ネットワーク符号化とある種の線型変換

— ロバストでセキュアなネットワーク符号化 —

栗原正純 (電気通信大学)

1. 概要 (線型変換，ロバスト，セキュア,「ロバストでセキュアな」)
2. 線型変換 (行列)
   - 2-1. ロバスト変換行列
   - 2-2. セキュア変換行列
   - 2-3. ロバストでセキュアな変換行列 $\Leftarrow *$
3. ロバストでセキュアなネットワーク符号化 $\Leftarrow **$
4. 結論

2006/07/28(東大柏キャンパス)

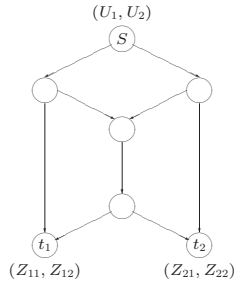
(2006/7/27/21:03 作成日)

概要 (関連研究)

- ロバストでセキュアなネットワーク符号化 ($\Leftarrow$ 線型変換)
- セキュアなネットワーク符号化
  - N. Cai and R. W. Yeung, "Secure network coding", 2002
  - J. Feldman, *et. al.*,"On the capacity of secure network coding", 2004 ($\Leftarrow$ 線型変換)
  - K. Bhattad, K. R. Narayanan, "Weakly secure network coding", 2005 ($\Leftarrow$ 線型変換)
  - 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", 2005

  ⋆山本博資, "(k, L, n) しきい値秘密分散システム", 1985
- ロバストなネットワーク符号化
  - 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", 2006 ($\Leftarrow$ 線型変換)

概要 (ネットワーク符号化)



- (U_1, U_2) : 送信シンボル；ソースノード S
- $(Z_{j,1}, Z_{j,2})$: 受信シンボル； シンクノード t_j, $j = 1, 2$
- 符号化：

$$\begin{aligned} t_1 &: (U_1, U_2)M_1 = (Z_{11}, Z_{12}) \\ t_2 &: (U_1, U_2)M_2 = (Z_{21}, Z_{22}) \end{aligned}$$

M_1, M_2 : 正則行列 $\Leftarrow$ 伝送行列

- 復号化：

$$\begin{aligned} t_1 &: (Z_{11}, Z_{12})M_1^{-1} = (U_1, U_2) \\ t_2 &: (Z_{21}, Z_{22})M_2^{-1} = (U_1, U_2) \end{aligned}$$

- U_1, U_2 : 送信シンボル
- $X_1, X_2 \in \mathbf{F}_q$: 情報シンボル
- $(U_1, U_2) \Leftarrow (X_1, X_2)$: 代入

$$\begin{aligned} \underline{(U_1, U_2)} &= (X_1, X_2) \\ &= \underline{(X_1, X_2)\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}} \end{aligned}$$

- 符号化・復号化 (シンク t_1)

$$\begin{aligned} \underline{(X_1, X_2)\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} M_1} &= \underline{(U_1, U_2)M_1} \\ &= (Z_{11}, Z_{12}) \end{aligned}$$

$$\begin{aligned} &\underline{(Z_{11}, Z_{12})}M_1^{-1}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}^{-1} \\ &= \underline{(U_1, U_2)M_1}M_1^{-1}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}^{-1} \\ &= (X_1, X_2) \end{aligned}$$

行列 F で表現

- $F^{-1} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, $F = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}^{-1}$.

⇓

- F : 2×2 正則行列 i.e., $^{\exists}F^{-1}$
- $(U_1, U_2) \Leftarrow (X_1, X_2)$: 代入

$$(U_1, U_2) = (X_1, X_2)F^{-1}$$

- 符号化・復号化 (シンク t_1)

$$\begin{aligned} \underline{(X_1, X_2)F^{-1}M_1} &= \underline{(U_1, U_2)M_1} \\ &= (Z_{11}, Z_{12}) \end{aligned}$$

$$\begin{aligned} &\underline{(Z_{11}, Z_{12})}M_1^{-1}F \\ &= \underline{(X_1, X_2)F^{-1}M_1}M_1^{-1}F \\ &= (X_1, X_2) \end{aligned}$$

概要 (線型変換 F)

- ネットワーク符号化が与えられている

  $\Longrightarrow$ ソースから各シンク t_j への 伝送行列 M_j が与えられている

$$(Z_{j,1}, \ldots, Z_{j,h}) = (U_1, \ldots, U_h)M_j$$

- F : $h \times h$ 正則行列とする
- $(U_1, \ldots, U_h) \Leftarrow (X_1, \ldots, X_h) \in \mathbf{F}_q^h$: 送信シンボル に 情報シンボル を 代入

$$(U_1, \ldots, U_h) = (X_1, \ldots, X_h)F^{-1}$$

- 符号化 :

$$\begin{aligned} (X_1, \ldots, X_h)F^{-1}M_1 &= (U_1, \ldots, U_h)M_j \\ &= (Z_{j,1}, \ldots, Z_{j,h}) \end{aligned}$$

