The 24th Symposium on Information Theory
and Its Applications (SITA2001)
Kobe, Hyogo, Japan, Dec. 4 - 7, 2001

2 元線形ブロック符号を用いた周期的時変畳込み符号の構成法
The Construction of Periodically Time-variant Convolutional Codes using Binary Linear Block Codes

小笠原 尚徳* 小林 学* 平澤 茂一*
Naonori OGASAHARA Manabu KOBAYASHI Shigeichi HIRASAWA

Abstract— Convolutional codes are known to be potentially superior than block codes. In this paper, we propose a new construction method for periodically time-variant convolutional codes. The lower bound on the minimum free distance of the proposed convolutional codes is proved to be larger than the minimum distance of binary linear block codes. We show that there exists some periodically time-variant convolutional codes which are superior than BCH convolutional codes.

Keywords— BCH convolutional codes, Binary linear block codes, Periodically time-variant convolutional codes, Minimum condition, Noncatastorophic

1 まえがき

ブロック符号の構成法を利用した畳込み符号は，1970年頃から様々な研究者によって提案されているが，未だ一般的に良いとされる符号の構成には至っていない．J.Rosenthal は BCH 符号の検査行列を連接させた行列を用いることにより，情報系列が満たすべき条件を定めた BCH 畳込み符号を提案した [4]．この符号は時不変畳込み符号であり，かつその最小自由距離の下界は BCH 限界で保証することができる．

一方，一般の 2 元線形ブロック符号の中には BCH 限界以上の最小距離を持つ符号や符号化率のより高い符号が知られている [3]．本研究では 2 元線形ブロック符号のパリティ検査行列に着目し，Rosenthal の符号を拡張した時変畳込み符号を提案する．また，提案する符号の最小自由距離の下界が 2 元線形ブロック符号の最小距離以上となる事を示す．更に BCH 畳込み符号よりも性能の優れた時変畳込み符号が構成可能であることを構成例により示す．

2 周期的時変畳込み符号の基本的な構成法

2.1 時変畳込み符号の定義

符号ブロックの長さ n，情報ブロックの長さ k，符号器の遅延素子数 δ を持つ 2 元組織畳込み符号を考える．行列 A, B_t, C_t, D をそれぞれ $A \in \mathbb{F}_2^{\delta\times\delta}$，$B_t \in \mathbb{F}_2^{\delta\times k}$, $C_t \in \mathbb{F}_2^{(n-k)\times\delta}$，$D \in \mathbb{F}_2^{(n-k)\times k}$ とする．ここで，$\mathbb{F}_2$ は要素数 2 のガロア体とする．更に，$\boldsymbol{x}_t \in \mathbb{F}_2^{\delta}$, $\boldsymbol{u}_t \in \mathbb{F}_2^{k}$, $\boldsymbol{y}_t \in \mathbb{F}_2^{n-k}$, $\boldsymbol{v}_t \in \mathbb{F}_2^{n}$ をそれぞれ時点 $t\ (=0,1,2,\cdots)$ における状態ベクトル，情報ベクトル，検査ベクトル，符号ベクトルとする．この時，周期的時変組織畳込み符号を次のように定義する．

$$\begin{aligned} \boldsymbol{x}_{t+1} &= A\boldsymbol{x}_t + B_t\boldsymbol{u}_t,\ \boldsymbol{x}_0 = 0, \\ \boldsymbol{y}_t &= C_t\boldsymbol{x}_t + D\boldsymbol{u}_t, \\ \boldsymbol{v}_t &= \begin{bmatrix} \boldsymbol{y}_t \\ \boldsymbol{u}_t \end{bmatrix}. \end{aligned} \tag{1}$$

ここで，行列 B_t, C_t は時変行列であり，それぞれの周期が違う場合も考慮する．つまり，周期的時変畳込み符号の周期は行列 B_t, C_t の各々の周期の最小公倍数となる．また，符号 $\mathcal{C}$ の最小自由距離 $d_f(\mathcal{C})$ は，非全零の符号語に対して次式で定義される．

$$d_f(\mathcal{C}) = \min\left(\sum_{t=0}^{\infty} wt(\boldsymbol{u}_t) + \sum_{t=0}^{\infty} wt(\boldsymbol{y}_t)\right) \tag{2}$$

