数理解析研究所講究録 1299 巻 2003 年 20-28

畳み込み符号に関する McEliece の定理の修正

(Correction to a theorem of McEliece on convolution codes)

北大・理　橋本　有也 (Yuya Hashimoto)
Division of Mathematics, Graduate School of Science,
Hokkaido Univ.

1 Introduction

Let $F := \mathrm{GF}(q)$. All vectors and matrices are assumed to be those on F. Let $F((D))$ be the ring of formal Laurent series with variable D, and $F(D)$ the rational ring field viewed as a subring of $F((D))$ by a standard way:

$$\begin{aligned} F((D)) &:= \left\{ X(D) = \sum_{i \geq M} x_i D^i \,\middle|\, M \in \mathbb{Z},\ x_i \in F \text{ for all } i \right\}, \\ F(D) &:= \left\{ \frac{P(D)}{Q(D)} \,\middle|\, P(D),\ Q(D) \in F[D],\ Q(D) \neq 0 \right\} \subset F((D)), \end{aligned}$$

where $F[D]$ is a ring of polynomials.

We shall start with the definition of a convolutional code. A convolutional code is a function which maps a sequence of k-dimensional vectors (information words) $\boldsymbol{u}(0), \boldsymbol{u}(1), \ldots$ to a sequence of n-dimensional vectors (codewords) $\boldsymbol{x}(0), \boldsymbol{x}(1), \ldots$. A convolutional code is equipped with a register $\boldsymbol{s}$, which takes an m-dimensional vector(state vector) $\boldsymbol{s}(i)$ at a time i. When a vector $\boldsymbol{u}(i)$ at a time i is input, the convolutional code with a state vector $\boldsymbol{s}(i)$ put out a vector $\boldsymbol{x}(i)$ and the state of the encoder turns to $\boldsymbol{s}(i+1)$. The encoder for a convolution code is formally described by

$$\begin{aligned} \boldsymbol{s}(i+1) &= \boldsymbol{s}(i)\mathcal{A} + \boldsymbol{u}(i)\mathcal{B},\ \boldsymbol{s}(0) = 0, \\ \boldsymbol{x}(i) &= \boldsymbol{s}(i)\mathcal{C} + \boldsymbol{u}(i)\mathcal{D}, \end{aligned}$$

where four matrices $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$, $\mathcal{D}$ have the sizes

$$\begin{aligned} \mathcal{A} &: m \times m, \\ \mathcal{B} &: k \times m, \\ \mathcal{C} &: m \times n, \\ \mathcal{D} &: k \times n. \end{aligned}$$

We furthermore assume that $\mathcal{D}$ is of rank k.

Now we define three vectors $\boldsymbol{X}(D), \boldsymbol{D}(D), \boldsymbol{S}(D)$ on $F((D))$ by

$$\boldsymbol{X}(D) = \sum_{i \geq 0} \boldsymbol{x}(i) D^i,\ \boldsymbol{U}(D) = \sum_{i \geq 0} \boldsymbol{u}(i) D^i,\ \boldsymbol{S}(D) = \sum_{i \geq 0} \boldsymbol{s}(i) D^i.$$

Furthermore define a $k \times n$ matrix $G(D)$ called a *generator matrix* on the rational function field $F(D)$ by

$$G(D) := \mathcal{D} + \mathcal{B}\left(\frac{1}{D}I_m - \mathcal{A}\right)^{-1}\mathcal{C}.$$

Then

$$\boldsymbol{X}(D) = \boldsymbol{U}(D)G(D)$$

and the rank of $G(D)$ is k. Since $G(D)$ has entries from $F(D)$, nothing essential is lost by considering the rational subcode of the code. Thus we shall adopt the following as the definition of a convolutional code:

Definition 1.1 C is said to be an (n,k) *convolutional code* for $1 \leq k \leq n$, if C is a k-dimensional subspace of $F(D)^n$.

