修正済

線型ネットワーク符号とその構成法

On the Linear Network Codes and their Novel Construction Methods

栗原正純*
Masazumi Kurihara

電気通信大学 情報通信工学科†
Dept. of Information and Communication Engeneering, Univ. of Electro-Communications

1 まえがき

本稿では, **ネットワーク符号化**の一手法である**線型ネットワーク符号** (Linear Network Code(**LNC**)) の幾つかの新しい構成法について述べる. 具体的には, **マルチキャスト LNC**, **ブロードキャスト LNC**, **ロバスト LNC** を扱う. これらの符号を構成する前処理として, ベースとなる**最大 LNC** という符号を構成する. ネットワーク符号化の特徴の一つは, 中継ノードでも符号化を行なうことである. 最大 LNC をベースにすることで, 最大 LNC により設定された中継ノードでの符号化手続きを一切変更することなく, 最大 LNC から直接それぞれの目的の LNC を構成可能であることを示す. これらの方法は, 従来提案されている構成法 [1, 2, 3] とは異なる.

2 準備

数学的準備として既知ではない定理 2.1 と線型代数関連の書籍などに記載されている定理 2.2 を記す.

定理 2.1 N 個の有限体 $\mathbf{F}$ 上の $m \times n$ 行列 $H_1, \ldots, H_N$ は
$\text{rank } H_i = n \text{ for all } i \in \{1, \ldots, N\}$
を満たすとする. このとき, $|\mathbf{F}| > N$ ならば,
$\text{rank } GH_i = n \text{ for all } i \in \{1, \ldots, N\}$
を満たす $\mathbf{F}$ 上の $n \times m$ 行列 G が存在する. ∎

定理 2.2 $m \times n$ 行列 A, B に対し, 次の不等式が成り立つ.
$\text{rank } (A+B) \leq \text{rank } A + \text{rank } B.$ ∎

3 ネットワーク

ネットワークを次のようなグラフとして定める: Unit capacity, directed, acycle multi-graph (V, E), ソースノード $s \in V$, シンクノードの集合 $T \subseteq V$. Unit capacity であるリンク $e \in E$ は, 1 単位時間に $\mathbf{F}$ の要素シンボル 1 個を伝送可能な通信路である. 各 $t \in T$ に対し, ソース s からシンク t への**最大流**を h_t と表す. 以下, 術語や記号などはほぼ [3] に従うので, 紙面の都合上, 説明の足らない部分は [3] を参照のこと.

4 マルチキャスト LNC(最小 LNC)

s からすべての $t \in T$ への**マルチキャスト**による**伝送レート**の上限は $h := \min_{t \in T} h_t$ となる [4]. そして, **線型ネットワーク符号** (LNC) を用いることで, レート h を達成するマルチキャスト伝送が可能である [1]. さらに, LNC の構成法も提案されている [2, 3]. 特に, $|\mathbf{F}| > |T|$ ならば, LNC を構成できることが知られている [5].

ネットワーク上の topological order に従って, 各 $e \in E$ に対し, local coding vector と global coding vector を定めることでマルチキャスト LNC は得られる [3] . 特に, global coding vector は伝送レート h に対応させて $\mathbf{F}$ 上の h **次元ベクトル**とする. 各 $t \in T$ に対し, s **から** t **への** h **本の** link-disjoint-path 上のリンクに付随する global coding vector より, $\mathbf{F}$ 上の正則な $h \times h$ **伝送行列** B_t が定まる. これより, s からの送信シンボル列 $y^h \in \mathbf{F}^h$ と t での受信シンボル列 $z_t^h \in \mathbf{F}^h$ の関係は, 次のように表すことができる:

$$\begin{array}{ccc} \mathbf{F}^h & \stackrel{B_t}{\rightarrow} & \mathbf{F}^h \\ y^h & \mapsto & z_t^h = y^h B_t \end{array}$$

