# ネットワーク符号化とある種の線型変換 (改定版 作成日 2006/7/26/12:42)

栗原 正純

電気通信大学情報通信工学科，〒 182–8585 東京都調布市調布ヶ丘 1–5–1，kuri@ice.uec.ac.jp

**あらまし**　本稿では、ロバストでセキュアなネットワーク符号化の構成方法について議論する．マルチキャストネットワークに対応したネットワーク符号化が与えられたと仮定する．このとき，ロバストでセキュアなネットワーク符号化を構成するために，与えられたネットワーク符号化に対応したある種の正則行列を構成できる．ソースノードで生成された情報シンボルを，その行列を用いて線型変換することだけで，与えられた符号化を情報理論的にロバストでセキュアなネットワーク符号化に変更可能であることを示す．

**キーワード**　ネットワーク符号化，セキュアネットワーク符号化，ロバストネットワーク符号化，ロバスト変換，セキュア変換，

# On some robust and secure transformations for linear network coding

Masazumi KURIHARA

Dept. of Info. & Comm. Eng., Univ. of Electro-Comm., Chofu-shi, Tokyo, 182–8585 Japan, kuri@ice.uec.ac.jp

**Abstract**　In this paper we consider the problem of constructing some robust and secure network coding for a multicast network. Suppose that any linear network coding for the multicast network is given. Then a regular matrix corresponding to the given coding can be constructed to get some robust and secure network coding. We transform the information symboles only at the source node by using the matrix. We then show that the given coding can become an information theoretic robust and secure network coding.

**Key words**　Network coding, secure network coding, robust network coding, secure transformation, robust transformation

## 1. ま え が き

Cai and Yeung [1] は，情報理論的に安全なネットワーク符号化の問題を定式化し，その構成法を示した．それは，マルチキャスト通信が可能なネットワークにおいて，あるしきい値以下の本数の通信路 (リンク) を盗聴可能な者が存在すると仮定した場合における安全性の問題である．また，この問題が，暗号理論における秘密分散法と関連があることも述べている．

Feldman ら [2] は，ソースノードで生成された情報シンボル列をそのまま出力する前に，線型変換行列を用いて情報シンボル列を変換し，その後，その変換されたシンボル列を出力することを考えた．このとき，ある種の性質を持たせた変換行列を用いることで，必ずしも安全ではない与えられたネットワーク符号化を，Cai and Yeung [1] の提案と本質的に同等な安全なネットワーク符号化に変換可能であることを示した．その後，Bhattad ら [3] も，このような線型変換を用いて，安全なネットワーク符号化に関する類似の研究を行なっている．

また，原田と山本 [4] は，Cai and Yeung [1] による安全なネットワーク符号化の問題を，山本 [5] による秘密分散法に関連する問題に拡張し，しきい値以上の本数の通信路を盗聴されても情報理論的に安全な強いランプ型の安全なネットワーク符号化の構成法を提案した．その構成法は，最初から安全なネットワーク符号化を構成しようとするものであり，Feldman ら [2] や Bhattad ら [3] のように，線型変換行列を利用して，与えられたネットワーク符号化を安全なネットワーク符号化に変換しようとする手法とは異なる．

一方，Demchig [6] は，このような線型変換の別の利用法として，ロバスト性を考慮したネットワーク符号化の研究を行なった．本稿で扱うロバスト性とは，リンク切断などで，本来，すべての情報シンボルを復号するために必要なデータのすべてを受信できない場合でも，限られた受信データから幾つかの情報シンボルを一意に決定し復号可能とすることである．この意味で Koetter [7] らが述べているネットワーク符号化のロバスト性とは異なる．Demchig [6] は，ネットワーク中に発生したリンク切断によるシンクノードへの影響をできるだけ減らすには，ネットワークがどのような構造をもてばよいかの研究を行なった．文献 [6] では，リンク切断後に，その切断情報をもとに構成した変換行列を用いて，ソースノードで生成された情報シンボル列を変換した後に出力することで，その切断の影響を低減しようとしている．

本稿では，上記の研究結果を踏まえて，ソースノードで生成された情報シンボル列に，ある線型変換を施すことで，与えられたネットワーク符号化をある種のロバストでセキュアなネットワーク符号化に変更することを考える．そのために必要な線型変換の構成条件を示し，情報理論的にロバスト性と安全性を評価する．具体的には，ソースノードから出力する $m$ 個の情報シンボル列 $X^m$ とネットワーク中で観測する $k$ 個の観測シンボル列 $W^k$ に対し，$H(X^m|W^k)$ と $H(X^m)$ の関係を評価する．

本稿の構成は以下の通り．2. では，本稿で扱う線型変換行列について理解しやすいように，ネットワーク符号化とは切り離して，ロバスト性と安全性に関する線型変換行列の概念についてのみ説明する．3. では，前節で定義した線型変換行列の概念を利用し，与えられたネットワーク符号化をロバストでセキュアなネットワーク符号化に変更するための線型変換行列の構成条件を示し，その評価を行なう．4. では，本稿で扱う線型変換行列の応用として，マルチキャスト通信ではないネットワークの伝送可能性について述べる．5. は，むすびである．

## 2. 線型変換行列

本節では，本稿で扱う線型変換について理解しやすいように，ネットワーク符号化とは切り離して，ロバスト性と安全性を考慮した 2 種類の線型変換行列ついて説明する．今後用いる記号の説明として $A := B$ は，$A$ は $B$ により定義される，あるいは，$B$ により $A$ を定義する，を意味する．

### 2.1 符号化と復号化

情報源を有限体 $\mathbf{F}_q$ 上の離散的情報源とする．各 $X_1, \ldots, X_h$ を情報シンボルとし，長さ $h$ の行ベクトルを $X^h := (X_1, \ldots, X_h)$ とする．

$n$ 個の $\mathbf{F}_q$ 上の長さ $h$ の列ベクトル $\boldsymbol{g}_j$, $j = 1, \ldots, n$ は，次の条件を満たすものとする．ただし，$n \geq h$．　任意の $h$ 個の

$\boldsymbol{g}_{j_1},\dots,\boldsymbol{g}_{j_h} \in \{\boldsymbol{g}_1,\dots,\boldsymbol{g}_n\}$ に対し，

$$\mathrm{rank}[\boldsymbol{g}_{j_1}\cdots\boldsymbol{g}_{j_h}] = h \tag{1}$$

このとき，符号化を以下の関数で定義する．各 $j=1,\dots,n$ に対し，

$$\begin{array}{rccc}\varphi_{(j)}: & \mathbf{F}_q^h & \to & \mathbf{F}_q \\ & X^h & \mapsto & V_j\end{array} \tag{2}$$

$$\varphi_{(j)}(X^h) := X^h\boldsymbol{g}_j =: V_j \tag{3}$$

$V_j$ を $\boldsymbol{g}_j$ に関する符号シンボルとよぶ．符号化の手続きで用いる $\{\boldsymbol{g}_1,\dots,\boldsymbol{g}_n\}$ の情報は復号側にも既知と仮定する．

一方，任意の $h$ 個の $j_1,\dots,j_h \in \{1,\dots,n\}$ に対し，長さ $h$ の行ベクトル $V^h_{(j_1,\dots,j_h)} = (V_{j_1},\dots,V_{j_h})$ と $h\times h$ 行列 $G_{(j_1,\dots,j_h)} = [\boldsymbol{g}_{j_1}\cdots\boldsymbol{g}_{j_h}]$ と記す．そして，復号化を以下の関数で定義する．

$$\begin{array}{rccc}\psi_{(j_1,\dots,j_h)}: & \mathbf{F}_q^h & \to & \mathbf{F}_q^h \\ & V^h_{(j_1,\dots,j_h)} & \mapsto & X^h\end{array} \tag{4}$$

$$\psi_{(j_1,\dots,j_h)}(V^h_{(j_1,\dots,j_h)}) := V^h_{(j_1,\dots,j_h)}G^{-1}_{(j_1,\dots,j_h)} \tag{5}$$

上記の符号化・復号化の定義より，任意の $h$ 個の符号シンボルから情報 $X^h$ を一意に復号可能であることは明らか．

## 2.2 ロバスト変換

はじめに，ロバストという言葉を使用する意味について説明する．前節では，$h$ 個の情報シンボルから $n$ 個の符号シンボルを与える符号化を定義した．この符号化では，任意の $h$ 個の符号シンボルから $h$ 個の情報シンボルを一意に復号可能である．しかし，一般に，$h$ より少ない符号シンボルからでは，情報シンボルの一部分も一意に復号可能であるとは限らない．そこで，ある特定の $g$ 個の符号シンボルならば，情報シンボルの一部分である $f$ 個を一意に復号可能であるような符号化・復号化の方法を実現することを目的とする．このとき，特定の符号シンボルからのみの復号に限定され，さらに，特定の情報シンボルの一部分しか得ることができないのではあるが，$h$ より少ない符号シンボルからでも情報シンボルの一部分を一意に復号可能という意味でロバスト (丈夫な) という言葉を用いる．Demchig [6] は，本節で述べる線型変換を利用したロバスト性に関して最初に研究を行なった．