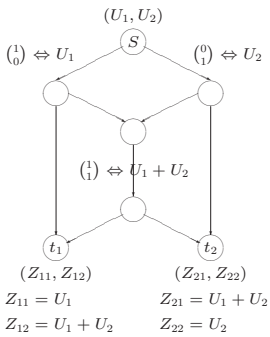
- 復号化 :

$$\begin{aligned} \underline{(Z_{j,1}, \ldots, Z_{j,h})}M_j^{-1}F &= \underline{(X_1, \ldots, X_h)F^{-1}M_1}M_j^{-1}F \\ &= (X_1, \ldots, X_h) \end{aligned}$$

ただし，シンク t_j は、M_j と F を既知とする

$\Longrightarrow$ この正則行列，すなわち，線型変換 (行列) F に着目する

概要 ((与えられた) ネットワーク符号化)



- リンクベクトルとその符号シンボル：

$$\begin{aligned} (U_1, U_2)\binom{1}{0} &= U_1 \\ (U_1, U_2)\binom{0}{1} &= U_2 \\ (U_1, U_2)\binom{1}{1} &= U_1 + U_2 \end{aligned}$$

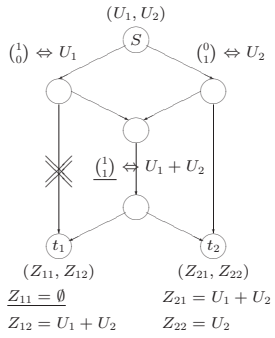
- シンク 1 : t_1

$$\begin{aligned} (Z_{11}, Z_{12}) &= (U_1, U_2)M_1 \\ M_1 &= \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \end{aligned}$$

- シンク 2 : t_2

$$\begin{aligned} (Z_{21}, Z_{22}) &= (U_1, U_2)M_2 \\ M_2 &= \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \end{aligned}$$

概要(ロバストな場合(リンク障害))



- U_1, U_2 : **送信シンボル**
- $X_1, X_2 \in \mathbf{F}_q$: **情報シンボル**
- **ロバスト変換行列** F over $\mathbf{F}_2$ **:**

$$F = [\, \underline{\boldsymbol{f}_1}\, \boldsymbol{f}_2 \,] = \begin{bmatrix} 1 & 1 \\ \underline{1} & 0 \end{bmatrix}$$

$$F^{-1} = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$$

- $(U_1, U_2) \Leftarrow (X_1, X_2)$: **代入**

$$\begin{aligned}(U_1, U_2) &= (X_1, X_2)F^{-1} \\ &= (X_2, X_1 + X_2)\end{aligned}$$

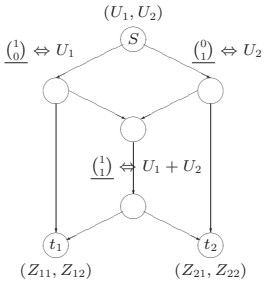
- **シンク** $1 : t_1$

$$Z_{12} = (X_1, X_2)F^{-1}\binom{1}{0} = X_1$$

- **シンク** $2 : t_2$

$$\begin{aligned}(Z_{21}, Z_{22}) &= (X_1, X_2)F^{-1}M_2 \\ &= (X_1, X_1 + X_2)\end{aligned}$$

概要(セキュアな場合 : しきい値 $= 1$)



- (U_1, U_2) : **送信シンボル**
- $(X_1, Y_1) \in \mathbf{F}_q^2$: **情報シンボルと乱数**
  X_1 : **情報シンボル(等確率に生起)**
  Y_1 : **一様乱数**
- **セキュア変換行列** F over $\mathbf{F}_3 = \{0, 1, 2\}$ **:**

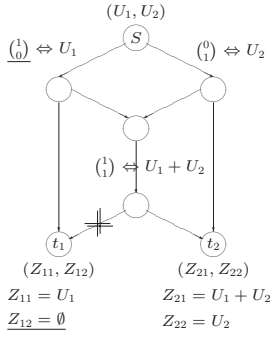
$$F = [\, \underline{\boldsymbol{f}_1}\, \boldsymbol{f}_2 \,] = \begin{bmatrix} 1 & 1 \\ \underline{2} & 0 \end{bmatrix}$$

$$F^{-1} = \begin{bmatrix} 0 & 2 \\ 1 & 1 \end{bmatrix}$$

- $(U_1, U_2) \Leftarrow (X_1, Y_1) \in \mathbf{F}_3^2$: **代入**
  $(U_1, U_2) = (X_1, Y_1)F^{-1} = (Y_1, 2X_1 + Y_1)$
- **各リンクの符号シンボル**

$$\begin{aligned}(U_1, U_2)\binom{1}{0} &= Y_1 \\ (U_1, U_2)\binom{0}{1} &= 2X_1 + Y_1 \\ (U_1, U_2)\binom{1}{1} &= 2X_1 + 2Y_1\end{aligned}$$