ただし $wt(\cdot)$ はハミング重みを表す。

2.2 最小性と非カタストロフィック

上で定義した周期的時変畳込み符号が畳込み符号として不利な性質を持たないための条件を以下で示す．まず初めに，最小性を示すために必要な概念として可制御性，可観測性について定義する．

定義 2.1 可制御とは任意の初期時点 τ における状態ベクトル $\boldsymbol{x}_\tau$ がある時点 $t_1(>\tau)$ において，$\boldsymbol{x}_{t_1} = 0$ となるような情報系列 $\boldsymbol{u}_t\ (\tau \le t \le t_1)$ が存在する事である．

定義 2.2 可観測とは任意の初期時点 τ とある時点 $t_1(>\tau)$ において，状態ベクトル $\boldsymbol{x}_\tau$ を入出力ベクトル $\boldsymbol{u}_t$，$\boldsymbol{y}_t\ (\tau \le t \le t_1)$ から決定できる事である．

補題 2.1 上で定義した周期的時変畳込み符号が可制御となるための条件は，初期時点を τ とし，$\boldsymbol{x}_t = 0$ となる時点を $t_1 + 1\ (>\tau)$ とした時，行列

$$F(\tau, t_1) = \left[A^{t_1-\tau}B_\tau \ \ A^{t_1-\tau-1}B_{\tau+1}\cdots AB_{t_1-1}\ \ B_{t_1}\right] \tag{3}$$

がフルランクとなる事である．また，この行列を以後，可制御行列と呼ぶ．

証明 $\boldsymbol{x}_{t_1+1} = 0$ となる時，式 (1) より次式が成立する．

$$-A^{t_1-\tau+1}\boldsymbol{x}_\tau = F(\tau, t_1)\begin{bmatrix} \boldsymbol{u}_\tau \\ \boldsymbol{u}_{\tau+1} \\ \vdots \\ \boldsymbol{u}_{t_1} \end{bmatrix} \tag{4}$$

この時，式 (4) が成立するような情報系列 $\boldsymbol{u}_t$ が存在する条件は行列 $F(\tau, t_1)$ がフルランクとなる事である．□

補題 2.2 上で定義した周期的時変畳込み符号が可観測となるための条件は，初期時点 $^\forall\tau$，$^\exists t_1(>\tau)$ に対して，行列

$$M(\tau, t_1) = \begin{bmatrix} C_\tau \\ C_{\tau+1}A \\ \vdots \\ C_{t_1}A^{t_1-\tau} \end{bmatrix} \tag{5}$$

がフルランクとなる事である．また，この行列を以後，可観測行列と呼ぶ．

証明 式 (1) より次式が成立する．

$$\begin{bmatrix} \boldsymbol{y}_\tau - D\boldsymbol{u}_\tau \\ \boldsymbol{y}_{\tau+1} - C_{\tau+1}B_\tau\boldsymbol{u}_\tau - D\boldsymbol{u}_{\tau+1} \\ \vdots \\ \boldsymbol{y}_{t_1} - C_{t_1}\sum_{i=\tau}^{t_1-1} A^{t_1-1-i}B_i\boldsymbol{u}_i - D\boldsymbol{u}_{t_1} \end{bmatrix} = M(\tau, t_1)\boldsymbol{x}_\tau \tag{6}$$

従って，行列 $M(\tau, t_1)$ がフルランクであれば，$\boldsymbol{x}_\tau$ を入出力ベクトルから決定する事ができる．□

ここで，最小性を示す定理の準備として，線形システム

* 早稲田大学理工学部経営システム工学科，〒169-8555 東京都新宿区大久保 3-4-1，School of Science and Engineering, Waseda University, 3-4-1 Ohkubo Shinjyuku-ku, Tokyo, 169-8555 Japan