### 2.2.1 問題設定 (ロバスト)

次の二つの性質 P1, 2 を満たすような符号化・復号化について考える．

[**性質** 2.1] **P1**) 集合 $\{1,\dots,n\}$ の中から任意の $g$ 個の $t_1,\dots,t_g$ を選び，固定し，添字集合 $T := \{t_1,\dots,t_g\}$ を定義する．また，$\{1,\dots,h\}$ の中から任意の $f$ 個の $s_1,\dots,s_f$ を選び，固定し，添字集合 $S := \{s_1,\dots,s_f\}$ を定義する．ただし，$f \leqq g$. このとき，特定の $g$ 個の符号シンボル $W_T^g = (W_{t_1},\dots,W_{t_g})$ から特定の $f$ 個の情報シンボル $X_S^f = (X_{s_1},\dots,X_{s_f})$ を一意に復号可能である．すなわち，$H(X_S^f|W_T^g) = 0$. 言い換えると，次の復号化の関数が存在する．

$$\begin{array}{rccc}\xi_T: & \mathbf{F}_q^g & \to & \mathbf{F}_q^f \\ & W_T^g & \mapsto & X_S^f\end{array} \tag{6}$$

**P2**) 任意の $h$ 個の符号シンボルから情報シンボル $X^h$ を一意に復号可能である．すなわち，$H(X^h|W^h_{(j_1,\dots,j_h)}) = 0$. ∎

文献 [6] では，$g=f$ の場合を扱っている ( [6] の定理 2,3 を参照).

### 2.2.2 ロバスト変換行列の構成

いま，既存 (2.1 節) の符号化手続きで用いる $\{\boldsymbol{g}_1,\dots,\boldsymbol{g}_n\}$ をそのまま利用し，性質 P1,2 を満たす符号化・復号化について考える．

そこで，次の二つの条件 C1, 2 を満たす $h$ 個の $\mathbf{F}_q$ 上の長さ $h$ の列ベクトル $\boldsymbol{f}_i$, $i=1,\dots,h$ を定義する．

[**条件** 2.2] **C1**) $\mathrm{rank}\,[\boldsymbol{f}_1\cdots\boldsymbol{f}_h] = h$.

**C2**) 以下の関係を満たす $\mathbf{F}_q$ 上の $g\times f$ 行列 $D$ が存在する．

$$\left[\boldsymbol{g}_{t_1}\cdots\boldsymbol{g}_{t_g}\right]D = \left[\boldsymbol{f}_{s_1}\cdots\boldsymbol{f}_{s_f}\right] \tag{7}$$

条件 C1,2 を満たすベクトル $\boldsymbol{f}_i$, $i=1,\dots,h$ から構成される $h\times h$ 行列を $F := [\boldsymbol{f}_1\cdots\boldsymbol{f}_h]$ と定義し，ロバスト変換行列とよぶことにしよう．

### 2.2.3 符 号 化

ロバスト変換行列 $F$ を用いて，$\boldsymbol{g}_j$ に関する符号シンボル $V_j$ に代わる，新たな符号シンボル $W_j$ を以下のように定義する．

$$W_j := X^hF^{-1}\boldsymbol{g}_j = \varphi_{(j)}(X^hF^{-1}) \tag{8}$$

### 2.2.4 復 号 化

復号側は，$\{\boldsymbol{g}_1,\dots,\boldsymbol{g}_n\}$ の情報以外に，$F$ と $D$ の情報も既知と仮定する．

1) 以下の手続きにより，特定の $g$ 個の符号シンボル $W_T^g$ から情報シンボル $X_S^f$ を一意に復号可能である．

$$\begin{aligned}\xi_T(W_T^g) &:= W_T^gD && (9)\\ &= X^hF^{-1}[\boldsymbol{g}_{t_1}\cdots\boldsymbol{g}_{t_g}]D && (10)\\ &= X^hF^{-1}[\boldsymbol{f}_{s_1}\cdots\boldsymbol{f}_{s_f}] && (11)\\ &= X_S^f && (12)\end{aligned}$$

2) 以下の手続きにより，任意の $h$ 個の符号シンボル $W^h_{(j_1,\dots,j_h)}$ から情報シンボル $X^h$ を一意に復号可能である．

$$\begin{aligned}&\psi_{(j_1,\dots,j_h)}(W^h_{(j_1,\dots,j_h)})\times F && (13)\\ &= X^hW^h_{(j_1,\dots,j_h)}G^{-1}_{(j_1,\dots,j_h)}F = X^h && (14)\end{aligned}$$

以上より，ロバスト変換行列 $F$ は，性質 P1,2 を満たすことが分かる．

## 2.3 セキュア変換

前節において考えたロバスト性とは別に，本節では，安全性を考慮した場合の線型変換行列について考える．以下に記述する内容は，文献 [5] の秘密分散システムに関する記述内容に含まれる内容である．

### 2.3.1 問題設定 (セキュア)

情報源を $\mathbf{F}_q$ 上の離散的無記憶情報源とする．さらに，その情報源から出力される各情報シンボルは等確率で生起するものとする．各 $X_1,\dots,X_{h-r}$ を情報シンボルとし，各 $Y_1,\dots,Y_r$ を $\mathbf{F}_q$ 上の一様乱数とする．このとき，任意の $m$ 個の情報シンボル $X_{i_1},\dots,X_{i_m}$ に対し，$H(X_{i_1},\dots,X_{i_m}) = m\log q$ である．前節で定義した $X^h$ とは異なり，改めて，長さ $h$ の行ベクトル $X^h := (X_1,\dots,X_{h-r},Y_1,\dots,Y_r)$ を定義する．この変更に伴い，性質 P1 にて定義した $f$ 個の $s_1,\dots,s_f$ は，$s_1,\dots,s_f \in \{1,\dots,h-r\}$ を満たすように変更し，改めて，$S := \{s_1,\dots,s_f\}$ と定義する．

以下に示す性質をもつ符号化・復号化を実現させることを考える．

[**性質** 2.3] **P3**) 任意の $m$ 個の $i_1,\dots,i_m \in \{1,\dots,h-r\}$ に対する，$(X_{i_1},\dots,X_{i_m})$ を考える．また，任意の $k$ 個の $j_1,\dots,j_k \in \{1,\dots,n\}$ に対する，$(W_{j_1},\dots,W_{j_k})$ を考える．簡単のために，$X^m = (X_{i_1},\dots,X_{i_m})$, $W^k = (W_{j_1},\dots,W_{j_k})$ と記す．このとき，以下が成り立つ．

**P3-1**) $m = h-r$ and $k \leqq r$ のとき，

$$H(X^m|W^k) = H(X^m) \tag{15}$$

**P3-2**) $m = h-r$ and $r \leqq k < h$ のとき，

$$H(X^m|W^k) = \frac{h-k}{m}H(X^m) \tag{16}$$

**P3-3**) $m+k = h$ のとき，

$$H(X^m|W^k) = H(X^m) \tag{17}$$

∎

### 2.3.2 セキュア変換行列の構成

性質 2.3 の各性質を満たす符号化・復号化について考える．そこで，次のような条件を考える．

［**条件** 2.4］ **C3**) 任意の $k$ 個の $\boldsymbol{g}_{j_1},\ldots,\boldsymbol{g}_{j_k}\in\{\boldsymbol{g}_1,\ldots,\boldsymbol{g}_n\}$ に対し，$\mathrm{rank}\,[\boldsymbol{f}_1\cdots\boldsymbol{f}_{h-r}\boldsymbol{g}_{j_1}\cdots\boldsymbol{g}_{j_k}]=h-r+k$ を満たす．ただし，$k\leqq r$ である．

**C4**) 任意の $k$ 個の $\boldsymbol{g}_{j_1},\ldots,\boldsymbol{g}_{j_k}\in\{\boldsymbol{g}_1,\ldots,\boldsymbol{g}_n\}$ に対し，$\mathrm{rank}\,[\boldsymbol{f}_1\cdots\boldsymbol{f}_{h-r}\boldsymbol{g}_{j_1}\cdots\boldsymbol{g}_{j_k}]=h$ を満たす．ただし，$r\leqq k<h$ である．

**C5**) 任意の $h$ 個の $\boldsymbol{c}_1,\ldots,\boldsymbol{c}_h\in\{\boldsymbol{f}_1,\ldots,\boldsymbol{f}_{h-r},\boldsymbol{g}_1,\ldots,\boldsymbol{g}_n\}$ に対し，$\mathrm{rank}\,[\boldsymbol{c}_1\cdots\boldsymbol{c}_h]=h$ を満たす． ∎

### 2.3.3 符号化・復号化

符号化・復号化の手続きは，それぞれ 2.2.3 節と 2.2.4 節の 2) における手続きと同じである．

このとき，山本 [5] により，次のことが分かっている．行列 $F$ が条件 C1,3 を満たす場合，性質 P3-1 を満たす．行列 $F$ が条件 C1,4 を満たす場合，性質 P3-2 を満たす．そして，行列 $F$ が条件 C1,5 を満たす場合，性質 P3-3 を満たす．このような行列 $F$ をセキュア変換行列とよぶことにする．