概要(ロバストでセキュアな場合 : しきい値 $= 1$)



- **ロバストでセキュアな変換行列** F over $\mathbf{F}_2 = \{0, 1\}$ **:**

$$F = [\, \underline{\boldsymbol{f}_1}\, \boldsymbol{f}_2 \,] = \begin{bmatrix} 1 & 1 \\ \underline{0} & 1 \end{bmatrix}$$

$$F^{-1} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

- $(U_1, U_2) \Leftarrow (X_1, Y_1) \in \mathbf{F}_2^2$: **代入**

$$(U_1, U_2) = (X_1, Y_1)F^{-1} = (X_1, X_1 + Y_1)$$

- **各リンクの符号シンボル**

$$\begin{aligned}(U_1, U_2)\binom{1}{0} &= X_1 \\ (U_1, U_2)\binom{0}{1} &= X_1 + Y_1 \\ (U_1, U_2)\binom{1}{1} &= Y_1\end{aligned}$$

概要(「ロバストでセキュアな」について)

- (E, V) **:** **マルチキャストネットワーク(** E **: リンク集合,** V **: ノード集合)**
- h **: ネットワーク符号化容量**
- $(X_1, \ldots, X_{h-r}, Y_1, \ldots, Y_r)$ **: 情報シンボルと乱数**

  しきい値 $= r$

  - $X_1, \ldots, X_{h-r}$ **:** $h - r$ **個の情報シンボル(等確率に生起)**
  - $Y_1, \ldots, Y_r$ **:** r **個の一様乱数**
- **セキュアな場合 :**

$$(X_1, \ldots, X_{h-r})$$

- **ロバストでセキュアな場合 :**
  - $X_{s_1}, \ldots, X_{s_f} \in \{X_1, \ldots, X_{h-r}\}$:
    ロバストで要求される f **個の情報シンボル** $\Longrightarrow$ **一意に復号可能**
  - $X_{i_1}, \ldots, X_{i_{h-r-f}} \in (\{X_1, \ldots, X_{h-r}\} \setminus \{X_{s_1}, \ldots, X_{s_f}\})$:
    残りの $h - r - f$ **個の情報シンボル**

$$(\underbrace{X_{s_1}, \ldots, X_{s_f}}_{\text{ロバスト}}, \underbrace{X_{i_1}, \ldots, X_{i_{h-r-f}}}_{\text{セキュア}})$$

線型変換 F (符号化・復号化 (与えられた符号化))

- $(X_1, \ldots, X_h) \in \mathbf{F}_q^h$: **長さ** h **の情報シンボル列**
- $\boldsymbol{g}_1, \ldots, \boldsymbol{g}_n \in \mathbf{F}_q^h$: n **個の符号化用列ベクトル**

  性質) $\forall \boldsymbol{g}_{j_1}, \ldots, \boldsymbol{g}_{j_h} \in \{\boldsymbol{g}_1, \ldots, \boldsymbol{g}_n\} \implies \mathrm{rank}[\boldsymbol{g}_{j_1} \cdots \boldsymbol{g}_{j_h}] = h$
- **符号化** : $(X_1, \ldots, X_h) \mapsto V_j$
  (符号シンボル)

$$V_j = (X_1, \ldots, X_h)\boldsymbol{g}_j \quad \text{for} \quad j = 1, \ldots, n$$

- **復号化** : $(V_{j_1}, \ldots, V_{j_h}) \mapsto (X_1, \ldots, X_h)$

$$\begin{aligned}&\forall V_{j_1}, \ldots, V_{j_h} \in \{V_1, \ldots, V_n\} \\ &\quad (X_1, \ldots, X_h) = (V_{j_1}, \ldots, V_{j_h})[\boldsymbol{g}_{j_1} \cdots \boldsymbol{g}_{j_h}]^{-1}\end{aligned}$$