上記の伝送行列 B_t を与える符号化を**マルチキャスト LNC** 又は**最小 LNC** ということにしよう. s から t へのデータ伝送の一連の流れは以下の通り: s で生成された**情報シンボル列** $x^h \in \mathbf{F}^h$ を**送信シンボル列** $y^h = x^h I_h \in \mathbf{F}^h$ に符号化し, s から y^h を送信する. t では**受信シンボル列** $z_t^h = y^h B_t \in \mathbf{F}^h$ を受信し, B_t^{-1} を用いて z_t^h から $z_t^h B_t^{-1} = x^h$ を復元する. ここで, I_h と B_t^{-1} はそれぞれ $h \times h$ 単位行列と B_t の逆行列を表す. 一連の操作を以下に示す:

$$\begin{array}{ccccccc} \mathbf{F}^h & \stackrel{I_h}{\rightarrow} & \mathbf{F}^h & \stackrel{B_t}{\rightarrow} & \mathbf{F}^h & \stackrel{B_t^{-1}}{\rightarrow} & \mathbf{F}^h \\ x^h & \mapsto & y^h & \mapsto & z_t^h & \mapsto & z_t^h B_t^{-1} \end{array}$$

5 最大 LNC

本節では, 前節にて説明したマルチキャスト LNC を一般化したものを考える. まず, 最大流の列 $\{h_t \mid t \in T\}$ の最大値を考え, その値を $\overline{h} := \max_{t \in T} h_t$ とする. そして, global coding vector を $\mathbf{F}$ 上の $\overline{h}$ **次元ベクトル**とする. 各 $t \in T$ に対し, s **から** t **への** h_t **本の** link-disjoint-path 上のリンクに付随する global coding vector より, $\text{rank} H_t = h_t$ を満たす $\mathbf{F}$ 上の $\overline{h} \times h_t$ **伝送行列** H_t を得ることができる. これより, s からの送信シンボル列 $y^{\overline{h}} \in \mathbf{F}^{\overline{h}}$ と t での受信シンボル列 $z_t^{h_t} \in \mathbf{F}^{h_t}$ の関係は, 次のように表すことができる:

$$\begin{array}{ccc} \mathbf{F}^{\overline{h}} & \stackrel{H_t}{\rightarrow} & \mathbf{F}^{h_t} \\ y^{\overline{h}} & \mapsto & z_t^{h_t} = y^{\overline{h}} H_t \end{array}$$

上記の伝送行列 H_t を与える符号化を**最大 LNC** ということにしよう. このとき, 定理 2.1 より, 任意の非負整数 k に対し, $|\mathbf{F}| > |\{t \mid t \in T,\ h_t \geq k\}|$ ならば,
$\text{rank} GH_t = k \text{ for all } t \in \{t \mid t \in T,\ h_t \geq k\}$
を満たす $\mathbf{F}$ 上の $k \times \overline{h}$ **符号化行列** G が存在する. さらに, $\text{rank} GH_t = k$ より, $(GH_t)(GH_t)^{-1} = I_k$ を満たす $h_t \times k$ 行列 $(GH_t)^{-1}$ が存在する. このような G を用いた s から t へのデータ伝送の流れは以下の通り: s で生成された情報シンボル列 $x^k \in \mathbf{F}^k$ を G を用いて送信シンボル列 $y^{\overline{h}} = x^k G \in \mathbf{F}^{\overline{h}}$ に符号化し, s から $y^{\overline{h}}$ を送信する. t では受信シンボル列 $z_t^{h_t} = y^{\overline{h}} H_t \in \mathbf{F}^{h_t}$ を受信し, $z_t^{h_t}$ から $z_t^{h_t}(GH_t)^{-1} = x^k$ を復元することができる. 一連の操作を以下に示す:

$$\begin{array}{ccccccc} \mathbf{F}^k & \stackrel{G}{\rightarrow} & \mathbf{F}^{\overline{h}} & \stackrel{H_t}{\rightarrow} & \mathbf{F}^{h_t} & \stackrel{(GH_t)^{-1}}{\rightarrow} & \mathbf{F}^k \\ x^k & \mapsto & y^{\overline{h}} & \mapsto & z_t^{h_t} & \mapsto & z_t^{h_t}(GH_t)^{-1} \end{array}$$

明らかに, $k \leq h$ のとき, $\{t \mid t \in T,\ h_t \geq k\} = T$ である. これより, 最大 LNC からマルチキャスト LNC を構成できる. 以上より, 符号化行列 G を用いて最大 LNC からマルチキャスト LNC を構成できる.