［**Remark** 2.5］ (安全なネットワーク符号化との関係について) ネットワーク符号化とは切り離して，安全なネットワーク符号化 [1]〜[4] において扱われている安全性のみを，行列 $F$ の満たす条件で分類すると以下の通りである．文献 [1]〜[3] において扱う安全性は，行列 $F$ が条件 C1,3 を満たす場合で，性質 P3-1 を満たす．一方，原田と山本 [4] は，文献 [1]〜[3] において扱う安全性が，行列 $F$ が条件 C1,4 を満たすときの性質 P3-2 も満たすことを指摘した．さらに，彼らが提案した安全性は，行列 $F$ が条件 C1,5 を満たす場合と同等であり，性質 P3-3 を満たす．これは，文献 [1]〜[3] の安全性を強めたものになっている．これらの秘密分散法に関する安全性の強さについては，文献 [5] において述べられている． ∎

## 2.4 準備 (線型空間)

以下の節で用いる線型代数や線型空間に関する基礎的な事実を確認のために以下に記述する．

記号 $A$, $B$, $H$ をそれぞれ $\mathbf{F}_q$ 上の $h\times m$ 行列，$h\times n$ 行列，$n\times m$ 行列とする．ただし，$n\leqq h$, $m\leqq h$, $m\leqq n$ を満たすものとする．$A$, $B$, $H$ に対し，$A=BH$ という関係を考える．このとき，次の 2 点が成り立つ．1) $\mathrm{rank}\,A=m$ かつ $\mathrm{rank}\,B=n$ ならば $\mathrm{rank}\,H=m$ が成り立つ．2) $\mathrm{rank}\,B=n$ かつ $\mathrm{rank}\,H=m$ ならば $\mathrm{rank}\,A=m$ が成り立つ．

$\mathbf{F}_q$ 上の線型空間 $V$ の空でない部分集合 $S=\{\boldsymbol{x}_1,\ldots,\boldsymbol{x}_k\}$, $|S|=k$, に対し，$S$ から生成される部分空間を

$$\begin{aligned}\langle S\rangle &= \langle\boldsymbol{x}_1,\ldots,\boldsymbol{x}_k\rangle\\ &:= \{\alpha_1\boldsymbol{x}_1+\cdots+\alpha_k\boldsymbol{x}_k|\alpha_1,\ldots,\alpha_k\in\mathbf{F}_q\}\end{aligned}$$

と定義する．次に，線型空間 $V$ の部分空間 $W_1$, $W_2$ の共通部分空間を

$$W_1\cap W_2 := \{\boldsymbol{x}|\boldsymbol{x}\in W_1 \text{ and } \boldsymbol{x}\in W_2\}$$

と定義する．最後に，部分空間 $W_1$, $W_2$ の和空間を

$$W_1+W_2 := \{\boldsymbol{x}_1+\boldsymbol{x}_2|\boldsymbol{x}_1\in W_1,\ \boldsymbol{x}_2\in W_2\}$$

と定義する．

## 2.5 ロバストでセキュアな変換行列

本節では，前節までに定義した変換行列のロバスト性と安全性の両方の性質を考慮した変換行列を考えよう．まず，線型空間 $F_q^h$ の部分空間やその基底について以下のように定義する．ロバストに対応した添字集合 $T$ により定まるベクトル集合を $G_0=\{\boldsymbol{g}_j|j\in T\}=\{\boldsymbol{g}_{0,1},\ldots,\boldsymbol{g}_{0,g}\}$ とする．そして，集合 $\{\boldsymbol{g}_1,\ldots,\boldsymbol{g}_n\}$ の任意の部分集合 $G_j$ の要素を $G_j=\{\boldsymbol{g}_{j_1},\ldots,\boldsymbol{g}_{j_{k_j}}\}=\{\boldsymbol{g}_{j,1},\ldots,\boldsymbol{g}_{j,k_j}\}\subset\{\boldsymbol{g}_1,\ldots,\boldsymbol{g}_n\}$ と表す．ただし，$|G_j|=k_j<h$ を満たすものとする．ここでは，添字 $j$ に対し，$\boldsymbol{g}_{j,p}=\boldsymbol{g}_{j_p}$, $p=1,\ldots,k_j$ という対応を考えている．このとき，部分集合 $G_j$ に対し，部分空間 $\langle G_0\rangle$ と $\langle G_j\rangle$ の共通部分空間 $\langle G_0\rangle\cap\langle G_j\rangle$ の次元を $\dim\langle G_0\rangle\cap\langle G_j\rangle:=v_j$ とする．そして，共通部分空間 $\langle G_0\rangle\cap\langle G_j\rangle$ の基底を $\boldsymbol{v}_{j,1},\ldots,\boldsymbol{v}_{j,v_j}$ とする．さらに，その基底 $\boldsymbol{v}_{j,1},\ldots,\boldsymbol{v}_{j,v_j}$ を拡大して，部分空間 $\langle G_0\rangle$ の基底を $\boldsymbol{u}_{j,1},\ldots,\boldsymbol{u}_{j,g-v_j},\boldsymbol{v}_{j,1},\ldots,\boldsymbol{v}_{j,v_j}$ とする．同様に，$\langle G_j\rangle$ の基底を $\boldsymbol{v}_{j,1},\ldots,\boldsymbol{v}_{j,v_j},\boldsymbol{w}_{j,1},\ldots,\boldsymbol{w}_{j,k_j-v_j}$ とする．

上記の準備より，条件 C1,2 以外に，さらに，以下の条件 C6,7 を満たす変換行列 $F$ を考える．

［**条件** 2.6］ **C6**) 任意の部分集合 $G_j=\{\boldsymbol{g}_{j,1},\ldots,\boldsymbol{g}_{j,k_j}\}\subset\{\boldsymbol{g}_1,\ldots,\boldsymbol{g}_n\}$, $|G_j|=k_j<h$, に対し，以下が成り立つ．任意の $\ell$ 個の $\boldsymbol{c}_1,\ldots,\boldsymbol{c}_\ell\in\{\boldsymbol{f}_i\mid i\in S\}$ に対し，$\mathrm{rank}\left[\boldsymbol{c}_1\cdots\boldsymbol{c}_\ell\boldsymbol{v}_{j,1}\cdots\boldsymbol{v}_{j,v_j}\right]=\ell+v_j$ を満たす．ただし，$\ell\leqq g-v_j$.

**C7**) 任意の部分集合 $G_j=\{\boldsymbol{g}_{j,1},\ldots,\boldsymbol{g}_{j,k_j}\}\subset\{\boldsymbol{g}_1,\ldots,\boldsymbol{g}_n\}$, $|G_j|=k_j<h$, に対し，以下が成り立つ．任意の $h$ 個の $\boldsymbol{c}_1,\ldots,\boldsymbol{c}_\ell\in\{\boldsymbol{f}_i\mid i\in\{1,\ldots,h-r\}\setminus S\}$ に対し，
$\mathrm{rank}\left[\boldsymbol{c}_1\cdots\boldsymbol{c}_\ell\boldsymbol{u}_{j,1}\cdots\boldsymbol{u}_{j,g-v_j}\boldsymbol{v}_{j,1}\cdots\boldsymbol{v}_{j,v_j}\boldsymbol{w}_{j,1}\cdots\boldsymbol{w}_{j,k_j-v_j}\right]=\ell+g+k_j-v_j$ を満たす．ただし，$\ell\leqq h-(\ell+g+k_j-v_j)$. ∎

［**補題** 2.7］ 条件 2.6 C6) において，以下の i) と ii) は同値である．i) $\mathrm{rank}\,[\boldsymbol{c}_1\cdots\boldsymbol{c}_\ell\boldsymbol{v}_{j,1}\cdots\boldsymbol{v}_{j,v_j}]=\ell+v_j$. ii) $\mathrm{rank}\,[\boldsymbol{c}_1\cdots\boldsymbol{c}_\ell\boldsymbol{g}_{j,1}\cdots\boldsymbol{g}_{j,k_j}]=\ell+k_j$.

(証明) 補題 3.5 の証明を参照． ∎

条件 C1,2,6,7 を満たす行列 $F$ を用いて符号化を定める．任意の部分集合 $G_j$ の要素 $\boldsymbol{g}_{j,p}$, $p=1,\ldots,k_j$ に対応する符号シンボルを $W_{j,p}=X^hF^{-1}\boldsymbol{g}_{j,p}$ と定める．

［**性質** 2.8］ **P4**) 任意の $m$ 個の $i_1,\ldots,i_m\in\{1,\ldots,h-r\}$ に対する，$(X_{i_1},\ldots,X_{i_m})$ を考える．また，任意の部分集合 $G_j=\{\boldsymbol{g}_{j,1},\ldots,\boldsymbol{g}_{j,k_j}\}\subset\{\boldsymbol{g}_1,\ldots,\boldsymbol{g}_n\}$, $|G_j|=k_j<h$, に対応する符号シンボル列 $(W_{j,1},\ldots,W_{j,k_j})$ を考える．ただし，$m+k_j\leqq h$ とする．簡単のために，$X^m=(X_{i_1},\ldots,X_{i_m})$, $W_j^k=(W_{j,1},\ldots,W_{j,k_j})$ と記す．このとき，以下が成り立つ．

$$H(X^m|W_j^{k_j})=\frac{d-k_j}{m}H(X^m) \tag{18}$$

ただし，

$$d:=\mathrm{rank}\left[\boldsymbol{f}_{i_1}\cdots\boldsymbol{f}_{i_m}\boldsymbol{g}_{j,1}\cdots\boldsymbol{g}_{j,k_j}\right]\ (\leqq h) \tag{19}$$ ∎