ただし, $\{\boldsymbol{g}_1, \ldots, \boldsymbol{g}_n\}$ **を既知とする**

線型変換 (ロバスト変換 F) $1/2$

- **ロバストからの要求 :** $\{W_1, \ldots, W_n\}$ **符号シンボル**
  - $T = \{t_1, \ldots, t_g\} \subset \{1, \ldots, n\}$: **符号シンボル用添字集合** $(g < h)$
    $\Longrightarrow (W_{t_1}, \ldots, W_{t_g})$
  - $S = \{s_1, \ldots, s_f\} \subset \{1, \ldots, h\}$: **情報シンボル用添字集合** $(f \leq g)$
    $\Longrightarrow (X_{s_1}, \ldots, X_{s_f})$
- **性質 :**

P1) $(W_{t_1}, \ldots, W_{t_g}) \quad \mapsto \quad (X_{s_1}, \ldots, X_{s_f})$ **ロバスト**

P2) $\forall W_{j_1}, \ldots, W_{j_h} \in \{W_1, \ldots, W_n\}$ $(W_{j_1}, \ldots, W_{j_h}) \mapsto (X_1, \ldots, X_h)$ **任意の** h **個の符号シンボル**

- **条件 :** $h \times h$ **変換行列** $F = [\boldsymbol{f}_1 \cdots \boldsymbol{f}_h]$ **は次の条件を満たす**

C1) $\mathrm{rank}\ F = h$
C2) **次のような** $g \times f$ **行列** D **が存在する :**

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

線型変換 (ロバスト変換 F) 2/2

- **符号化** :

$$W_j = (X_1, \ldots, X_h)F^{-1}\boldsymbol{g}_j \quad \text{for} \quad j = 1, \ldots, n$$

- **復号化** : ($\{\boldsymbol{g}_1, \ldots, \boldsymbol{g}_n\}$, F, D **を既知とする**)

1) $(W_{t_1}, \ldots, W_{t_g})$ **の場合** (P1) : **ロバスト (特定の g 個)**

$$\begin{aligned}(W_{t_1}, \ldots, W_{t_g})D &= (X_1, \ldots, X_h)F^{-1}[\boldsymbol{g}_{t_1} \cdots \boldsymbol{g}_{t_g}]D \\ &= (X_1, \ldots, X_h)F^{-1}[\boldsymbol{f}_{s_1} \cdots \boldsymbol{f}_{s_f}] \\ &= (X_{s_1}, \ldots, X_{s_f})\end{aligned}$$

2) $^{\forall}W_{j_1}, \ldots, W_{j_h} \in \{W_1, \ldots, W_n\}$ **の場合** (P2) : **任意の h 個**

$$\begin{aligned}&\underline{(W_{j_1}, \ldots, W_{j_h})}[\boldsymbol{g}_{j_1} \cdots \boldsymbol{g}_{j_h}]^{-1}F \\ &= \underline{(X_1, \ldots, X_h)F^{-1}[\boldsymbol{g}_{j_1} \cdots \boldsymbol{g}_{j_h}]}[\boldsymbol{g}_{j_1} \cdots \boldsymbol{g}_{j_h}]^{-1}F \\ &= (X_1, \ldots, X_h)\end{aligned}$$

線型変換 (セキュア変換 F) 1/2

- $(X_1, \ldots, X_{h-r}, Y_1, \ldots, Y_r) \in \mathbf{F}_q^h$: **情報シンボルと乱数 (しきい値 $= r$)**
  - $X_1, \ldots, X_{h-r}$ **: 情報シンボル (等確率で生起)**
  - $Y_1, \ldots, Y_r$ **: 一様乱数**
- **性質** [山本, 1985] **:** (P3-3)

> $^{\forall}X_{i_1}, \ldots, X_{i_m} \in \{X_1, \ldots, X_{h-r}\}$ **: 情報シンボル**
> $^{\forall}W_{j_1}, \ldots, W_{j_k} \in \{W_1, \ldots, W_n\}$ **: 符号シンボル**
>
> $$\Longrightarrow \boxed{H(X_{i_1}, \ldots, X_{i_m} \mid W_{j_1}, \ldots, W_{j_k}) = H(X_{i_1}, \ldots, X_{i_m})}$$
>
> **ただし,** $m + k \le h$, $k < h$, $m \le h - r$

- **条件** [山本, 1985] **:** $h \times h$ **変換行列** $F = [\boldsymbol{f}_1 \cdots \boldsymbol{f}_h]$ **は次の条件を満たす**