理論でよく使われる重み行列 [6] とその性質について述べる．初期時点 τ , $^{\exists}t_1(>\tau)$ とした時，重み行列はシステムの入出力関係を定める $(n-k)\times k$ の行列

$$W(t,\tau)=C_tA^{t-\tau}B_\tau \tag{7}$$

で定義される．重み行列が持つ重要な性質の一つは，それが状態ベクトルの線形変換によって不変な事である．つまり，ある正則行列 T で状態ベクトルを次のように変換したとする．

$$\bar{\boldsymbol{x}}_t=T\boldsymbol{x}_t \tag{8}$$

この時，式 (1) によるシステムは状態ベクトル $\bar{\boldsymbol{x}}_t$ によって，次のようになる．

$$\begin{aligned}\bar{\boldsymbol{x}}_{t+1} &= \bar{A}\bar{\boldsymbol{x}}_t+\bar{B}_t\boldsymbol{u}_t,\\ \boldsymbol{y}_t &= \bar{C}_t\bar{\boldsymbol{x}}_t+D\boldsymbol{u}_t.\end{aligned} \tag{9}$$

ただし，

$$\begin{aligned}\bar{A}&=TAT^{-1}\\ \bar{B}_t&=TB_t\\ \bar{C}_t&=C_tT^{-1}\end{aligned} \tag{10}$$

である．システム (9) による重み行列は式 (10) より，

$$\begin{aligned}\bar{W}(t,\tau) &= \bar{C}_t\bar{A}^{t-\tau}\bar{B}_\tau\\ &= C_tT^{-1}(TA^{t-\tau}T^{-1})TB_\tau\\ &= W(t,\tau)\end{aligned}$$

となる．すなわち，重み行列は状態ベクトルに対する線形変換に対し，不変である事が示された．以上の事を踏まえ次の定理を示す．

定理 2.1　式 (1) によるシステムが可制御かつ可観測であるならば，遅延素子数が最小のシステムで実現できる．

証明　今，システム (1) が可制御かつ可観測で最小のシステムでないとする．この時，$\bar{\boldsymbol{x}}_t=T\boldsymbol{x}_t$ によるシステムが最小システムとなるような正則行列 T が存在する．また，このシステムの行列組 $\bar{A}\in\mathbb{F}^{\delta\times\delta}$, $\bar{B}_t\in\mathbb{F}^{\delta\times k}$, $\bar{C}_t\in\mathbb{F}^{(n-k)\times\delta}$ を次のように定義する．

$$\bar{A}=\begin{bmatrix}\bar{A}^{11} & \bar{A}^{12}\\ \mathbf{0} & \bar{A}^{22}\end{bmatrix},\bar{B}_t=\begin{bmatrix}\bar{B}_t^1\\ \mathbf{0}\end{bmatrix},\ \bar{C}_t=[\bar{C}_t^1\quad\bar{C}_t^2]. \tag{11}$$

$$\bar{A}^{11}\in\mathbb{F}^{a\times a},\quad \bar{B}_t^1\in\mathbb{F}^{a\times k},\quad \bar{C}_t^1\in\mathbb{F}^{(n-k)\times a}.$$

ここで，$a<\delta$ が成立すると仮定する．重み行列は線形変換に対し不変であるので，

$$\begin{aligned}C_tA^{t-\tau}B_\tau &= \bar{C}_t\bar{A}^{t-\tau}\bar{B}_\tau\\ &= \bar{C}_t^1(\bar{A}^{11})^{t-\tau}\bar{B}_\tau^1\end{aligned} \tag{12}$$

が成立する．式 (12) はシステム (1) が最小の行列組 $(\bar{A}^{11},\bar{B}_t^1,\bar{C}_t^1)$ で実現できるという事を示している．ここで，時点 t,τ が範囲 $t_0\le\tau\le t\le t_1$ とした時を考える．この時，次の行列を定義すると，

$$K(t_0,t_1)=\begin{bmatrix}\bar{C}_{t_0}^1\\ \bar{C}_{t_0+1}^1\bar{A}^{11}\\ \vdots\\ \bar{C}_{t_1}^1(\bar{A}^{11})^{t_1-t_0}\end{bmatrix} \tag{13}$$

式 (12) から $t_0\le t\le t_1$ に対して次式が成立する．

$$M(t_0,t_1)A^{t_0-\tau}B_\tau=K(t_0,t_1)(\bar{A}^{11})^{t_0-\tau}\bar{B}_\tau^1 \tag{14}$$

また，行列 $L(t_0,t_1)$ を次のように定義した時，

$$L(t_0,t_1)=\left[(\bar{A}^{11})^{t_1-t_0}\bar{B}_{t_0}^1\cdots\bar{A}^{11}\bar{B}_{t_1-1}^1\ \bar{B}_{t_1}^1\right] \tag{15}$$