6 ブロードキャスト LNC

本節で述べる**ブロードキャスト**によるデータ伝送の枠組みは [1] において述べられているものである。

前処理として, 最大 LNC が既に構成されているものと仮定する. このとき, 以下の定理が成り立つ.

定理 6.1 $|\mathbf{F}| > |T|$ ならば, すべての伝送行列 $H_t, t \in T$ を変更することなく, 次に示すデータ伝送が可能である: すべての $t \in T$ に対し, s から t へメッセージを伝送レート h_t で伝送することが可能である. ∎

例えば, $|\{h_t \mid t \in T\}| = 3$ の場合を考えよう. 3 種類の最大流を $h_1 > h_2 > h_3$ と表し, $T_i := \{t \mid t \in T,\ h_t = h_i\}$, $i = 1, 2, 3$ とする. h_1, h_2, h_3 の最小公倍数を L とし, パラ

*e-mail: kuri@ice.uec.ac.jp
†〒 182-8585 東京都 調布市 調布ヶ丘 1-5-1

メータ $(d_1, d_2, d_3) := (h_1, h_1 - h_2, h_2 - h_3)$ と $(c_1, c_2, c_3) := (L/h_1, L/h_2 - L/h_1, L/h_3 - L/h_2)$ を定める． これより，$(L/h_1, L/h_2, L/h_3) = (c_1, c_1 + c_2, c_1 + c_2 + c_3)$ である．

ブロードキャストを実現するために**補助行列** F_i, $i = 2, 3$ と**符号化行列** G_i, $i = 1, 2, 3$ の 2 種類を以下のように定める．

1. $\mathbf{F}$ 上の $\overline{h} \times d_i$ 行列 F_i, $i = 2, 3$ は以下を満たす:
   i. rank $[H_{t_2} F_2] = \overline{h}$ for all $t_2 \in T_2$,
   ii. rank $[H_{t_3} F_3 F_2] = \overline{h}$ for all $t_3 \in T_3$.
   ここで，“[”, “]” を用いた $[H_{t_2} F_2]$ は H_{t_2} と F_2 を部分行列としてもつ $\overline{h} \times \overline{h}$ 行列を表す．以下同様．
2. $\mathbf{F}$ 上の $h_i \times \overline{h}$ 行列 G_i, $i = 1, 2, 3$ は以下を満たす:
   i. rank$G_1 H_{t_1} = h_1$ for all $t_1 \in T_1$,
   ii. rank$G_1[H_{t_2} F_2] = h_1$, rank$G_2 H_{t_2} = h_2$ for all $t_2 \in T_2$,
   iii. rank$G_1[H_{t_3} F_3 F_2] = h_1$, rank$G_2[H_{t_3} F_3] = h_2$, rank$G_3 H_{t_3} = h_3$ for all $t_3 \in T_3$.

定理 2.1 より，$|\mathbf{F}| > |T|$ のとき，上記の条件を満たす行列 G_i, $i = 1, 2, 3$ が存在する．また，上記の条件を満たす行列 F_i, $i = 2, 3$ は最大 LNC を構成する際に容易に構成できる．以下に各段階での手続きを記す．

(情報): 各 $t \in T$ に対して**メッセージ** $(x_1, \ldots, x_L) \in \mathbf{F}^L$ を L/h_t 単位時間で伝送するために，情報シンボル列 $x_1, \ldots, x_L$ を以下のように加工し，**データ行列** D_1, D_2, D_3 で表す．

1. $x_1, \ldots, x_L$ を $c_1 \times h_1$ 行列 D_1 の各成分に対応するように並び換える．ここで，$L = c_1 h_1$.
2. $D_2^{(1)} := D_1 G_1 F_2$ として得られる $t_1 d_2$ 個の成分を $c_2 \times h_2$ 行列 D_2 に並べ換える．ここで $t_1 d_2 = c_2 h_2$.
3. $D_3^{(1)} := D_1 G_1 F_3$, $D_3^{(2)} := D_2 G_2 F_3$ として得られるそれぞれ $t_1 d_3$ 個と $t_2 d_3$ 個の成分を $c_3 \times h_3$ 行列 D_3 に並べ換える．ここで，$(t_1 + t_2) d_3 = c_3 h_3$.

