement. The first paper published by the second author was also about line digraphs and de Bruijn graphs [6], and Professor Hikoe Enomoto helped that study greatly. It has passed 20 years. We would like to dedicate this study to his sixtieth birthday.

References

[1] R. R. Berlekamp, Algebraic coding theory. McGraw-Hill Book Co., New York-Toronto, Ont.-London 1968.
[2] N.G. de Bruijn, A Combinatorial Problem. Koninklijke Nederlandse Akademie v. Wetenschappen 49 (1946), 758–764.
[3] S.W. Golomb, Shift register sequences. Holden-Day, Inc., San Francisco, 1967.
[4] Z. Huaxiao, Z. Fuji, H. Qiongxiang On the number of spanning trees and Eulerian tours in iterated line digraphs. Discrete Appl. Math. 73 (1997), no. 1, 59–67.
[5] X.L. Li, Z. Fuji On the numbers of spanning trees and Eulerian tours in generalized de Bruijn graphs. Discrete Math. 94 (1991), no. 3, 189–197.
[6] M. Imori, M. Matsumoto, H. Yamada The line digraph of a regular and pancircular digraph is also regular and pancircular. Graphs and Combinatorics 4 (1988), 235–239.

[7] R. Lidl, H. Niederreiter Introduction to Finite Fields Cambridge University Press, 1986.
[8] F. J. MacWilliams and N. J. A. Sloane, The theory of error-correcting codes, North-Holland, 1977.

Ochanomizu University
E-mail address: hagita@is.ocha.ac.jp

Hiroshima University
E-mail address: m-mat@math.sci.hiroshima-u.ac.jp

Hiroshima University

Hiroshima University