If $G(D)$ is generator matrix for C, then $\operatorname{rank} G(D) = k$ and C is $F(D)$-row space of $G(D)$. In other words, an *information word* $\boldsymbol{u}(D) \in F(D)^k$ is encoded as the *codeword* $\boldsymbol{x}(D) \in F(D)^n$ by

$$\boldsymbol{x}(D) = \boldsymbol{u}(D)G(D).$$

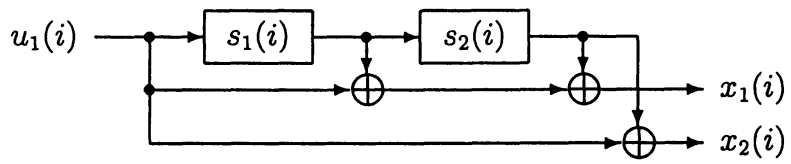
Example 1.2 Consider the following state space realization $(\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D})$ for a convolutional code over $F = \mathrm{GF}(2)$ with $(n,k,m) = (2,1,2)$ whose encoding matrices are given by

$$\mathcal{A} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \ \mathcal{B} = \begin{pmatrix} 1 & 0 \end{pmatrix}, \ \mathcal{C} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \ \mathcal{D} = \begin{pmatrix} 1 & 1 \end{pmatrix}.$$

The generating matrix of this code has the following form:

$$G(D) = \begin{pmatrix} 1 + D + D^2 & 1 + D^2 \end{pmatrix}.$$

This code is physically realized by the following circuit:



Example 1.3 Consider the following state space realization $(\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D})$ for a convolutional code over $F = \mathrm{GF}(2)$ with $(n,k,m) = (4,3,2)$. Then the encoding matrices are given by

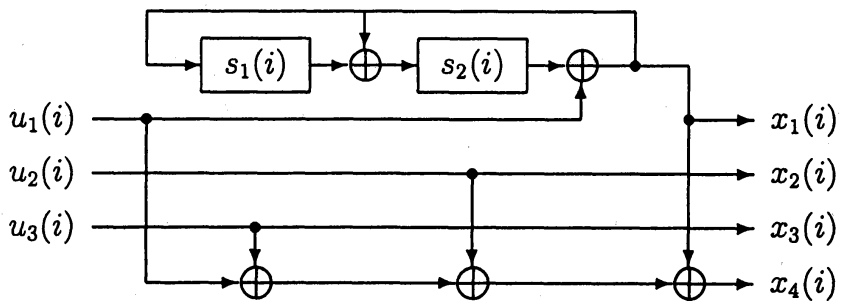
$$\mathcal{A} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \ \mathcal{B} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \\ 0 & 0 \end{pmatrix},$$

$$\mathcal{C} = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \ \mathcal{D} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}.$$

Then we have

$$G(D) = \begin{pmatrix} \frac{1}{1+D+D^2} & 0 & 0 & \frac{D+D^2}{1+D+D^2} \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}.$$

This code is realized by the following circuit:



Definition 1.4 The *weight* of a formal Laurant series $X(D) = \sum_{i \geq m} x_i D^i \in F((D))$ is defined to be the number of non-zero coefficients:

$$\mathrm{wt}(X(D)) := \sharp \{i \; ; \; x_i \neq 0\}.$$

Clearly, the weight of $X(D)$ is finite if and only if $X(D)$ is a Laurant polynomial. The weight of a vector $\boldsymbol{X}(D) = (X_1(D), \ldots, X_n(D)) \in F(D)^n$ is defined to be the sum of the weights of its constituent $X_i(D)$.

$$\mathrm{wt}(\boldsymbol{X}(D)) := \sum_{i=1}^{n} \mathrm{wt}(X_i(D)).$$

Furthermore, the weight of a matrix $K(D) = (k_{ij}(D))$ over $F(D)$ is defined to be the sum of the weights of its constituent $k_{ij}(D)$:

$$\mathrm{wt}(K(D)) := \sum_{i,j} \mathrm{wt}(k_{ij}(D)).$$

Example 1.5 Let $F = \mathrm{GF}(2)$. The weight of $1/(1+D) = 1 + D + D^2 + \cdots$ is infinity. The weight of $(1+D^3)/D^2 = D^{-2} + D$ is 2.

Definition 1.6 A generator matrix $G(D)$ of a convolutional code is said to be *catastrophic* if there is a vector $\boldsymbol{u}(D) \in F(D)^k$ of infinite weight while the corresponding codeword $\boldsymbol{x}(D) = \boldsymbol{u}(D)G(D)$ has a finite weight.

In 1968 Massey and Sain [1] proved the following theorem, which allows us to tell whether a given *polynomial* generator matrix is catastrophic or not.