先程と同様に 式 (14) は $t_0\le\tau\le t_1$ に対し，

$$\begin{aligned}&M(t_0,t_1)A^{-(t_1-t_0)}F(t_0,t_1)\\ &\qquad=K(t_0,t_1)(\bar{A}^{11})^{-(t_1-t_0)}L(t_0,t_1)\end{aligned} \tag{16}$$

と表される．システム (1) は可制御かつ可観測なので，t_0 に対してある t_1 が適当な大きさであれば，式 (16) の行列 M , F の rank は δ である．また，行列 A の rank も δ であるので左辺の rank は δ である．一方，式 (16) の右辺の行列 K , L の rank は高々 a である．すなわち，

$$\delta=\mathrm{rank}\left\{M(t_0,t_1)A^{-(t_1-t_0)}F(t_0,t_1)\right\}\le a \tag{17}$$

となり，$\delta>a$ であった事に矛盾し，定理が証明された．□

次に，非カタストロフィックについて考える．式 (1) が周期 r ，符号化率 k/n の時変畳込み符号であるとする．ここで，情報ベクトルと検査ベクトルを次のように多項式表現する．

$$U(z)=\sum_{j=0}^{\infty}\begin{bmatrix}\boldsymbol{u}_{rj}\\ \boldsymbol{u}_{rj+1}\\ \vdots\\ \boldsymbol{u}_{rj+r-1}\end{bmatrix}z^j,\ Y(z)=\sum_{j=0}^{\infty}\begin{bmatrix}\boldsymbol{y}_{rj}\\ \boldsymbol{y}_{rj+1}\\ \vdots\\ \boldsymbol{y}_{rj+r-1}\end{bmatrix}z^j. \tag{18}$$

また，符号ベクトルについても同様の方法で，$V(z)$ と定義する．この時，式 (1) から次式が成立する．

$$\begin{aligned}Y(z)=&\left[\frac{z}{I-A^rz}M(0,r-1)F(0,r-1)\right.\\ &\left.+\begin{bmatrix}D & & & & \\ C_1B_0 & D & & & \\ C_2AB_0 & C_2B_1 & D & & \\ \vdots & \vdots & & \ddots & \\ C_{r-1}A^{r-2}B_0 & \cdots & \cdots & C_{r-1}B_{r-2} & D\end{bmatrix}\right]U(z)\end{aligned} \tag{19}$$

ここで，式 (19) の右辺の $U(z)$ の係数にある行列を $G_0(z)$ とする．この時，式 (1) の符号化率 rk/rn の時不変畳込み符号の生成行列は

$$V(z)=\begin{bmatrix}G_0(z)\\ I\end{bmatrix}U(z) \tag{20}$$

である．従って，式 (1) による符号化率 rk/rn の時不変畳込み符号の生成行列は有理関数による組織生成行列である事が得られた．符号化率 k/n ，周期 r の時変畳込み符号は符号化率 rk/rn の時不変畳込み符号と得られる符号語集合が同じである．従って，次の定理により符号化率 rk/rn の時不変畳込み符号が非カタストロフィックである事を示せば良い．

定理 2.2　式 (1) による符号化率 rk/rn の時不変畳込み符号は非カタストロフィックである．

証明　有理生成行列 $G(z)$ を持つ時不変畳込み符号が非カタストロフィックとなる必要十分条件は次の条件のいずれかが成り立つ事である [2] .

(1) 無限の重みを持つ入力 $U(z)$ に対し，
$V(z)=G(z)U(z)$ が有限重みの出力でない

(2) $G(z)$ が有限重み左逆行列を持つ

式 (20) は有限重み左逆行列 $[\mathbf{0}\quad I]$ を持ち，(2) の条件を満たす．□

2.3　最小自由距離

後述する構成法 I や構成法 II は可制御行列が 2 元線形符号の検査行列となるように行列 A,B_t,C_t が定義される．次の定理ではそのような構成を利用する事により，最小自由距離の下限を与える．