> **C1)** $\mathrm{rank}\ F = h$
> **C5)** $^{\forall}\boldsymbol{g}_{j_1}, \ldots, \boldsymbol{g}_{j_k} \in \{\boldsymbol{g}_1, \ldots, \boldsymbol{g}_n\}$ **に対し, 以下が成立する :**
>
> $$^{\forall}\boldsymbol{f}_{i_1}, \ldots, \boldsymbol{f}_{i_m} \in \{\boldsymbol{f}_1, \ldots, \boldsymbol{f}_{h-r}\}$$
> $$\Longrightarrow \mathrm{rank}[\boldsymbol{f}_{i_1}, \ldots, \boldsymbol{f}_{i_m}\boldsymbol{g}_{j_1}, \ldots, \boldsymbol{g}_{j_k}] = m + k$$
>
> **ただし,** $m + k \le h$, $k < h$, $m \le h - r$

線型変換 (セキュア変換 F) 2/2

- **符号化** :

$$W_j = (X_1, \ldots, X_h)F^{-1}\boldsymbol{g}_j \quad \text{for} \quad j = 1, \ldots, n$$

- **復号化** : ($\{\boldsymbol{g}_1, \ldots, \boldsymbol{g}_n\}$, F **を既知とする**)

$$^{\forall}W_{j_1}, \ldots, W_{j_h} \in \{W_1, \ldots, W_n\} \quad \Longrightarrow$$

$$\begin{aligned}&(W_{j_1}, \ldots, W_{j_h})[\boldsymbol{g}_{j_1} \cdots \boldsymbol{g}_{j_h}]^{-1}F \\ &= (X_1, \ldots, X_h)F^{-1}[\boldsymbol{g}_{j_1} \cdots \boldsymbol{g}_{j_h}][\boldsymbol{g}_{j_1} \cdots \boldsymbol{g}_{j_h}]^{-1}F \\ &= (X_1, \ldots, X_h)\end{aligned}$$

線型変換 (ロバストでセキュアな変換 F : 準備 (線型部分空間)) 1/4

- $G_0 = \{\boldsymbol{g}_j | j \in T\} = \{\boldsymbol{g}_{0,1}, \ldots, \boldsymbol{g}_{0,g}\} \subset \{\boldsymbol{g}_1, \ldots, \boldsymbol{g}_n\}$, $|G_0| = g$ **:**
  ロバストに対応した列ベクトル : $\{W_j | j \in T\}$
- $^{\forall}G_j = \{\boldsymbol{g}_{j,1}, \ldots, \boldsymbol{g}_{j,k_j}\} \subset \{\boldsymbol{g}_1, \ldots, \boldsymbol{g}_n\}$, $|G_j| = k_j < h$
- **ベクトル** $\boldsymbol{g}_{j,p}$ **に対応する符号シンボルの表現 :** $W_{j,p} \Leftrightarrow \boldsymbol{g}_{j,p}$ for $p = 1, \ldots, k_j$
- $\langle G_j \rangle$ **:** G_j **から生成される部分空間**

$$\langle G_j \rangle = \langle \boldsymbol{g}_{j,1}, \ldots, \boldsymbol{g}_{j,k_j} \rangle := \{\alpha_1\boldsymbol{g}_{j,1} + \cdots + \alpha_{k_j}\boldsymbol{g}_{j,k_j} | \alpha_1, \ldots, \alpha_{k_j} \in \mathbf{F}_q\}$$

- $v_j = \dim\langle G_0 \rangle \cap \langle G_j \rangle$**:** $\langle G_0 \rangle$ **と** $\langle G_j \rangle$ **の共通部分空間の次元**
- $\boldsymbol{v}_{j,1}, \ldots, \boldsymbol{v}_{j,v_j}$ **:** $\langle G_0 \rangle \cap \langle G_j \rangle$ **の基底 (次元** v_j **)**
- $\boldsymbol{u}_{j,1}, \ldots, \boldsymbol{u}_{j,g-v_j}, \boldsymbol{v}_{j,1}, \ldots, \boldsymbol{v}_{j,v_j}$ **:** $\langle G_0 \rangle$ **の基底 (次元** g **)**
- $\boldsymbol{v}_{j,1}, \ldots, \boldsymbol{v}_{j,v_j}, \boldsymbol{w}_{j,1}, \ldots, \boldsymbol{w}_{j,k_j-v_j}$ **:** $\langle G_j \rangle$ **の基底 (次元** k_j **)**
- $\boldsymbol{u}_{j,1}, \ldots, \boldsymbol{u}_{j,g-v_j}, \boldsymbol{v}_{j,1}, \ldots, \boldsymbol{v}_{j,v_j}, \boldsymbol{w}_{j,1}, \ldots, \boldsymbol{w}_{j,k_j-v_j}$ **:** $\langle G_0 \rangle + \langle G_j \rangle$ **の基底 (次元** $g + k_j - v_j$ **)**