［**定理** 2.9］ 条件 C1,2,6,7 を満たす行列 $F$ を用いて符号化を行なうことで，性質 P1,2,4 を満たす符号化・復号化が可能である．

(証明) 付録 1. に記す． ∎

情報シンボル列 $X^m$ に関する添字集合 $\{i_1,\ldots,i_m\}$ に対応する集合 $\{\boldsymbol{f}_{i_1},\ldots,\boldsymbol{f}_{i_m}\}$ を次のように 2 個の集合に直和分割する．

$$\begin{aligned}u &:= |\{\boldsymbol{f}_{i_1},\ldots,\boldsymbol{f}_{i_m}\}\cap\{\boldsymbol{f}_i|i\in S\}|\\ \{\boldsymbol{f}_{s'_1},\ldots,\boldsymbol{f}_{s'_u}\} &:= \{\boldsymbol{f}_{i_1},\ldots,\boldsymbol{f}_{i_m}\}\cap\{\boldsymbol{f}_i|i\in S\}\\ \{\boldsymbol{f}_{i'_1},\ldots,\boldsymbol{f}_{i'_{m-u}}\} &:= \{\boldsymbol{f}_{i_1},\ldots,\boldsymbol{f}_{i_m}\}\setminus\{\boldsymbol{f}_{s'_1},\ldots,\boldsymbol{f}_{s'_u}\}\end{aligned}$$

［**定理** 2.10］ 式 (19) の行列 $\left[\boldsymbol{f}_{i_1}\cdots\boldsymbol{f}_{i_m}\boldsymbol{g}_{j,1}\cdots\boldsymbol{g}_{j,k_j}\right]$ の階数は，以下のようになる．

$$\begin{aligned}d&=\mathrm{rank}\left[\boldsymbol{f}_{i_1}\cdots\boldsymbol{f}_{i_m}\boldsymbol{g}_{j,1}\cdots\boldsymbol{g}_{j,k_j}\right]\\ &=\begin{cases}m+k_j-(u+v_j-g) & (u\geqq g-v_j)\\ m+k_j & (u\leqq g-v_j)\end{cases}\end{aligned} \tag{20}$$

(証明) 定理 3.7 の証明を参照． ∎

## 3. ロバストでセキュアなネットワーク符号化

Feldman ら [2] や Bhattad ら [3] が既存のネットワーク符号化にセキュア変換行列を適用することでセキュアなネットワーク符号化を与えたように，本節では，ロバストでセキュアな線型変換を用いたロバストでセキュアなネットワーク符号化を考えよう．

### 3.1 線型ネットワーク符号化

本節では，マルチキャスト通信に対応する，1 個のソースノードと複数個のシンクノードが存在するネットワークを扱う．ネットワークは，ノード集合 $V$ とリンク集合 $E$ からなるサイクルの無い有向グラフ $(V, E)$ で表わされる．各リンクは，有限体 $\mathbf{F}_q$ の要素を伝送シンボルとし，1 つのシンボルのみを伝送することが可能であるとする．すなわち，リンク容量を 1 とする．このとき，マルチキャスト通信で伝送可能な最大シンボル個数を示すネットワーク符号化容量 [8] を $h$ とする．Li ら [9] は，線型ネットワーク符号化を行なうことで，ソースノードから各シンクノードへ，同時に，情報シンボル $X_1, \ldots, X_h \in \mathbf{F}_q$ を伝送することが可能であることを示した．情報シンボルを長さ $h$ の行ベクトル $X^h = (X_1, \ldots, X_h) \in \mathbf{F}_q^h$ と記述する．

以下では，ネットワーク符号化として線型な場合について考える．各リンク $e \in E$ には，$\mathbf{F}_q$ 上の長さ $h$ の列ベクトル $\boldsymbol{g}(e) \in \mathbf{F}_q^h$ が付随している．このベクトル $\boldsymbol{g}(e)$ をリンク $e$ に付随するリンクベクトルとよぶ．このとき，ネットワーク符号化容量 $h$ の情報伝送を達成する線型ネットワーク符号化を実現するには，リンクベクトルが以下の条件 L1, 2 を満たすことが必要十分である．

［**条件** 3.1］ **L1**) ソースノード以外の各ノードに対し，その出力リンクのリンクベクトルは，その入力リンクのリンクベクトルの $\mathbf{F}_q$ 上の線型結合により得られるベクトルとする．

**L2**) 各シンクノードに対し，その入力リンクに付随するリンクベクトルの中に少なくとも $h$ 個の線型独立なベクトルが存在する． ∎

リンクベクトルの条件 L1 より，各リンク $e \in E$ には，情報ベクトル $X^h$ とリンクベクトル $\boldsymbol{g}(e)$ の積で表現されるシンボル $V(e) = X^h \boldsymbol{g}(e)$ が伝送される．また，リンクベクトルの条件 L1,2 より，シンクノードでは，$h$ 個の入力リンク $e_1, \ldots, e_h$ に付随する線型独立なリンクベクトル $\boldsymbol{g}(e_1), \ldots, \boldsymbol{g}(e_h)$ と伝送シンボル $V(e_1), \ldots, V(e_h)$ を得ることで，$(V(e_1), \ldots, V(e_h))[\boldsymbol{g}(e_1) \cdots \boldsymbol{g}(e_h)]^{-1} = X^h$ として，すべての情報 $X^h$ を一意に決定し，復号可能となる．すなわち，このような復号を可能にする符号化が，線型ネットワーク符号化である．

### 3.2 問題設定

ネットワークに対し，そのリンク集合 $E$ の部分集合を幾つか取り出す．そして，その部分集合に対し，ロバスト性や安全性を考慮することにする．

はじめに，安全性も考慮することより，2.3 節と同様に，ソースノードで生成される情報を $X^h = (X_1, \ldots, X_{h-r}, Y_1, \ldots, Y_r)$ とする．

$N+1$ 個のリンク集合 $E$ の部分集合を $E_0, E_1, \ldots, E_N$ とする．このとき，ロバスト性をもたせるリンク集合を $E_0$ のみとし，それ以外のリンク集合 $E_1, \ldots, E_N$ に対しては，式 (27) を満たす意味での安全性をもたせる問題設定を考える．各 $E_j$, $j = 0, 1, \ldots, N$, に対し，その濃度を $k_j := |E_j| (< h)$ と記し，その要素であるリンクを $E_j = \{e_{j,1}, \ldots, e_{j,k_j}\}$ とする．さらに，$E_j$ の各リンク $e_{j,p}$, $p = 1, \ldots, k_j$, に付随するリンクベクトル $\boldsymbol{g}(e_{j,p})$ を簡略して $\boldsymbol{g}_{j,p}$ と記し，それら全体の集合を $G_j := \{\boldsymbol{g}_{j,1}, \ldots, \boldsymbol{g}_{j,k_j}\}$ とする．ここで，これ以降の説明と記述を簡単にするために，$\mathrm{rank}[\boldsymbol{g}_{j,1} \cdots \boldsymbol{g}_{j,k_j}] = k_j$ を仮定する．この仮定により，以降の説明において一般性を失うことはない．また，$E_0$ に対しては，$g = k_0$ とする．

各 $j = 1, \ldots, N$ に対し，線型空間 $\mathbf{F}_q^h$ の部分空間 $\langle G_0 \rangle$ と $\langle G_j \rangle$ の共通部分空間 $\langle G_0 \rangle \cap \langle G_j \rangle$ の次元を $\dim \langle G_0 \rangle \cap \langle G_j \rangle = v_j$ と表すことにし，その共通部分空間の基底を $\boldsymbol{v}_{j,1}, \ldots, \boldsymbol{v}_{j,v_j}$ とする．さらに，その共通部分空間 $\langle G_0 \rangle \cap \langle G_j \rangle$ の基底 $\boldsymbol{v}_{j,1}, \ldots, \boldsymbol{v}_{j,v_j}$ を拡大して，部分空間 $\langle G_0 \rangle$ の基底を $\boldsymbol{u}_{j,1}, \ldots, \boldsymbol{u}_{j,g-v_j}, \boldsymbol{v}_{j,1}, \ldots, \boldsymbol{v}_{j,v_j}$ とする．同様に，部分空間 $\langle G_j \rangle$ の基底を $\boldsymbol{v}_{j,1}, \ldots, \boldsymbol{v}_{j,v_j}, \boldsymbol{w}_{j,1}, \ldots, \boldsymbol{w}_{j,k_j-v_j}$ とする．

### 3.3 ロバストでセキュアな変換行列の構成

与えられたネットワーク符号化に対するロバストでセキュアな変換行列の条件を以下に示す．

［**条件** 3.2］ $h$ 個の $\mathbf{F}_q$ 上の長さ $h$ の列ベクトルを $\boldsymbol{f}_i \in \mathbf{F}_q^h$, $i = 1, \ldots, h$ とし，$h \times h$ 行列を $F := [\boldsymbol{f}_1 \cdots \boldsymbol{f}_h]$ とする．

**1**) $\mathrm{rank}\ F = h$.

**2**) 集合 $\{1, \ldots, h-r\}$ の中から任意の $f$ 個の $s_1, \ldots, s_f$ を選び，固定し，添字集合 $S := \{s_1, \ldots, s_f\}$ とする．このとき，$[\boldsymbol{g}_{0,1} \cdots \boldsymbol{g}_{0,g}]D = [\boldsymbol{f}_{s_1} \cdots \boldsymbol{f}_{s_f}]$ を満たす $\mathbf{F}_q$ 上の $g \times f$ 行列 $D$ が存在する．ただし，$f \leqq g$.