定理 2.3　式 (1) のシステムが可制御かつ可観測の条件を満たし，任意の τ に対し，可制御行列 $F(\tau,\tau+(d-1)\nu-1)$ が (N,K,d) 2 元線形符号の検査行列であるとする．ここで，ν は可観測行列 $M(\tau,\tau+i-1)$ がフルランクとなる最小の整数 i とする．更に，次の制約式が成立すると仮定する．

$$N\ge(d-1)k\nu. \tag{21}$$

このとき，周期的時変畳込み符号 $\mathcal{C}$ は符号化率 k/n ，遅延素子数 $N-K$ を持つ．また，最小自由距離 $d_f(\mathcal{C})$ は次の下界で抑えられる．

$$d_f(\mathcal{C}) \geq d \tag{22}$$

証明　可制御行列が検査行列となる仮定からシステム (1) で定義した行列のサイズにおいて，遅延素子数 $\delta = N-K$ であり，他は定義したものと同じである．従って，符号化率 k/n，遅延素子数 $N-K$ である事がわかる．

いま有限重み符号語についてのみ考えれば良いため，$\boldsymbol{u}_0 = \boldsymbol{u}_1 = \cdots = \boldsymbol{u}_{\tau-1} = 0$, $\boldsymbol{u}_\tau \neq 0$ かつ $\boldsymbol{x}_\tau = 0$, $\boldsymbol{x}_\gamma \neq 0$, $\boldsymbol{x}_{\gamma+1} = 0$ を仮定する．証明は 2 つの場合 (i) $\gamma-\tau+1 \leq (d-1)\nu$, (ii) $\gamma-\tau+1 > (d-1)\nu$ に分けて証明する．

(i) $\gamma-\tau+1 \leq (d-1)\nu$ のとき

$\boldsymbol{x}_{\gamma+1} = 0$ より式 (4) が成立し，更に $\boldsymbol{x}_\tau = 0$ より次式が成り立つ．

$$\left[A^{\gamma-\tau}B_\tau \cdots AB_{\gamma-1}\ B_\gamma\right] \begin{bmatrix} \boldsymbol{u}_\tau \\ \boldsymbol{u}_{\tau+1} \\ \vdots \\ \boldsymbol{u}_\gamma \end{bmatrix} = 0. \tag{23}$$

左辺に現れる可制御行列は $(N-K)\times(d-1)k\nu$ の 2 元線形符号の検査行列の一部分である．従って $\boldsymbol{u}_\tau \neq 0$ であることから，$wt(\boldsymbol{u}_\tau, \boldsymbol{u}_{\tau+1}, \cdots, \boldsymbol{u}_\gamma) \geq d$ が成立する．従って $wt(\boldsymbol{v}_\tau, \boldsymbol{v}_1, \cdots, \boldsymbol{v}_\gamma) \geq d$ が成り立つ．

(ii) $\gamma-\tau+1 > (d-1)\nu$ のとき

$$wt(\boldsymbol{u}_\tau, \cdots, \boldsymbol{u}_{\tau+(d-1)\nu-1}) \geq d$$

のときは，定理が明らかに成立するので

$$wt(\boldsymbol{u}_\tau, \cdots, \boldsymbol{u}_{\tau+(d-1)\nu-1}) = b < d \tag{24}$$

を仮定する．このとき最大 b 個の非零 $\boldsymbol{u}_j$ が範囲 $\tau \leq j \leq \tau+(d-1)\nu-1$ に存在する．また ν 個の連続する全零ベクトル $\boldsymbol{u}_t, \boldsymbol{u}_{t+1}, \cdots, \boldsymbol{u}_{t+\nu-1}$ が少なくとも $(d-1)-b$ 個，範囲 $[\tau+1, \tau+(d-1)\nu-1]$ に存在する．そのような連続するベクトルの一つを $\boldsymbol{u}_t, \boldsymbol{u}_{t+1}, \cdots, \boldsymbol{u}_{t+\nu-1}$ とする．このとき (6) 式より次の等式が導かれる．

$$\begin{bmatrix} \boldsymbol{y}_t \\ \boldsymbol{y}_{t+1} \\ \vdots \\ \boldsymbol{y}_{t+\nu-1} \end{bmatrix} = \begin{bmatrix} C_t \\ C_{t+1}A \\ \vdots \\ C_{t+\nu-1}A^{\nu-1} \end{bmatrix} \boldsymbol{x}_t \tag{25}$$