Theorem 1.7 (Massey-Sain theorem, [1], [2, Theorem 6.3]) *Let $G(D)$ be a polynomial generator matrix of an (n, k) convolutional code and let $\Delta_k(D)$ the greatest common divisor of the $k \times k$ minors of $G(D)$. Then the following three conditions are equivalent:*

(a) *$G(D)$ is non-catastrophic.*

(b) *$\Delta_k(D)$ is a power of D.*

(c) *$G(D)$ has a right inverse matrix, all of whose entries are of finite weight.*

The Massey-Sain theorem can not be directly applied to arbitrary generator matrices, i.e. those which may have non-polynomial entries. In 1998 R. J. McEliece [2] stated the following theorem, where the condition (b) was replaced by a weaker condition (b′).

Theorem 1.8 (McEliece theorem, [2, Theorem 6.6]) *Let $G(D)$ is an arbitrary generator matrix for an (n, k) convolutional code. Let $\beta(D)$ be the least common multiple of the denominators in $G(D)$, let $G'(D)$ be the matrix obtained from $G(D)$ by multiplying each entry by $\beta(D)$. And let $\alpha(D)$ be the greatest common divisor of the $k \times k$ minors of $G'(D)$, and the ratio $\alpha(D)/\beta(D)$ is reduced to lowest terms, say $\alpha'(D)/\beta'(D)$. Then the following three conditions are equivalent.*

(a) *$G(D)$ is non-catastrophic.*

(b′) *$\alpha'(D)$ is a power of D.*

(c) *$G(D)$ has a right inverse matrix, all of whose entries are of finite weight.*

Unfortunately, this important theorem does not hold in this form. The condition looks too weak as is shown in the following section.

2 A proof of McEliece theorem

In this section, we give a proof of Theorem 1.8 (McEliece theorem) in a little improved form. We first show that the original McEliece theorem does not hold (Example 2.1). Next we prove McEliece theorem in a revised form (Theorem 2.2).

Example 2.1 Consider the following generator matrix for the $(4, 3, 2)$ convolutional code over GF(2).

$$G(D) = \begin{pmatrix} \frac{1}{1+D+D^2} & 0 & 0 & \frac{1+D}{1+D+D^2} \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}.$$

The least common multiple of the denominators is $\beta(D) = 1 + D + D^2$, and the matrix obtained by multiplying each of the entries of $G(D)$ by $\beta(D)$ is

$$G'(D) = \begin{pmatrix} 1 & 0 & 0 & 1+D \\ 0 & 1+D+D^2 & 0 & 1+D+D^2 \\ 0 & 0 & 1+D+D^2 & 1+D+D^2 \end{pmatrix}.$$

The greatest common divisor of the 3×3 minors of $G'(D)$ is $\alpha(D) = (1 + D + D^2)^2$, so that the ratio α/β is

$$\frac{\alpha(D)}{\beta(D)} = \frac{(1+D+D^2)^2}{(1+D+D^2)} = \frac{1+D+D^2}{1} = \frac{\alpha'(D)}{\beta'(D)}.$$

Thus $\alpha'(D) = 1 + D + D^2$, which is not a power of D. We see that (b′) fails.

But if now we define

$$K(D) = \begin{pmatrix} 1+D+D^2 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix},$$

it follows that

$$\begin{aligned} G(D)K(D) &= \begin{pmatrix} \frac{1}{1+D+D^2} & 0 & 0 & \frac{1+D}{1+D+D^2} \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1+D+D^2 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = I_3. \end{aligned}$$

Thus $G(D)$ has a right inverse matrix, all of whose entries are of finite weight. We see that (c) holds. Therefore, the McEliece theorem does not hold.

According to this observation, we must replace (b′). Our replacement is stated as follows;

Theorem 2.2 (Main theorem) *Let $G(D)$ be an arbitrary generator matrix for an (n, k) convolutional code. Let $\beta(D)$ be the least common multiple of the denominators in $G(D)$, let $G'(D)$ be the matrix obtained from $G(D)$ by multiplying each entry by $\beta(D)$. And let $(\gamma_1(D), \ldots, \gamma_k(D))$ be the elementary divisor for $G'(D)$, and the ratio $\gamma_k(D)/\beta(D)$ be reduced to lowest terms, say $\gamma'_k(D)/\beta'(D)$. Then the following three conditions are equivalent.*

(a) *$G(D)$ is non-catastrophic.*

(b″) *$\gamma'_k(D)$ is a power of D.*

(c) *$G(D)$ has a right inverse matrix, all of whose entries are of finite weight.*

In order to prove Theorem 2.2 (main theorem), we need to quote the following well-known fact.