**3**) 各 $E_j$, $j = 1, \ldots, N$, に対し，以下を満たす．任意の $\ell$ 個の $\boldsymbol{c}_1, \ldots, \boldsymbol{c}_\ell \in \{\boldsymbol{f}_{s_1}, \ldots, \boldsymbol{f}_{s_f}\}$ に対し，$\mathrm{rank}\,[\boldsymbol{c}_1 \cdots \boldsymbol{c}_\ell \boldsymbol{v}_{j,1} \cdots \boldsymbol{v}_{j,v_j}] = \ell + v_j$ を満たす．ただし，$\ell \leqq g - v_j$ を満たす．

**4**) 各 $E_j$, $j = 0, 1, \ldots, N$, に対し，以下を満たす．任意の $\ell$ 個の $\boldsymbol{c}_1, \ldots, \boldsymbol{c}_\ell \in \{\boldsymbol{f}_i \mid i \in \{1, \ldots, h-r\} \setminus S\}$ に対し，$\mathrm{rank}\,[\boldsymbol{c}_1 \cdots \boldsymbol{c}_\ell \boldsymbol{u}_{j,1} \cdots \boldsymbol{u}_{j,g-v_j} \boldsymbol{v}_{j,1} \cdots \boldsymbol{v}_{j,v_j} \boldsymbol{w}_{j,1} \cdots \boldsymbol{w}_{j,k_j-v_j}] = \ell + g + k_j - v_j$ を満たす．ただし，$\ell \leqq h - (g + k_j - v_j)$ を満たす． ∎

［**Remark** 3.3］ 条件 3.2 の 3) において，共通部分空間の次元が $v_j = g$ となる場合は，$\ell \leqq g - v_j = 0$ となり，条件を満たす $\boldsymbol{c}_1, \ldots, \boldsymbol{c}_\ell$ を考えることはできないことに注意する．明らかに，$j = 0$ の場合も同様である． ∎

［**Remark** 3.4］ 条件 3.2 の 3) や 4) を満たすための有限体 $\mathbf{F}_q$ の大きさについて考える．

まず，条件 3.2 3) の場合について考える．次元 $g$ の部分空間 $\langle G_0 \rangle$ の中に条件 3) を満たす $f$ 個の $\boldsymbol{f}_{s_1}, \ldots, \boldsymbol{f}_{s_f}$ が存在する必要がある．まず，1 個の $E_j$ について考える．$f$ 個中 $p$ 個の $\boldsymbol{f}_{s_1}, \ldots, \boldsymbol{f}_{s_p}$ が求まり，$p+1$ 個目の $\boldsymbol{f}_{s_{p+1}}$ が部分空間 $\langle G_0 \rangle$ の中に存在するための十分条件は，

$$q^g > \sum_{d=0}^{g-1} \binom{v_j + p}{d} (q-1)^d \tag{21}$$

となる．したがって，$p = 0, 1, \ldots, f-1$ であることより，

$$q^g > \sum_{d=0}^{g-1} \binom{v_j + f - 1}{d} (q-1)^d \tag{22}$$

が成り立てばよい．そして，上記の関係がすべての $E_j$, $j = 1, \ldots, N$ に対して成り立つことが必要である．さらに，条件 3.2 1) を成立させるための条件として，新たに $j = N+1$ の場合を考えて，$v_{N+1} = 0$ とする．すなわち，$\mathrm{rank}[\boldsymbol{f}_{s_1} \cdots \boldsymbol{f}_{s_f}] = f$ が成り立つ必要があるので，$v_{N+1} = 0$ としている．したがって，条件 3.2 3) を満たす $f$ 個の $\boldsymbol{f}_{s_1}, \ldots, \boldsymbol{f}_{s_f}$ が存在するための十分条件は，次式が成立することである．

$$q^g > \sum_{j=1}^{N+1} \sum_{d=0}^{g-1} \binom{v_j + f - 1}{d} (q-1)^d \tag{23}$$

次に，条件 3.2 4) の場合について考える．次元 $h$ の線型空間 $\mathbf{F}_q^h$ の中に条件 4) を満たす $h - r - f$ 個の $\boldsymbol{f}_{i_1}, \ldots, \boldsymbol{f}_{i_{h-r-f}}$ が存在する必要がある．条件 3) の場合と同様に，まず，1 個の $E_j$ について考える．$h - r - f$ 個中 $p$ 個の $\boldsymbol{f}_{i_1}, \ldots, \boldsymbol{f}_{i_p}$ が求まり，$p+1$ 個目の $\boldsymbol{f}_{i_{p+1}}$ が線型空間 $\mathbf{F}_q^h$ の中に存在するための十分条件は，

$$q^h > \sum_{d=0}^{h-1} \binom{g + k_j - v_j + p}{d} (q-1)^d \tag{24}$$

となる．したがって，$p=0,1,\ldots,h-r-f-1$ であることより，

$$q^h > \sum_{d=0}^{h-1} \binom{g+k_j-v_j+h-r-f-1}{d}(q-1)^d \qquad (25)$$

が成り立てばよい．そして，上記の関係がすべての $E_j$, $j=0,\ldots,N$ に対して成り立つことが必要である．また，前記と同様に，条件 3.2 1) が成立することを考慮すると，rank$[\boldsymbol{f}_{i_1}\cdots\boldsymbol{f}_{i_{h-r-f}}\boldsymbol{f}_{s_1}\cdots\boldsymbol{f}_{s_f}]=h-r$ が成り立つ必要がある．しかし，この条件は，$E_0$ の場合を考えれば十分である．なぜなら，$\boldsymbol{f}_{s_1},\ldots,\boldsymbol{f}_{s_f}\in\langle G_0\rangle$ であるから．したがって，条件 3.2 4) を満たす $h-r-f$ 個の $\boldsymbol{f}_{i_1},\ldots,\boldsymbol{f}_{i_{h-r-f}}$ が存在するための十分条件は，次式が成立することである．

$$q^h > \sum_{j=0}^{N}\sum_{d=0}^{h-1} \binom{g+k_j-v_j+h-r-f-1}{d}(q-1)^d \qquad (26)$$

以上より，条件 3.2 を満たす行列 $F$ が存在するための十分条件は，式 (23) と (26) がともに成立することである． ∎

[**補題** 3.5] 条件 3.2 3) において，以下の i) と ii) は同値である．i) “rank $[\boldsymbol{c}_1\cdots\boldsymbol{c}_\ell\boldsymbol{v}_{j,1}\cdots\boldsymbol{v}_{j,v_j}]=\ell+v_j$”． ii) “rank $[\boldsymbol{c}_1\cdots\boldsymbol{c}_\ell\boldsymbol{g}_{j,1}\cdots\boldsymbol{g}_{j,k_j}]=\ell+k_j$”．

(証明) 最初に，i→ii) を示す．$H$ を $g\times(\ell+v_j)$ 行列として，関係式

$$[\boldsymbol{c}_1\cdots\boldsymbol{c}_\ell\boldsymbol{v}_{j,1}\cdots\boldsymbol{v}_{j,v_j}]=[\boldsymbol{u}_{j,1}\cdots\boldsymbol{u}_{j,g-v_j}\boldsymbol{v}_{j,1}\cdots\boldsymbol{v}_{j,v_j}]H$$

を考える．このとき，i) より，rank $[\boldsymbol{c}_1\cdots\boldsymbol{c}_\ell\boldsymbol{v}_{j,1}\cdots\boldsymbol{v}_{j,v_j}]=\ell+v_j$. また，$\boldsymbol{u}_{j,1},\ldots,\boldsymbol{u}_{j,g-v_j},\boldsymbol{v}_{j,1},\ldots,\boldsymbol{v}_{j,v_j}$ は，$\langle G_0\rangle$ の基底であるから，rank $[\boldsymbol{u}_{j,1}\cdots\boldsymbol{u}_{j,g-v_j}\boldsymbol{v}_{j,1}\cdots\boldsymbol{v}_{j,v_j}]=g$ である．ゆえに，rank $H=\ell+v_j$. 次に，関係式

$$\begin{aligned}&[\boldsymbol{c}_1\cdots\boldsymbol{c}_\ell\boldsymbol{v}_{j,1}\cdots\boldsymbol{v}_{j,v_j}\boldsymbol{w}_{j,1}\cdots\boldsymbol{w}_{j,k_j-v_j}]\\&=[\boldsymbol{u}_{j,1}\cdots\boldsymbol{u}_{j,g-v_j}\boldsymbol{v}_{j,1}\cdots\boldsymbol{v}_{j,v_j}\boldsymbol{w}_{j,1}\cdots\boldsymbol{w}_{j,k_j-v_j}]\\&\quad\times\left[\begin{array}{c|c}H&\mathbf{O}\\\hline\mathbf{O}&I_{k_j-v_j}\end{array}\right]\end{aligned}$$