ここで $\boldsymbol{x}_t$ は

$$\boldsymbol{x}_t = \left[A^{t-\tau-1}B_\tau \cdots AB_{t-2}\ B_{t-1}\right] \begin{bmatrix} \boldsymbol{u}_\tau \\ \boldsymbol{u}_{\tau+1} \\ \vdots \\ \boldsymbol{u}_{t-1} \end{bmatrix} \tag{26}$$

であるので，$\boldsymbol{x}_t = 0$ だと仮定すると，式 (23) の議論から $\boldsymbol{u}_\tau \neq 0$ より，$wt(\boldsymbol{u}_\tau, \cdots, \boldsymbol{u}_{t-1}) \geq d$ となり，仮定に矛盾する．従って，$\boldsymbol{x}_\tau \neq 0$ とすると (25) 式の右辺の可観測行列はフルランクであるから，少なくとも 1 つの非零の $\boldsymbol{y}_j$, $t \leq j \leq t+\nu-1$, が存在する．ところで，このような連続するベクトルは $(d-1)-b$ 個あったので，$\boldsymbol{y}_{\tau+1}$ から $\boldsymbol{y}_{\tau+(d-1)\nu-1}$ に $(d-1)-b$ の非零の出力が存在する．従って，

$$wt(\boldsymbol{v}_\tau, \boldsymbol{v}_{\tau+1}, \cdots, \boldsymbol{v}_{\tau+(d-1)\nu-1}) \geq (d-1) \tag{27}$$

が成り立つ．ここで $\boldsymbol{u}_\gamma \neq 0$ （$\boldsymbol{x}_\gamma \neq 0, \boldsymbol{x}_{\gamma+1} = 0$ より）も考慮すると $wt(\boldsymbol{v}_\tau, \boldsymbol{v}_1, \cdots, \boldsymbol{v}_\gamma) \geq d$ となる．以上より定理が成り立つ．□

3　構成法 I

本節では任意の 2 元線形符号に対して，構成可能な周期的時変畳込み符号について構成する．

3.1　2 元線形符号を利用した時変畳込み符号の定義

式 (1) において，行列 A を $\mathbb{F}_2$ 上の $\delta\times\delta$ の単位行列とする．この時，式 (1) と同様，符号化率 k/n , 遅延素子数 δ の周期的時変畳込み符号は次のように定義される．

$$\begin{aligned} \boldsymbol{x}_{t+1} &= \boldsymbol{x}_t + B_t\boldsymbol{u}_t,\ \boldsymbol{x}_0 = 0, \\ \boldsymbol{y}_t &= C_t\boldsymbol{x}_t + D\boldsymbol{u}_t, \\ \boldsymbol{v}_t &= \begin{bmatrix} \boldsymbol{y}_t \\ \boldsymbol{u}_t \end{bmatrix}. \end{aligned} \tag{28}$$

ここで，行列 B_t は 2 元線形符号 (N,K,d) の検査行列を k 列ずつに分割した行列と定義する．つまり，2 元線形符号の検査行列を

$$\left[E_0\ \ E_1\ \ \cdots\ \ E_{\lfloor N/k\rfloor-1}\right],\ E_i \in \mathbb{F}_2^{\delta\times k}. \tag{29}$$

とした時 [1]，行列 B_t を周期 $\lfloor N/k\rfloor$ の

$$B_t = E_{t \bmod \lfloor N/k\rfloor} \tag{30}$$

として定義する．また，行列 C_t は行列 $[I\,I\,\cdots]^T$ を $n-k$ 行ずつに分割した行列として定義する．ただし，行列 $I \in \mathbb{F}_2^{\delta\times\delta}$ は単位行列である．つまり，行列 C_t の成分を c_{ij}^t $(1 \leq i \leq n-k, 1 \leq j \leq \delta)$ とする時，

$$c_{ij}^t = \begin{cases} 1 & (\ j = (n-k)t+i \bmod \delta \text{ のとき}) \\ 0 & (\text{それ以外のとき}) \end{cases} \tag{31}$$

と定義する．またこの事から，行列 C_t の周期は正の整数 $i\,(= \min\{j \mid j\delta \bmod (n-k) = 0, j = 1,2,\cdots\})$ に対して，$i\delta/(n-k)$ である．

以上の事から，式 (28) の畳込み符号の周期は

$$\mathrm{LCM}(\lfloor N/k\rfloor, i\delta/(n-k)) \tag{32}$$

となる．

3.2　最小性と最小自由距離

式 (28) は式 (1) を基に構成した式であるので，定理 2.2 が成り立ち非カタストロフィックを満足する．本節では初めに，式 (28) で定義した周期的時変畳込み符号が最小性を満足する事を示す．