線型変換 (ロバストでセキュアな変換 F : 性質) 2/4

- **性質 :**

> **P1)** $(W_{0,1}, \ldots, W_{0,g}) \quad \mapsto \quad (X_{s_1}, \ldots, X_{s_f})$ **ロバスト (特定の g 個の符号シンボル)**
>
> **P2)** $^{\forall}W_{j_1}, \ldots, W_{j_h} \in \{W_1, \ldots, W_n\}$ **任意の h 個の符号シンボル**
> $(W_{j_1}, \ldots, W_{j_h}) \mapsto (X_1, \ldots, X_h)$
>
> **P4)** $^{\forall}X_{i_1}, \ldots, X_{i_m} \in \{X_1, \ldots, X_{h-r}\}$ **: 情報シンボル** **セキュア**
> $^{\forall}W_{j,1}, \ldots, W_{j,k_j} \in \{W_1, \ldots, W_n\}$ **: 符号シンボル**
>
> $$\Longrightarrow \quad H(X_{i_1}, \ldots, X_{i_m} \mid W_{j,1}, \ldots, W_{j,k_j})$$
> $$= \begin{cases} \dfrac{m - (u + v_j - g)}{m} H(X_{i_1}, \ldots, X_{i_m}) & (u + v_j \ge g) \\ H(X_{i_1}, \ldots, X_{i_m}) & (u + v_j \le g) \end{cases}$$
>
> **ただし,** $u = |\{X_{i_1}, \ldots, X_{i_m}\} \cap \{X_i | i \in S\}|$, $m + k_j \le h$, $k_j < h$, $m \le h - r$

- **分子 :** $\boxed{m - (u + v_j - g)} = m - u + (g - v_j) \ge \boxed{m - u}$ if $u + v_j \ge g$

線型変換 (ロバストでセキュアな変換 F : 条件) 3/4

- **条件 :** $h \times h$ **変換行列** $F = [\boldsymbol{f}_1 \cdots \boldsymbol{f}_h]$ **は次の条件を満たす**

> **C1)** $\mathrm{rank}\ F = h$
> **C2)** **次のような** $g \times f$ **行列** D **が存在する :** $\langle G_0 \rangle$
>
> $$\left[\boldsymbol{g}_{0,1} \cdots \boldsymbol{g}_{0,g}\right] D = \left[\boldsymbol{f}_{s_1} \cdots \boldsymbol{f}_{s_f}\right]$$
>
> **C6)** $^{\forall}G_j = \{\boldsymbol{g}_{j,1}, \ldots, \boldsymbol{g}_{j,k_j}\} \subset \{\boldsymbol{g}_1, \ldots, \boldsymbol{g}_n\}$, $|G_j| = k_j < h$, **に対し, 以下が成り立つ:** $\langle G_0 \rangle \cap \langle G_j \rangle$
>
> $$^{\forall}\boldsymbol{c}_1, \ldots, \boldsymbol{c}_\ell \in \{\boldsymbol{f}_i \mid i \in S\}$$
> $$\Longrightarrow \quad \mathrm{rank}\left[\boldsymbol{c}_1 \cdots \boldsymbol{c}_\ell \boldsymbol{v}_{j,1}, \ldots, \boldsymbol{v}_{j,v_j}\right] = \ell + v_j$$
>
> **ただし,** $\ell \le g - v_j$
>
> **C7)** $^{\forall}G_j = \{\boldsymbol{g}_{j,1}, \ldots, \boldsymbol{g}_{j,k_j}\} \subset \{\boldsymbol{g}_1, \ldots, \boldsymbol{g}_n\}$, $|G_j| = k_j < h$, **に対し, 以下が成り立つ:** $\langle G_0 \rangle + \langle G_j \rangle$
>
> $$^{\forall}\boldsymbol{c}_1, \ldots, \boldsymbol{c}_\ell \in \{\boldsymbol{f}_i \mid i \in \{1, \ldots, h-r\} \setminus S\}$$
> $$\Longrightarrow \quad \mathrm{rank}\left[\boldsymbol{c}_1 \cdots \boldsymbol{c}_\ell \boldsymbol{u}_{j,1}, \ldots, \boldsymbol{u}_{j,g-v_j} \boldsymbol{v}_{j,1}, \ldots, \boldsymbol{v}_{j,v_j} \right.$$
> $$\left. \boldsymbol{w}_{j,1}, \ldots, \boldsymbol{w}_{j,k_j-v_j}\right] = \ell + g + k_j - v_j$$
>
> **ただし,** $\ell \le h - (\ell + g + k_j - v_j)$