を考える．ここで，$I_{k_j-v_j}$ は $(k_j-v_j)\times(k_j-v_j)$ 単位行列である．このとき，$\boldsymbol{u}_{j,1},\ldots,\boldsymbol{u}_{j,g-v_j},\boldsymbol{v}_{j,1},\ldots,\boldsymbol{v}_{j,v_j},\boldsymbol{w}_{j,1},\ldots,\boldsymbol{w}_{j,k_j-v_j}$ は $\langle G_0\rangle$ と $\langle G_j\rangle$ の和空間 $\langle G_0\rangle+\langle G_j\rangle$ の基底であるから，rank $[\boldsymbol{u}_{j,1}\cdots\boldsymbol{u}_{j,g-v_j}\boldsymbol{v}_{j,1}\cdots\boldsymbol{v}_{j,v_j}\boldsymbol{w}_{j,1}\cdots\boldsymbol{w}_{j,k_j-v_j}]=g+k_j-v_j$ である．また，rank $H=\ell+v_j$ より，rank $\left[\begin{array}{c|c}H&\mathbf{O}\\\hline\mathbf{O}&I_{k_j-v_j}\end{array}\right]=\ell+k_j$. ゆえに，rank $[\boldsymbol{c}_1\cdots\boldsymbol{c}_\ell\boldsymbol{v}_{j,1}\cdots\boldsymbol{v}_{j,v_j}\boldsymbol{w}_{j,1}\cdots\boldsymbol{w}_{j,k_j-v_j}]=\ell+k_j$. 最後に，関係式

$$\begin{aligned}&[\boldsymbol{c}_1\cdots\boldsymbol{c}_\ell\boldsymbol{g}_{j,1}\cdots\boldsymbol{g}_{j,k_j}]\\&=[\boldsymbol{c}_1\cdots\boldsymbol{c}_\ell\boldsymbol{v}_{j,1}\cdots\boldsymbol{v}_{j,v_j}\boldsymbol{w}_{j,1}\cdots\boldsymbol{w}_{j,k_j-v_j}]\left[\begin{array}{c|c}I_\ell&\mathbf{O}\\\hline\mathbf{O}&T\end{array}\right]\end{aligned}$$

を考える．ここで，$T$ は部分空間 $\langle G_j\rangle$ の基底変換を行なう $k_j\times k_j$ 正則行列になるので rank $T=k_j$ である．このとき，rank $[\boldsymbol{f}_{s_1}\cdots\boldsymbol{f}_{s_\ell}\boldsymbol{v}_{j,1}\cdots\boldsymbol{v}_{j,v_j}\boldsymbol{w}_{j,1}\cdots\boldsymbol{w}_{j,k_j-v_j}]=\ell+k_j$ かつ rank $\left[\begin{array}{c|c}I_\ell&\mathbf{O}\\\hline\mathbf{O}&T\end{array}\right]=\ell+k_j$. ゆえに，rank $[\boldsymbol{f}_{s_1}\cdots\boldsymbol{f}_{s_\ell}\boldsymbol{g}_{j,1}\cdots\boldsymbol{g}_{j,k_j}]=\ell+k_j$ となる．

次に，ii→i) を示す．ほぼ，上記証明を逆順に示せばよいが，念のため以下に示す．関係式

$$\begin{aligned}&[\boldsymbol{c}_1\cdots\boldsymbol{c}_\ell\boldsymbol{v}_{j,1}\cdots\boldsymbol{v}_{j,v_j}\boldsymbol{w}_{j,1}\cdots\boldsymbol{w}_{j,k_j-v_j}]\\&=[\boldsymbol{c}_1\cdots\boldsymbol{c}_\ell\boldsymbol{g}_{j,1}\cdots\boldsymbol{g}_{j,k_j}]\left[\begin{array}{c|c}I_\ell&\mathbf{O}\\\hline\mathbf{O}&T^{-1}\end{array}\right]\end{aligned}$$

を考える．このとき，ii) より，rank $[\boldsymbol{c}_1\cdots\boldsymbol{c}_\ell\boldsymbol{g}_{j,1}\cdots\boldsymbol{g}_{j,k_j}]=\ell+k_j$. また，rank $\left[\begin{array}{c|c}I_\ell&\mathbf{O}\\\hline\mathbf{O}&T^{-1}\end{array}\right]=\ell+k_j$. ゆえに，rank $[\boldsymbol{c}_1\cdots\boldsymbol{c}_\ell\boldsymbol{v}_{j,1}\cdots\boldsymbol{v}_{j,v_j}\boldsymbol{w}_{j,1}\cdots\boldsymbol{w}_{j,k_j-v_j}]=\ell+k_j$. 次に，関係式

$$\begin{aligned}&[\boldsymbol{c}_1\cdots\boldsymbol{c}_\ell\boldsymbol{v}_{j,1}\cdots\boldsymbol{v}_{j,v_j}\boldsymbol{w}_{j,1}\cdots\boldsymbol{w}_{j,k_j-v_j}]\\&=[\boldsymbol{u}_{j,1}\cdots\boldsymbol{u}_{j,g-v_j}\boldsymbol{v}_{j,1}\cdots\boldsymbol{v}_{j,v_j}\boldsymbol{w}_{j,1}\cdots\boldsymbol{w}_{j,k_j-v_j}]\\&\quad\times\left[\begin{array}{c|c}H&\mathbf{O}\\\hline\mathbf{O}&I_{k_j-v_j}\end{array}\right]\end{aligned}$$

を考える．このとき，rank $[\boldsymbol{f}_{s_1}\cdots\boldsymbol{f}_{s_\ell}\boldsymbol{v}_{j,1}\cdots\boldsymbol{v}_{j,v_j}\boldsymbol{w}_{j,1}\cdots\boldsymbol{w}_{j,k_j-v_j}]=\ell+k_j$ かつ rank $[\boldsymbol{u}_{j,1}\cdots\boldsymbol{u}_{j,g-v_j}\boldsymbol{v}_{j,1}\cdots\boldsymbol{v}_{j,v_j}\boldsymbol{w}_{j,1}\cdots\boldsymbol{w}_{j,k_j-v_j}]=g+k_j-v_j$. したがって，rank $\left[\begin{array}{c|c}H&\mathbf{O}\\\hline\mathbf{O}&I_{k_j-v_j}\end{array}\right]=\ell+k_j$. ゆえに，rank$H=\ell+v_j$ である．最後に，関係式

$$[\boldsymbol{c}_1\cdots\boldsymbol{c}_\ell\boldsymbol{v}_{j,1}\cdots\boldsymbol{v}_{j,v_j}]=[\boldsymbol{u}_{j,1}\cdots\boldsymbol{u}_{j,g-v_j}\boldsymbol{v}_{j,1}\cdots\boldsymbol{v}_{j,v_j}]H$$

を考える．このとき，rank $[\boldsymbol{u}_{j,1}\cdots\boldsymbol{u}_{j,g-v_j}\boldsymbol{v}_{j,1}\cdots\boldsymbol{v}_{j,v_j}]=g$ かつ rank $H=\ell+v_j$ より，rank $[\boldsymbol{c}_1\cdots\boldsymbol{c}_\ell\boldsymbol{v}_{j,1}\cdots\boldsymbol{v}_{j,v_j}]=\ell+v_j$ となる．以上より，定理は証明された． ∎

### 3.4 符 号 化

条件 3.2 を満たす行列 $F$ を用いて，ソースノードから出力する情報ベクトル $X^h$ を $X^hF^{-1}$ に変換する．その結果，各リンク $e$ 上を伝送されるシンボルは $V(e)=X^h\boldsymbol{g}(e)$ から $W(e)=X^hF^{-1}\boldsymbol{g}(e)$ に変更される．そして，各リンク $e_{j,p}\in E_j$, $p=1,\ldots,k_j$ に対し，そのリンク上を伝送されるシンボルを $W_{j,p}=X^hF^{-1}\boldsymbol{g}_{j,p}$ と簡略して記す．このとき，条件 3.2 の設定と定理 2.9 より，以下の定理が成り立つ．

[**定理** 3.6] 任意の $m$ 個の $i_1,\ldots,i_m\in\{1,\ldots,h-r\}$ に対し，情報シンボルを $X^m=(X_{i_1},\ldots,X_{i_m})$ とする．また，任意の $E_j\in\{E_0,E_1,\ldots,E_N\}$ に対し，符号シンボルを $W_j^{k_j}=(W_{j,1},\ldots,W_{j,k_j})$ とする．ただし，$m+k_j\leqq h$ とする．このとき，以下が成り立つ．

$$H(X^m|W_j^{k_j})=\frac{d-k_j}{m}H(X^m) \qquad (27)$$

ただし，

$$d:=\mathrm{rank}\left[\boldsymbol{f}_{i_1}\cdots\boldsymbol{f}_{i_m}\boldsymbol{g}_{j,1}\cdots\boldsymbol{g}_{j,k_j}\right](\leqq h) \qquad (28)$$