補題 3.1 式 (28) で定義した周期的時変畳込み符号は可制御である．

証明　初期時点を τ , ある時点を t_1 とした時，式 (28) における可制御行列 $F(\tau, t_1)$ は行列 B_t の定義から 2 元線形符号の検査行列の一部でありフルランクである．□

補題 3.2 式 (28) で定義した周期的時変畳込み符号は可観測である

証明　初期時点 $^\forall\tau$, $^\exists t_1$ において，式 (28) から導かれる可観測行列 $M(\tau, t_1)$ は行列 C_t の定義より，フルランクである．□

定理 3.1　式 (28) の周期的時変畳込み符号は最小性を満足する．

証明　補題 3.1 , 補題 3.2 , 定理 2.1 より成立する．□

定理 3.2

$$N \geq (d-1)k\nu. \tag{33}$$

が成立すると仮定する．ただし，ν は可観測行列 $M(\tau, \tau+i-1)$ がフルランクとなる最小の整数 i とする．この時，式 (28) の周期的時変畳込み符号の最小自由距離の下界は 2 元線形符号の最小距離 d である．

[1] N/k が割り切れない時は余分な列を切り捨てた検査行列を考える．

証明　システム (28) は可制御かつ可観測である．また，式 (33) より可制御行列 $F(\tau,\tau+(d-1)\nu-1)$ が 2 元線形符号の検査行列である事から，定理 2.3 が適用でき，定理が成立する．　□

3.3 構成法 I の例

ここでは，原始 BCH 符号よりも良い 2 元最良線形符号 [3] をいくつか取り上げ，原始 BCH 符号を用いた BCH 畳込み符号（表 1 に示す）と 2 元最良線形符号を使った構成法 I の時変畳込み符号（表 2 に示す）とを比較する．　ここで，構成法 I で用いた 2 元線形符号はそ

表 1: BCH 畳込み符号（時不変）

BCH 符号 (N,K,d)	設計距離 d	遅延素子数 $N-K$	符号化率 $\max k/n$
(63,24,15)	15	39	0.093

表 2: 構成法 I (時変)

2 元線形符号 (N,K,d)	設計距離 d	遅延素子数 $N-K$	符号化率 $\max k/n$
(a) (63,28,15)	15	35	0.103
(b) (79,40,15)	15	39	0.114

れぞれ (a) 巡回符号，(b) Quadratic residue 符号 である [3]．また，最大符号化率は制約式 $N \geq (d-1)k\lceil\frac{N-K}{n-k}\rceil$ を満たす最大の値である．

4 構成法 II

本節では限られた範囲の 2 元線形符号に対してのみ構成可能な周期的時変畳込み符号を例を用いて示す．構成法 I に比べ，行列 C_t を時不変にして構成できる．

4.1 行列の構成例

ここでは，可観測行列がフルランクとなるような行列 A,C の構成を行い，それと同時に Srivastava code を効率的に用いた 2 元 $(146,101,13)$ 線形符号が可制御行列となるような行列 A, B_t の構成を行う．

式 (1) において行列 C_t が時不変になった行列 C によるシステムを考える．初めに，可観測行列となるような行列 A,C の構成を考える．$\xi \in \mathbb{F}_{2^m}$ を多項式基底により $\mathbb{F}_2$ 上の列ベクトル表現としたものを $[\xi]$ と表記する．また，原始多項式を $z^m+f_{m-1}z^{m-1}+\cdots+f_0$ と表記すると，α の行列表現，L_α は

$$L_\alpha = \begin{bmatrix} 0 & \cdots & 0 & -f_0 \\ 1 & & 0 & -f_1 \\ & \ddots & & \vdots \\ 0 & & 1 & -f_{m-1} \end{bmatrix} \tag{34}$$