Lemma 2.3 *Let R be a principal ideal domain. If G is a $k \times n$ matrix over R, then there exists a $k \times k$ non-singular matrix X, an $n \times n$ non-singular matrix Y and a $k \times n$ diagonal matrix $\Gamma = \mathrm{diag}(\gamma_1, \gamma_2, \ldots, \gamma_r)$ such that $XGY = \Gamma$, $\gamma_i | \gamma_{i+1}$ $(1 \le i < r)$, $\gamma_r \neq 0$,* $\mathrm{rank}\, G = r$. *And $(\gamma_1, \gamma_2, \ldots, \gamma_r)$ is unique up to multiplication by a unit.*

Definition 2.4 $(\gamma_1, \gamma_2, \ldots, \gamma_r)$ referred to in Lemma 2.3 is said to be an *elementary divisor* for G.

Corollary 2.5 *If $G(D)$ is an arbitrary generator matrix for an (n,k) convolutional code, then there exists a $k\times k$ non-singular matrix $X(D)$, an $n\times n$ non-singular matrix $Y(D)$ and a diagonal matrix $\Gamma(D) = \mathrm{diag}(\gamma_1(D),\ldots,\gamma_k(D))$ such that $X(D)G'(D)Y(D) = \Gamma(D)$, $\gamma_i(D)|\gamma_{i+1}(D)$ $(1 \le i < k)$, $\gamma_k(D) \neq 0$ where $G'(D) = \beta(D)G(D)$ and $\beta(D)$ is the least common multiple of the denominators in $G(D)$. And $(\gamma_1(D),\gamma_2(D),\ldots,\gamma_k(D))$ is unique up to multiplication by a unit.*

Proof. Since $G'(D)$ is a $k \times n$ matrix over a principal ideal domain $F[D]$ (polynomial ring) with $\mathrm{rank}\, G'(D) = k$, this result follows immediately from Lemma 2.3. □

Proof of main theorem.
The proof is proceeded as follows: (a)⇒(b″)⇒(c)⇒(a).

(a)⇒(b″) Suppose that $\gamma'_k(D)$ is not a power of D. We show that $G(D)$ is a catastrophic generator matrix. We define

$$\boldsymbol{u}(D) := \begin{pmatrix} 0 & \ldots & 0 & \dfrac{\beta'(D)}{\gamma'_k(D)} \end{pmatrix} X(D).$$

Since $X(D)$ is a non-singular matrix and $\gamma'_k(D)$ is not a unit, we have that $\gamma'_k(D)$ dose not divide a k-th row of $X(D)$. Since $\gamma'_k(D)$ is not a power of D, we have that

$$\mathrm{wt}(\boldsymbol{u}(D)) = +\infty.$$

And it follows that

$$\begin{aligned}
&\frac{1}{\beta(D)}\boldsymbol{u}(D)X(D)^{-1}\Gamma(D) \\
&\quad = \begin{pmatrix} 0 & \ldots & 0 & \dfrac{\beta'(D)}{\beta(D)\gamma'_k(D)} \end{pmatrix}\Gamma(D) \\
&\quad = \begin{pmatrix} 0 & \ldots & 0 & \dfrac{1}{\gamma_k(D)} \end{pmatrix}\begin{pmatrix} \gamma_1(D) & & 0 & \\ & \ddots & & 0 \\ 0 & & \gamma_k(D) & \end{pmatrix} \\
&\quad = \begin{pmatrix} 0 & \ldots & 0 & 1 & 0 & \ldots & 0 \end{pmatrix},
\end{aligned}$$

$$\begin{aligned}
\boldsymbol{x}(D) &= \boldsymbol{u}(D)G(D) \\
&= \frac{1}{\beta(D)}\boldsymbol{u}(D)G'(D) \\
&= \frac{1}{\beta(D)}\boldsymbol{u}(D)X(D)^{-1}X(D)G'(D)Y(D)Y(D)^{-1} \\
&= \frac{1}{\beta(D)}\boldsymbol{u}(D)X(D)^{-1}\Gamma(D)Y(D)^{-1} \\
&= \begin{pmatrix} 0 & \ldots & 0 & 1 & 0 & \ldots & 0 \end{pmatrix} Y(D)^{-1}
\end{aligned}$$

Since $Y(D)$ is a non-singular matrix, $Y(D)^{-1}$ is a matrix over $F[D]$. So,

$$\mathrm{wt}(\boldsymbol{x}(D)) < +\infty.$$

Thus $G(D)$ is a catastrophic generator matrix.