∎

定理 3.6 において，添字集合 $\{i_1,\ldots,i_m\}$ に対応する集合 $\{\boldsymbol{f}_{i_1},\ldots,\boldsymbol{f}_{i_m}\}$ を次のように 2 個の集合に直和分割する．

$$\begin{aligned}u&:=|\{\boldsymbol{f}_{i_1},\ldots,\boldsymbol{f}_{i_m}\}\cap\{\boldsymbol{f}_i|i\in S\}|\\\{\boldsymbol{f}_{s'_1},\ldots,\boldsymbol{f}_{s'_u}\}&:=\{\boldsymbol{f}_{i_1},\ldots,\boldsymbol{f}_{i_m}\}\cap\{\boldsymbol{f}_i|i\in S\}\\\{\boldsymbol{f}_{i'_1},\ldots,\boldsymbol{f}_{i'_{m-u}}\}&:=\{\boldsymbol{f}_{i_1},\ldots,\boldsymbol{f}_{i_m}\}\setminus\{\boldsymbol{f}_{s'_1},\ldots,\boldsymbol{f}_{s'_u}\}\end{aligned}$$

[**定理** 3.7] 定理 3.6 の式 (28) の行列 $\left[\boldsymbol{f}_{i_1}\cdots\boldsymbol{f}_{i_m}\boldsymbol{g}_{j,1}\cdots\boldsymbol{g}_{j,k_j}\right]$ の階数は，以下のようになる．

$$\begin{aligned}d&=\mathrm{rank}\left[\boldsymbol{f}_{i_1}\cdots\boldsymbol{f}_{i_m}\boldsymbol{g}_{j,1}\cdots\boldsymbol{g}_{j,k_j}\right]\\&=\begin{cases}m+k_j-(u+v_j-g) & (u\geqq g-v_j)\\ m+k_j & (u\leqq g-v_j)\end{cases}\end{aligned} \qquad (29)$$

(証明) 任意の $\ell$ 個の $\boldsymbol{c}_1,\ldots,\boldsymbol{c}_\ell\in\{\boldsymbol{f}_{s'_1},\ldots,\boldsymbol{f}_{s'_u}\}$ に対し，条件 3.2 3) と補題 3.5 より，rank $[\boldsymbol{c}_1\cdots\boldsymbol{c}_\ell\boldsymbol{g}_{j,1}\cdots\boldsymbol{g}_{j,k_j}]=\ell+k_j$. ただし，$\ell\leqq g-v_j$. $H$ を $(g+k_j-v_j)\times(\ell+k_j)$ 行列として，関係式

$$\begin{aligned}&[\boldsymbol{c}_1\cdots\boldsymbol{c}_\ell\boldsymbol{g}_{j,1}\cdots\boldsymbol{g}_{j,k_j}]\\&=[\boldsymbol{u}_{j,1}\cdots\boldsymbol{u}_{j,g-v_j}\boldsymbol{v}_{j,1}\cdots\boldsymbol{v}_{j,v_j}\boldsymbol{w}_{j,1}\cdots\boldsymbol{w}_{j,k_j-v_j}]H\end{aligned}$$

を考えると，rank $H = \ell + k_j$ となる．

次に，関係式

$$[\boldsymbol{f}_{i'_1} \cdots \boldsymbol{f}_{i'_{m-u}} \boldsymbol{c}_1 \cdots \boldsymbol{c}_\ell \boldsymbol{g}_{j,1} \cdots \boldsymbol{g}_{j,k_j}]$$
$$= [\boldsymbol{f}_{i'_1} \cdots \boldsymbol{f}_{i'_{m-u}} \boldsymbol{u}_{j,1} \cdots \boldsymbol{u}_{j,g-v_j} \boldsymbol{v}_{j,1} \cdots \boldsymbol{v}_{j,v_j} \boldsymbol{w}_{j,1} \cdots \boldsymbol{w}_{j,k_j-v_j}]$$
$$\times \left[\begin{array}{c|c} I_{m-u} & \mathbf{O} \\ \hline \mathbf{O} & H \end{array}\right]$$

を考える．条件 3.2 4) より，

rank $[\boldsymbol{f}_{i'_1} \cdots \boldsymbol{f}_{i'_{m-u}} \boldsymbol{u}_{j,1} \cdots \boldsymbol{u}_{j,g-v_j} \boldsymbol{v}_{j,1} \cdots \boldsymbol{v}_{j,v_j} \boldsymbol{w}_{j,1} \cdots \boldsymbol{w}_{j,k_j-v_j}] = m-u+g-v_j+k_j$ である．また，rank $\left[\begin{array}{c|c} I_{m-u} & \mathbf{O} \\ \hline \mathbf{O} & H \end{array}\right] = m-u+\ell+k_j$．ゆえに，$d = $ rank $[\boldsymbol{f}_{i'_1} \cdots \boldsymbol{f}_{i'_{m-u}} \boldsymbol{c}_1 \cdots \boldsymbol{c}_\ell \boldsymbol{g}_{j,1} \cdots \boldsymbol{g}_{j,k_j}] = m-u+\ell+k_j$ となる．

最後に，$u \geqq g - v_j$ のとき，$\ell = g - v_j (\leqq u)$ として，$d = m+k_j-(u+v_j-g)$ となる．一方，$u \leqq g-v_j$ のとき，$\ell = u (\leqq g-v_j)$ として，$d = m+k_j$ となる．以上より，定理は示された． ∎

## 4. 線型変換の応用

ロバスト変換行列のような線型変換の応用として，以下の二つの定理 4.1, 4.2 を証明することができる．定理 4.1, 4.2 と類似の結果は，Koetter [7] らによってもすでに示されている ( [7] の定理 8,9,10 を参照)．また，Demchig [6] もこのような線型変換行列を用いて定理 4.2 に類似した情報伝送の可能性について示そうと試みている ( [6] の定理 4,5 を参照)．

ノード $s$ からノード $t$ への最大流を maxflow$(s,t)$ と記す．

### 4.1 複数ソースノードが存在する場合

サイクルの無い有向グラフで表されるネットワーク NW1 は，$S$ 個のソースノード $s_1,\ldots,s_S$ と $T$ 個のシンクノード $t_1,\ldots,t_T$ をもつとする．このとき，以下の条件を満たす統合ソースノードとよぶノード $s$ とその出力リンクを NW1 に追加し，NW1′ と記す．

条件）各 $i = 1,\ldots,S$ に対し，$s$ から $s_i$ へシンボルを伝送するリンク容量 $h_i$ のリンクを追加する．ただし，$h_i \leqq \min_{1\leqq j\leqq T}$ maxflow$(s_i,t_j)$ を満たす．

このとき，以下の定理が成り立つ．

[**定理** 4.1] NW1′ において，$\sum_{i=1}^{S} h_i = \min_{1\leqq j\leqq T}$ maxflow$(s,t_j)$ が成り立つと仮定する．このとき，NW1 において，各ソースノード $s_i$ で生成される $h_i$ 個の情報シンボル $X_{i,1},\ldots,X_{i,h_i}$ の和集合となる $\sum_{j=1}^{S} h_i$ 個の情報シンボル $\cup_{i=1}^{S}\{X_{i,1},\ldots,X_{i,h_i}\}$ を，すべてのシンクノードが，同時に，受信可能な線型ネットワーク符号化を構成可能である． ∎

### 4.2 異なる最大流をもつ複数シンクノードが存在する場合

サイクルの無い有向グラフで表されるネットワーク NW2 は，1 個のソースノード $s$ と $T$ 個のシンクノード $t_1,\ldots,t_T$ をもつとする．このとき，以下の条件を満たす統合シンクノードとよぶノード $t$ とその入力リンクを NW2 に追加し，NW2′ と記す．

条件）各 $j = 1,\ldots,T$ に対し，$t_j$ から $t$ へシンボルを伝送するリンク容量 $h_j$ のリンクを追加する．ただし，$h_j \leqq$ maxflow$(s,t_j)$ を満たす．

このとき，以下の定理が成り立つ．

[**定理** 4.2] NW2′ において，$\sum_{j=1}^{T} h_j =$ maxflow$(s,t)$ が成り立つと仮定する．このとき，NW2 において，各 $j = 1,\ldots,T$ に対し，シンクノード $t_j$ が，ソースノード $s$ で生成される $h_j$ 個の情報シンボル $X_{j,1},\ldots,X_{j,h_j}$ を受信可能な線型ネットワーク符号化を構成可能である．ただし，$i \neq j$ となる異なるシンクノード $t_i$ と $t_j$ に対し，それぞれが受信する情報シンボルは，$\{X_{i,1},\ldots,X_{i,h_i}\} \cap \{X_{j,1},\ldots,X_{j,h_j}\} = \emptyset$ を満たすものとする．すなわち，ソースノードにおいて生成される情報シンボルは，$\sum_{j=1}^{T} h_j$ 個の $\cup_{j=1}^{T}\{X_{j,1},\ldots,X_{j,h_j}\}$ である． ∎

定理 4.2 より，直ちに, [7] の定理 10 や [6] の定理 5 の主張と類似の結果が得られる．

## 5. むすび

本稿では，ロバストでセキュアなネットワーク符号化およびそのための線型変換についての概念を与えた．

### 文献


[1] N. Cai and R. W. Yeung, "Secure network coding", IEEE ISIT'02, p.323, June 2002. http://personal.ie.cuhk.edu.hk/~ITIP/ISIT02/secure.ps

[2] J. Feldman, T. Malkin, R. A. Servedio and C. Stein, "On the capacity of secure network coding", Proc. 42nd Annual Allerton Conference on Communication, Control, and Computing, Sept. 2004.