である．$\mathbb{F}_2$ 上での α の乗算は次のようにして，L_α を左からかける事によって可能となる．

$$(L_\alpha)^i \times [\alpha^j] = [\alpha^{i+j}] \tag{35}$$

この時，符号長 73，情報記号数 28 の $(73,28,d)$ BCH 符号の検査行列が $A,\tilde{C}$ の可制御行列となるような行列 $A,\tilde{C}$ は次のように定義される．

$$A := \begin{bmatrix} (L_\alpha)^{kj_1} & 0 & \cdots & 0 \\ 0 & (L_\alpha)^{kj_2} & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & (L_\alpha)^{kj_9} \end{bmatrix} \tag{36}$$

$$\tilde{C} := \begin{bmatrix} [1] & [\alpha^{j_1}] & \cdots & [\alpha^{(n-k-1)j_1}] \\ [1] & [\alpha^{j_2}] & \cdots & [\alpha^{(n-k-1)j_2}] \\ \vdots & \vdots & \vdots & \\ [1] & [\alpha^{j_9}] & \cdots & [\alpha^{(n-k-1)j_9}] \end{bmatrix} \tag{37}$$

ただし，$1 \leq j_1 < \cdots < j_9 \leq d-1$ である．ここで，BCH 畳込み符号 [4] の構成法により，正則行列 S に対して，$A = SA^TS^{-1}$, $C = \tilde{C}^TS^{-1}$ と変換された行列 A, C の可観測行列はフルランクとなる．

次に，行列 A, B_t が可観測行列となるような行列 B_t を構成する．$(146,101,13)$ 2 元線形符号の検査行列を k 列ずつに区切って表現した行列を

$$[E_0 \;\; E_1 \;\; \cdots \;\; E_{\lfloor N/k \rfloor -1}] \tag{38}$$

とした時，行列 B_t は上で構成した正則行列 A を用い，周期 $\lfloor N/k \rfloor$ の

$$B_t = A^{\lfloor N/k \rfloor -t-1} E_{t \bmod \lfloor N/k \rfloor} \tag{39}$$

として定義する．

4.2 構成法 II の例

上で示した構成例の他にも構成できる例として，(178, 123, 15) 短縮 BCH 符号を使った周期的時変畳込み符号が構成できる．これらの例を以下の表にまとめる．ただし，最大符号化率は制約式 $N \geq (d-1)k\lceil\frac{N-K}{n-k}\rceil$ を満たす最大の値である．

表 3: 構成法 II

2 元線形符号 (N,K,d)	設計距離 d	遅延素子数 $N-K$	符号化率 $\max k/n$
(146,101,13)	13	45	0.211
(178,123,15)	15	55	0.179

5 考察

構成法 I の例では原始 BCH 符号を使った BCH 畳込み符号（時不変）と比較し，設計距離，遅延素子数，符号化率において勝っている事を示した．一方，構成法 II は限られた範囲の 2 元線形符号でしか構成できないので，原始 BCH 符号を使った BCH 畳込み符号を使って比較する場合，符号長などに開きがあり一概に比較できない．今後は構成法 I も含めて，一般の BCH 符号を使った BCH 畳込み符号とを比較する必要がある．また，回路規模の比較も今後必要である．更に，復号の計算量は最尤復号を用いた場合，遅延素子数の指数オーダとなるため，復号計算量の改善が今後の重要な課題である．

謝辞

平澤研究室の岩下将人氏，岡田知嗣氏，八木秀樹氏には本研究において大変お世話になりました．尚，本研究の一部は文部科学省平成 12・13 年度科学研究費補助金（課題番号 12875072）の助成による．

参考文献

[1] R.Johannesson and K.Sh.Zigangirov, *Fundamentals of Convolutional Coding*, New York:IEEE Press,1999.

[2] R. J. McEliece, *The algebraic theory of convolutional codes*, in Handbook of Coding Theory, Amsterdam,The Netherlands :Elsevier, pp. 1101-1107, 1998.

[3] S.Litsyn, *An update table of the best binary codes known*, in Handbook of Coding Theory, Amsterdam,The Netherlands :Elsevier, pp. 485-498, 1998.

[4] J. Rosenthal and E.V. York, "BCH convolutional codes," *IEEE Trans. Inform. Theory*, vol. 45, pp. 1833-1844, Sep. 1999.

[5] J.Rosenthal, J. M. Schumacher and E. V. York, "On behaviors and convolutional codes," *IEEE Trans. Inform. Theory*, vol. 42, pp. 1881-1891, Nov. 1996.

[6] 有本卓，線形システム理論，" 産業図書，pp.105-126, 1977.