線型変換 (ロバストでセキュアな変換 F) 4/4

- 情報シンボル $(X_{i_1},\dots,X_{i_m})$ と符号シンボル $(W_{j,1},\dots,W_{j,k_j})$ の関係：

$$(X_{i_1},\dots,X_{i_m}|W_{j,1},\dots,W_{j,k_j})$$
$$\Updownarrow$$
$$(\boldsymbol{f}_{i_1},\dots,\boldsymbol{f}_{i_m}|\boldsymbol{g}_{j,1},\dots,\boldsymbol{g}_{j,k_j})$$
$$\Updownarrow$$
$$(\underbrace{\boldsymbol{f}_{i'_1},\dots,\boldsymbol{f}_{i'_{m-u}}}_{\langle G_0\rangle,\ \dim\langle G_0\rangle=g},\underbrace{\overbrace{\boldsymbol{f}_{s'_1},\dots,\boldsymbol{f}_{s'_u}}^{u}}_{\{\boldsymbol{f}_i|i\in S\}}|\underbrace{\overbrace{\boldsymbol{g}_{j,t_1},\dots,\boldsymbol{g}_{j,t_{v_j}}}^{v_j}}_{\langle G_0\rangle\cap\langle G_j\rangle},\underbrace{\boldsymbol{g}_{j,p_1},\dots,\boldsymbol{g}_{j,p_{k_j-v_j}}}_{\langle G_0\rangle+\langle G_j\rangle})$$
$$\Updownarrow$$
$$(\underbrace{X_{i'_1},\dots,X_{i'_{m-u}}}_{},\underbrace{X_{s'_1},\dots,X_{s'_u}}_{},|\underbrace{W_{j,t_1},\dots,W_{j,t_{v_j}}}_{},\underbrace{W_{j,p_1},\dots,W_{j,p_{k_j-v_j}}}_{})$$

「線型変換 (ロバストでセキュアな変換 F) 4/4」の言い換え

1. $X_{i_1},\dots,X_{i_m}\in\{X_1,\dots,X_{h-r}\}$：情報シンボル
   $W_{j,1},\dots,W_{j,k_j}\in\{W_1,\dots,W_n\}$：符号シンボル
   $$\Longrightarrow H(X_{i_1},\dots,X_{i_m}\mid W_{j,1},\dots,W_{j,k_j})=\ ?$$
2. $(X_{i_1},\dots,X_{i_m})$：
   $$X_{i_p}\begin{cases}\in\{X_i\,|\in S\}\Longrightarrow \underline{X_{i_p}}\\ \notin\{X_i\,|\in S\}\Longrightarrow X_{i_p}\end{cases}$$
3. $(W_{j,1},\dots,W_{j,k_j})\rightleftharpoons(\boldsymbol{g}_{j,1},\dots,\boldsymbol{g}_{j,k_j})\rightleftharpoons\langle G_j\rangle$：
   $$W_{j,p}\rightleftharpoons\boldsymbol{g}_{j,p}\begin{cases}\in\langle G_0\rangle\cap\langle G_j\rangle\Longrightarrow \underline{W_{j,p}}\\ \notin\langle G_0\rangle\cap\langle G_j\rangle\Longrightarrow W_{j,p}\end{cases}$$
4. $$H(X_{i'_1},\dots,X_{i'_{m-u}},\underbrace{\overbrace{X_{s'_1},\dots,X_{s'_u}}^{u}|\overbrace{W_{j,t'_1},\dots,W_{j,t'_{v_j}}}^{v_j}}_{u+v_j\le\ (\text{or }\ge)\ g},W_{j,p_1},\dots,W_{j,p_{k_j-v_j}})$$
$$=\begin{cases}\dfrac{m-(u+v_j-g)}{m}H(X_{i_1},\dots,X_{i_m}) & (u+v_j\ge g)\\ H(X_{i_1},\dots,X_{i_m}) & (u+v_j\le g)\end{cases}$$

ロバストでセキュアなネットワーク符号化 1/3

- (E,V)：マルチキャストネットワーク (E：リンク集合, V：ノード集合)
- h：ネットワーク符号化容量
- $(X_1,\dots,X_{h-r},Y_1,\dots,Y_r)$：情報シンボル (等確率に生起) と乱数 (一様乱数)
  - $X_1,\dots,X_{h-r}$：$h-r$ 個の情報シンボル
  - $Y_1,\dots,Y_r$　　：r 個の乱数
- $E_0,E_1,\dots,E_N\subset E$：$N+1$ 個のリンク部分集合
$$E_j=\{e_{j,1},\dots,e_{j,k_j}\},\ |E_j|=k_j<h\quad\text{for}\quad j=0,\dots,N$$
- 各リンク部分集合 E_j, $j=0,1,\dots,N$ に付随するリンクベクトル：
$$G_j=\{\boldsymbol{g}_{j,1},\dots,\boldsymbol{g}_{j,k_j}\}$$
- E_0：ロバストに対応するリンク部分集合；$|E_0|=k_0=g$