(符号化と送信): データ行列 D_1, D_2, D_3 をそれぞれ符号化行列 G_1, G_2, G_3 を用いて符号化する．そして，時刻 m, $1 \le m \le c_1 + c_2 + c_3$, に s から送信する長さ $\overline{h}$ の送信シンボル列を $(c_1 + c_2 + c_3) \times \overline{h}$ 行列 $\begin{pmatrix} D_1 G_1 \\ D_2 G_2 \\ D_3 G_3 \end{pmatrix}$ の m 行目の行ベクトルに対応させる．

(受信):

1. 各 $t_1 \in T_1$ では，時刻 $1 \sim c_1$ までに，$Z_{t_1}^{(1)} := D_1 G_1 H_{t_1}$ を受信する．
2. 各 $t_2 \in T_2$ では，時刻 $1 \sim c_1$, $c_1 + 1 \sim c_1 + c_2$ までに，それぞれ $Z_{t_2}^{(1)} := D_1 G_1 H_{t_2}$, $Z_{t_2}^{(2)} := D_2 G_2 H_{t_2}$ を受信する．
3. 各 $t_3 \in T_3$ では，時刻 $1 \sim c_1$, $c_1 + 1 \sim c_1 + c_2$, $c_1 + c_2 + 1 \sim c_1 + c_2 + c_3$ までに，それぞれ $Z_{t_3}^{(1)} := D_1 G_1 H_{t_3}$, $Z_{t_3}^{(2)} := D_2 G_2 H_{t_3}$, $Z_{t_3}^{(3)} := D_3 G_3 H_{t_3}$ を受信する．

(復元): 下記の手続きで受信データからメッセージを復元する．

1. 各 $t_1 \in T_1$ では，H_{t_1}, G_1 を既知とする．
   $Z_{t_1}^{(1)} (G_1 H_{t_1})^{-1} = D_1$.
2. 各 $t_2 \in T_2$ では，H_{t_2}, G_1, G_2, F_2 を既知とする．
   $Z_{t_2}^{(2)} (G_2 H_{t_2})^{-1} = D_2$,
   $[Z_{t_2}^{(1)} D_2^{(1)}] (G_2 [H_{t_2} F_2])^{-1} = D_1$.
3. 各 $t_3 \in T_3$ では，$H_{t_3}, G_1, G_2, G_3, F_2, F_3$ を既知とする．
   $Z_{t_3}^{(3)} (G_3 H_{t_3})^{-1} = D_3$,
   $[Z_{t_3}^{(2)} D_3^{(2)}] (G_2 [H_{t_3} F_3])^{-1} = D_2$,
   $[Z_{t_3}^{(1)} D_3^{(1)} D_2^{(1)}] (G_1 [H_{t_3} F_3 F_2])^{-1} = D_1$.

上記の手続きにより，すべての $t \in T$ に対してメッセージ $(x_1, \ldots, x_L)$ をレート h_t で伝送することが可能である．以上より，符号化行列と補助行列を用いて最大 LNC からブロードキャスト LNC を構成できる．

7 ロバスト LNC

本節で述べる**ロバスト** LNC の枠組み及び構成法は最初に [2] において与えられた．その後，異なるアプローチでの構成法が [3] においても与えられた．ロバスト LNC は link failure に対応する符号である．ロバスト LNC で仮定する link failure とは，リンク故障で伝送データを伝送できないことを指している．理論的には，link failure が発生した unit capacity のリンクでは，そのリンク上を流れる $\mathbf{F}$ の要素である伝送シンボルが常に固定値の零元 $0 \in \mathbf{F}$ に変化すると仮定する．そして，シンク側では，受信データから送信データを復元するための**補助情報**として，発生した複数の link failure の位置情報を示す link failure pattern F を知ることができると仮定する．ネットワーク上で発生する link failure pattern の全体の集合を $\mathcal{F}$ とする．

前処理として，最大 LNC が既に構成されているものと仮定する．一般に，link failure pattern $F \in \mathcal{F}$ が発生することで，各 $t \in T$ では既存の伝送行列 H_t が変化する．それは，t と F により，$\overline{h} \times h_t$link failure 伝送行列 H_t^F が一意に定まり，その結果，H_t から $(H_t - H_t^F)$ に変化する．したがって，link failure pattern $F \in \mathcal{F}$ が発生した場合，各 $t \in T$ に対し，s から t への送受信シンボル列 $y^{\overline{h}}$ と $z_t^{h_t}$ の関係は以下のように表される:

$$\begin{array}{ccccc} \mathbf{F}^{\overline{h}} & \xrightarrow{(H_t - H_t^F)} & \mathbf{F}^{h_t} \\ y^{\overline{h}} & \mapsto & z_t^{h_t} = y^{\overline{h}} (H_t - H_t^F) \end{array}$$