(b″)⇒(c) Suppose that ${\gamma'}_k(D)$ is a power of D. Let $K'(D)$ be an $n \times k$ matrix as follows:

$$K'(D) = \mathrm{diag}\left(\frac{\gamma_k(D)}{\gamma_1(D)}, \frac{\gamma_k(D)}{\gamma_2(D)}, \ldots, \frac{\gamma_k(D)}{\gamma_k(D)}\right) = \begin{pmatrix} \frac{\gamma_k(D)}{\gamma_1(D)} & & 0 \\ & \ddots & \\ 0 & & \frac{\gamma_k(D)}{\gamma_k(D)} \\ & 0 & \end{pmatrix}.$$

Since $\gamma_i(D)$ divides $\gamma_{i+1}(D)$ for $1 \leq i < k$, we have that $\gamma_i(D)$ divides $\gamma_k(D)$ for $1 \leq i \leq k$. So, $K'(D)$ is a matrix over $F[D]$. We define

$$K(D) := \frac{\beta'(D)}{{\gamma'}_k(D)} Y(D)K'(D)X(D).$$

Since ${\gamma'}_k(D)$ is a power of D, we have that

$$\mathrm{wt}(K(D)) < +\infty.$$

And it follows that

$$\begin{aligned} \Gamma(D)K'(D) &= \begin{pmatrix} \gamma_1(D) & & 0 & \\ & \ddots & & 0 \\ 0 & & \gamma_k(D) & \end{pmatrix} \begin{pmatrix} \frac{\gamma_k(D)}{\gamma_1(D)} & & 0 \\ & \ddots & \\ 0 & & \frac{\gamma_k(D)}{\gamma_k(D)} \\ & 0 & \end{pmatrix} \\ &= \gamma_k(D) I_k, \end{aligned}$$

$$\begin{aligned} G(D)K(D) &= \frac{\beta'(D)}{{\gamma'}_k(D)} G(D)Y(D)K'(D)X(D) \\ &= \frac{\beta'(D)}{\beta(D){\gamma'}_k(D)} G'(D)Y(D)K'(D)X(D) \\ &= \frac{1}{\gamma_k(D)} X(D)^{-1}X(D)G'(D)Y(D)K'(D)X(D) \\ &= \frac{1}{\gamma_k(D)} X(D)^{-1}\Gamma(D)K'(D)X(D) \\ &= X(D)^{-1} I_k X(D) \\ &= I_k, \end{aligned}$$

where I_k is a $k \times k$ identity matrix. Thus $G(D)$ has a right inverse matrix, all of whose entries are of finite weight.

(c)⇒(a) Suppose that $K(D)$ is a right inverse matrix for $G(D)$, all of whose entries are of finite weight. If $G(D)$ is a catastrophic generator matrix, there exists $\boldsymbol{u}(D) \in F(D)^k$ such that

$$\mathrm{wt}(\boldsymbol{u}(D)) = +\infty, \ \mathrm{wt}(\boldsymbol{u}(D)G(D)) < +\infty.$$

But since $G(D)K(D) = I_k$ and $\mathrm{wt}(K(D)) < +\infty$, we have that

$$\mathrm{wt}(\boldsymbol{u}(D)) = \mathrm{wt}(\boldsymbol{u}(D)I_k) = \mathrm{wt}(\boldsymbol{u}(D)G(D)K(D)) < +\infty.$$

Thus $G(D)$ is a non-catastrophic generator matrix. □

Example 2.6

$$G(D) = \begin{pmatrix} \frac{1}{1+D+D^2} & 0 & 0 & \frac{1+D}{1+D+D^2} \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

in Example 2.1 is a non-catastrophic generator matrix.