  $\Rightarrow$ ロバストに対応する情報シンボル：$\{X_i|i\in S\}$, $\text{s.t. } S\subset\{1,\dots,h-r\},\ |S|=f\le g$
- $E_1,\dots,E_N$：セキュアなリンク部分集合

ロバストでセキュアなネットワーク符号化 2/3

- 条件：$h\times h$ 変換行列 $F=[\boldsymbol{f}_1\cdots\boldsymbol{f}_h]$ は次の条件を満たす

1) $\text{rank } F=h$

2) ロバスト対応のリンク部分集合 E_0 に対し，次のような $g\times f$ 行列 D が存在する：　$\boxed{\langle G_0\rangle}$
$$\left[\boldsymbol{g}_{0,1}\cdots\boldsymbol{g}_{0,g}\right]D=\left[\boldsymbol{f}_{s_1}\cdots\boldsymbol{f}_{s_f}\right]$$

3) 各リンク部分集合 E_j, $j=1,\dots,N$ に対し，以下を満たす：　$\boxed{\langle G_0\rangle\cap\langle G_j\rangle}$
$$^\forall\boldsymbol{c}_1,\dots,\boldsymbol{c}_\ell\in\{\boldsymbol{f}_i\mid i\in S\}$$
$$\Longrightarrow\quad\text{rank}\left[\boldsymbol{c}_1\cdots\boldsymbol{c}_\ell\boldsymbol{v}_{j,1},\dots,\boldsymbol{v}_{j,v_j}\right]=\ell+v_j$$
ただし，$\ell\le g-v_j$

4) 各リンク部分集合 E_j, $j=1,\dots,N$ に対し，以下を満たす：　$\boxed{\langle G_0\rangle+\langle G_j\rangle}$
$$^\forall\boldsymbol{c}_1,\dots,\boldsymbol{c}_\ell\in\{\boldsymbol{f}_i\mid i\in\{1,\dots,h-r\}\setminus S\}$$
$$\Longrightarrow\quad\text{rank}\left[\boldsymbol{c}_1\cdots\boldsymbol{c}_\ell\boldsymbol{u}_{j,1},\dots,\boldsymbol{u}_{j,g-v_j}\boldsymbol{v}_{j,1},\dots,\boldsymbol{v}_{j,v_j}\right.$$
$$\left.\boldsymbol{w}_{j,1},\dots,\boldsymbol{w}_{j,k_j-v_j}\right]=\ell+g+k_j-v_j$$
ただし，$\ell\le h-(\ell+g+k_j-v_j)$

ロバストでセキュアなネットワーク符号化 3/3

- 符号化：各リンク部分集合 E_j, $j=0,1,\dots,N$ に対し，
$$W_{j,p}=(X_1,\dots,X_{h-r},Y_1,\dots,Y_r)F^{-1}\boldsymbol{g}_{j,p}\quad\text{for}\quad p=1,\dots,k_j$$
ここで，$\boldsymbol{g}_{j,p}\in G_j$ はリンク $e_{j,p}\in E_j$ に付随するリンクベクトル

- 性質：

1) ロバスト対応のリンク部分集合 E_0 に対し，以下が成り立つ：
$$(W_{0,1},\dots,W_{0,g})\quad\mapsto\quad(X_{s_1},\dots,X_{s_f})$$

2) 各リンク部分集合 E_j, $j=0,1,\dots,N$ に対し，以下が成り立つ：
$$^\forall X_{i_1},\dots,X_{i_m}\in\{X_1,\dots,X_{h-r}\}$$
$$\Longrightarrow\quad H(X_{i_1},\dots,X_{i_m}\mid W_{j,1},\dots,W_{j,k_j})$$
$$=\begin{cases}\dfrac{m-(u+v_j-g)}{m}H(X_{i_1},\dots,X_{i_m}) & (u+v_j\ge g)\\ H(X_{i_1},\dots,X_{i_m}) & (u+v_j\le g)\end{cases}$$
ただし，$u=|\{X_{i_1},\dots,X_{i_m}\}\cap\{X_i|i\in S\}|$, $m+k_j\le h$, $k_j<h$, $m\le h-r$

結論

- 与えられた (ネットワーク) 符号化から構成する様々な線型変換 (ロバスト，セキュア，ロバストでセキュア) について説明した
- ロバストでセキュアなネットワーク符号化の構成法 (線型変換) とその性質について説明した

http://www.coding.ice.uec.ac.jp