定理 2.2 より，rank $(H_t - H_t^F) \ge h_t -$ rank H_t^F が成り立つ．一方，ある非負整数 k に対し，以下が成り立つと仮定する:
$h -$ rank $H_t^F \ge k$ for all $t \in T$, $F \in \mathcal{F}$.
さらに，$\mathbf{F}$ 上の $k \times \overline{h}$ 符号化行列 G を以下を満たすものとする:
rank $G(H_t - H_t^F) = k$ for all $t \in T$, $F \in \mathcal{F}$.
Rank $(H_t - H_t^F) \ge k$ と定理 2.1 より，$|\mathbf{F}| > |T| \times |\mathcal{F}|$ のとき，上記の条件を満たす G が存在する． このとき，G を用いて情報シンボル列 x^k を送信シンボル列 $y^{\overline{h}} = x^k G$ に符号化し，s から $y^{\overline{h}}$ を送信する．その後，各 $t \in T$ において，発生した link failure pattern F の補助情報を得られる場合，$(G((H_t - H_t^F))(G(H_t - H_t^F))^{-1} = I_k$ を満たす $h_t \times k$ 行列 $(G(H_t - H_t^F))^{-1}$ を用いて，受信シンボル列 $z_t^{h_t}$ から x^k を復元することができる．一連の操作を以下に示す:

$$\begin{array}{ccccccc} \mathbf{F}^k & \xrightarrow{G} & \mathbf{F}^{\overline{h}} & \xrightarrow{(H_t - H_t^F)} & \mathbf{F}^{h_t} & \xrightarrow{(G(H_t - H_t^F))^{-1}} & \mathbf{F}^k \\ x^k & \mapsto & y^{\overline{h}} & \mapsto & z_t^{h_t} & \mapsto & z_t^{h_t} (G(H_t - H_t^F))^{-1} \end{array}$$

ゆえに，シンク t が符号化行列 G と発生した link failure pattern F の補助情報を得られるものと仮定するならば，すべての $t \in T$ に対し，任意の link failure pattern $F \in \mathcal{F}$ が発生しても，s から t へ情報 x^k を正しく伝送できる．以上より，符号化行列 G を用いて最大 LNC からロバスト LNC を構成できる．

8 結論

本稿では，符号化行列 G をネットワーク伝送の目的に応じて構成し，最大 LNC に適用することで，最大 LNC から直接にマルチキャスト LNC，ブロードキャスト LNC，ロバスト LNC のそれぞれを構成可能であることを示し，線型ネットワーク符号の構成において新しい知見を与えた．このことを応用の側面から考えると，ネットワーク中の中継ノードにおける符号化手続きを，最大 LNC として一度設定すれば，後にそれらの設定を変更することなく，ソースとシンクのみでそれぞれ符号化と復元の手続きを実行するだけで，目的の LNC を得ることができることを示している．

参考文献

[1] S.-Y.R.Li, and *et. al.*, “Linear network coding,” *IEEE Trans. on IT*, vol. 49, no. 2, pp.371-381, Feb. 2003.
[2] R.Koetter and M.Medard, “An Algebraic Approach to Network Coding”, *IEEE/ACM Trans. on Networking*, vol. 11, no. 5, pp.782-795, Oct. 2003.
[3] S.Jaggi, and *et. al.*, ”Polynomial time algorithms for multicast network code construction,” *IEEE Trans. IT*, vol. 51, no. 6, pp.1973-1982, Jun. 2005.
[4] R.Ahlswede and *et. al.*, “Network information flow,” *IEEE Trans. on IT*, vol. 46, no. 4, pp.1204-1216, Jul. 2000.
[5] T.Ho and *et. al.*, “Network coding from a network flow perspective,” *Proc. IEEE ISIT*, p.442, Yokohama, Japana, Jun./Jul. 2003.