Example 2.7 Consider the following generator matrix for the $(3, 2, 2)$ convolutional code over GF(2).

$$G(D) = \begin{pmatrix} \frac{1}{1+D} & 0 & 1 \\ 0 & 1+D & 1+D \end{pmatrix}.$$

The least common multiple of the denominators is $\beta(D) = 1+D$, and the matrix obtained by multiplying each of the entries of $G(D)$ by $\beta(D)$ is

$$G'(D) = \begin{pmatrix} 1 & 0 & 1+D \\ 0 & (1+D)^2 & (1+D)^2 \end{pmatrix}.$$

The elementary divisor of $G'(D)$ is $(\gamma_1(D), \gamma_2(D)) = (1, (1+D)^2)$, so that the ratio γ_2/β is

$$\frac{\gamma_2(D)}{\beta(D)} = \frac{(1+D)^2}{1+D} = \frac{1+D}{1} = \frac{\gamma_2'(D)}{\beta'(D)}.$$

Thus $\gamma_2'(D) = 1 + D$, which is not a power of D. So, G(D) is a catastrophic generator matrix. Indeed, there exists

$$\boldsymbol{u}(D) = \begin{pmatrix} 0 & \frac{1}{1+D} \end{pmatrix} \in F(D)^2$$

such that

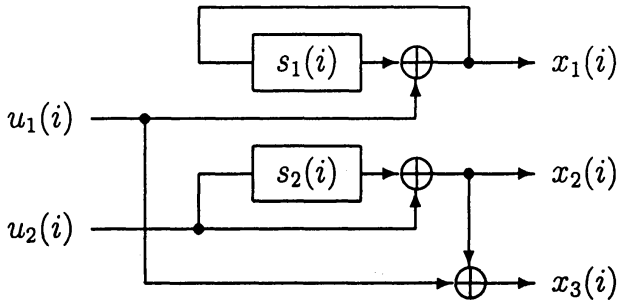
$$\mathrm{wt}(\boldsymbol{u}(D)) = +\infty,$$

$$\mathrm{wt}(\boldsymbol{x}(D)) = \mathrm{wt}(\boldsymbol{u}(D)G(D)) = \mathrm{wt}\left(\begin{pmatrix} 0 & 1 & 1 \end{pmatrix}\right) = 2 < +\infty.$$

And the encoding matrices are given by

$$\mathcal{A} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \ \mathcal{B} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \ \mathcal{C} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix}, \ \mathcal{D} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}.$$

This code is realized by the following circuit:



Finally, Theorem 2.2 (Main theorem) is an extension of Theorem 1.7 (Massey-Sain theorem). We prove that (b) and (b″) are equivalent if $G(D)$ is a polynomial generator matrix.

Definition 2.8 Let Δ_i be the greatest common divisor of the $i \times i$ minors of G. $(\Delta_1, \Delta_2, \ldots, \Delta_r)$ is said to be a *determinantal divisor* for G.

Lemma 2.9 *If $(\gamma_1, \gamma_2, \ldots, \gamma_r)$ is an elementary divisor and $(\Delta_1, \Delta_2, \ldots, \Delta_r)$ is a determinantal divisor for G, then $\Delta_1 = \gamma_1$, $\Delta_2 = \gamma_1\gamma_2$, $\ldots$, $\Delta_r = \gamma_1\gamma_2\cdots\gamma_r$, $\Delta_i = 0$ for $i > r$.*

Remark 2.10 *If $G(D)$ is a polynomial generator matrix for an (n, k) convolutional code, then the condition* (b) *of* Theorem 1.7 *and the condition* (b″) *of* Theorem 2.2 *are equivalent.*

Proof. Since $G(D)$ is a polynomial generator matrix, we have $\beta(D) = 1$. So, $G'(D) = G(D)$ and $\gamma'_k(D) = \gamma_k(D)$.

(b)⇒(b″) Suppose that $\Delta_k(D)$ is a power of D. Since $\gamma_k(D)$ divides $\Delta_k(D)$, we have that $\gamma_k(D)$ is a power of D, too.

(b″)⇒(b) Suppose that $\gamma_k(D)$ is a power of D. Since $\gamma_i(D)$ divides $\gamma_{i+1}(D)$, we have that $\gamma_i(D)$ divides $\gamma_k(D)$ for $1 \leq i \leq k$. So, $\gamma_i(D)$ is a power of D for $1 \leq i < k$, too. Since $\Delta_k(D) = \gamma_1(D)\cdots\gamma_k(D)$, we have that $\Delta_k(D)$ is a power of D. □

References

[1] J. L. Massey and M. K. Sain, *Inverses of linear sequential circuits*, IEEE Trans. Comput. **COM-17** (1968), pp. 330–337.

[2] *HANDBOOK OF CODING THEORY Vol. I* (Edited by V. Pless, W. Huffman and R. Brualdi), North-Holland, Amsterdam (1998), pp. 1065–1138.