[3] K. Bhattad, K. R. Narayanan, "Weakly secure network coding", First Workshop on Network coding, Theory and Applications, NETCOD2005, Italy, Apr. 2005.

[4] 原田邦彦，山本博資, "強いランプ型しきい値特性を持つ安全なネットワーク符号化法", Proc. SITA2005, Okinawa, pp.741-744, Nov. 2005.

[5] 山本博資, "$(k,L,n)$ しきい値秘密分散システム", IEICE, vol.J68-A No.9, pp.945-952, 1985.

[6] Batchuluun Demchig, "マルチキャストネットワークのリンク切断を考慮したロバストネットワーク符号", 電気通信大学情報通信工学専攻修士論文, March 2006.

[7] R. Koetter, M. Medard, "An Algebraic Approach to Network Coding", IEEE/ACM Transactions on Networking, vol. 11, no. 5, pp.782-795, Oct. 2003.

[8] R. Ahlswede, N. Cai, S.-Y. R. Li and R. W. Yeung, "Network information flow," IEEE Trans. on Information Theory, vol. 46, no. 4, pp.1204-1216, July 2000.

[9] S.-Y. R. Li, R. W. Yeung, and N. Cai, "Linear network coding," IEEE Trans. on Information Theory, vol. 49, no. 2, pp.371-381, Feb. 2003.

[10] R. W. Yeung, "Two Approaches to Quantifying the Bandwidth Advantage of Network Coding," presented at 2004 IEEE Information Theory Workshop, San Antonio, Oct. 25-29, 2004. http://personal.ie.cuhk.edu.hk/~pwkwok4/Yeung/12.pdf

[11] 栗原正純，楯岡考道, "組合せネットワーク上のルーティング制御とその応用," 信学技法 vol.105 no.662, IT2005-131, pp.211-216, March 2006.


## 付録

### 1. 定理 2.9 の証明

まず，性質 P1, 2 を満たすことは明らか．次に，P4 を満たすことを以下に示す．ここで，本証明中の数式の展開については文献 [5] を参考にした．

仮定として，パラメータ $r,k,m$ は $0 \leqq r < h$, $1 \leqq k \leqq h$, $1 \leqq m \leqq h-r$ を満たす．

任意の $k$ 個の符号シンボル $W_{j_1},\ldots,W_{j_k}$ と任意の $m$ 個の情報シンボル $X_{i_1},\ldots,X_{i_m}$ との関係 $H(X^m|W^k)$ について調べる．ここで，簡単のために、$X^m = (X_{i_1},\ldots,X_{i_m})$, $W^k = (W_{j_1},\ldots,W_{j_k})$ と記す．さらに，$W^{k-1} = (W_{j_1},\ldots,W_{j_{k-1}})$ と記す．

#### 1.1 $H(X^m|W^k)$ の上界

一般に，$X^m$ と $W^k$ に対し，以下のことが成り立つ．

$$H(X^m|W^k)$$
$$= H(X^m W^k) - H(W^k)$$
$$\geqq H(X^m W^{k-1}) - H(W^k)$$

$$
\begin{aligned}
&= H(X^m W^{k-1}) - H(W^{k-1}) - H(W_{j_k}|W^{k-1}) \\
&= H(X^m|W^{k-1}) - H(W_{j_k}|W^{k-1}) \\
&\geqq H(X^m|W^{k-1}) - H(W_{j_k}) \\
&\geqq H(X^m|W^{k-1}) - \log q
\end{aligned}
$$

これより、下記の $h-k$ 個の不等式の各辺同士の和をとることを考える.

$$
\begin{aligned}
H(X^m|W^h) &\geqq H(X^m|W^{h-1}) - \log q \\
H(X^m|W^{h-1}) &\geqq H(X^m|W^{h-2}) - \log q \\
&\vdots \\
H(X^m|W^{h-(h-k+1)}) &\geqq H(X^m|W^{h-(h-k)}) - \log q
\end{aligned}
$$

すると、

$$
H(X^m|W^h) \geqq H(X^m|W^k) - (h-k)\log q \tag{A·1}
$$

となり，$H(X^m|W^h) = 0$ より、

$$
H(X^m|W^k) \leqq (h-k)\log q \tag{A·2}
$$

次に，$m+k$ 個の $\boldsymbol{f}_{i_1}, \ldots, \boldsymbol{f}_{i_m}, \boldsymbol{g}_{j_1}, \ldots, \boldsymbol{g}_{j_k}$ について考える．値 $d$ の定義 $d = \mathrm{rank}\left[\boldsymbol{f}_{i_1} \cdots \boldsymbol{f}_{i_m} \boldsymbol{g}_{j_1} \cdots \boldsymbol{g}_{j_k}\right]$ と $\mathrm{rank}\left[\boldsymbol{g}_{j_1} \cdots \boldsymbol{g}_{j_k}\right] = k$ より，$m$ 個の $\boldsymbol{f}_{i_1}, \ldots, \boldsymbol{f}_{i_m}$ の中の $m+k-d$ 個は，他の $d$ 個の要素の線型従属関係により表現可能である．そこで，そのような線型従属関係で表現できるものを $\boldsymbol{f}_{i_1}, \ldots, \boldsymbol{f}_{i_m}$ から除いた残りの $m' := d-k$ 個を $\boldsymbol{f}_{u_1}, \ldots, \boldsymbol{f}_{u_{m'}}$ と定義し，それらに関する情報シンボルを $X_{u_1}, \ldots, X_{u_{m'}}$ とする．さらに，簡単に，$X^{m'} = (X_{u_1}, \ldots, X_{u_{m'}})$ と記す．式 (A·2) の関係は，$H(X^{m'}|W^k)$ でも成り立つ．すなわち，

$$
H(X^{m'}|W^k) \leqq (h-k)\log q \tag{A·3}
$$

一方，$X^{m'}$ の定義より，以下の関係が成り立つ.

$$
\begin{aligned}
H(X^m|W^k) &= H(X^m W^k) - H(W^k) \\
&= H(X^{m'} W^k) - H(W^k) \\
&= H(X^{m'}|W^k)
\end{aligned}
$$

したがって,

$$
\begin{aligned}
H(X^m|W^k) &= H(X^{m'}|W^k) \\
&\leqq H(X^{m'}) \leqq (h-k)\log q
\end{aligned} \tag{A·4}
$$

以上の議論より，$d \leqq h$ であるから次の不等式が成り立つ.

$$
H(X^m|W^k) \leqq (d-k)\log q \tag{A·5}
$$

### 1.2 $H(X^m|W^k)$ の下界

符号シンボル $W_j = X^h F^{-1} \boldsymbol{g}_j$ の定義より，$\mathbf{F}_q$ 上の長さ $h$ の行ベクトルを $U^h = X^h F^{-1}$ とすると,

$$
X^h = U^h F \tag{A·6}
$$

$$
W_j = U^h \boldsymbol{g}_i \tag{A·7}
$$

と書き表すことができる.

$$
\begin{aligned}
&H(X^m|W^k) = H(X^{m'}|W^k) \\
&= I(X^{m'}; U^h|W^k) + H(X^{m'}|U^h W^k) \\
&= I(U^h; X^{m'}|W^k) \\
&= H(U^h|W^k) - H(U^h|X^{m'} W^k) \\
&= H(W^k|U^h) + H(U^h) - H(W^k) \\
&\quad - H(U^h|X^{m'} W^k) \\
&= H(U^h) - H(W^k) - H(U^h|X^{m'} W^k) \\
&= h\log q - H(W^k) - H(U^h|X^{m'} W^k) \qquad \text{(A·8)} \\
&\geqq (h-k)\log q - H(U^h|X^{m'} W^k) \qquad \text{(A·9)}
\end{aligned}
$$

等式 (A·8) は，以下の関係による:

$$
\begin{aligned}
H(U^h) = H(U^h X^{m'}) &= H(X^{m'}) + H(U^h|X^{m'}) \\
&= H(X^{m'}) + (h-m')\log q \\
&= h\log q
\end{aligned}
$$

さらに，$X^{m'} W^k$ に関しては，$\mathrm{rank}\left[\boldsymbol{f}_{u_1} \cdots \boldsymbol{f}_{u_{m'}} \boldsymbol{g}_{j_1} \cdots \boldsymbol{g}_{j_k}\right] = k + m' = d \leqq h$ であることより，

$$
H(U^h|X^{m'} W^k) = (h-d)\log q \tag{A·10}
$$

ゆえに，不等式 (A·9) と式 (A·10) より，

$$
H(X^m|W^k) \geqq (d-k)\log q \tag{A·11}
$$

### 1.3 $H(X^m|W^k)$ の評価

式 (A·5), (A·11) より，下記の関係が得られる.

$$
H(X^m|W^k) = (d-k)\log q \tag{A·12}
$$

(定理 2.9 の証明終)∎