●□□□□□□□□□□□□□□□

セキュアネットワーク符号化アルゴリズム

— 条件付き正則行列の構成アルゴリズム (I) —

栗原正純 (電気通信大学)

1. **概要 (関連研究、目的、計算量 $O(h^3M)$, $O(h^2L)$)**
2. **(強いランプ型) 秘密分散符号化法** ([山本, 1985])
3. **セキュアネットワーク符号化アルゴリズムの概要**
4. **結論**

2006/11/28∼12/01(SITA2006 Hakodate)

(2006/11/30/22:41 作成日)

概要 (関連研究と目的) (1/2)

- **セキュアな ネットワーク符号化 (理論的条件設定)**
  - N. Cai and R. W. Yeung, "Secure network coding", 2002
  - J. Feldman, *et. al.*,"On the capacity of secure network coding", 2004
  - K. Bhattad, K. R. Narayanan, "Weakly secure network coding", 2005
  - 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
  - 原田邦彦, 山本博資, "線形ネットワーク符号化に対する強いランプ型秘密分散法", 2006
- **(強い)(ランプ型) 秘密分散符号化法に基づく安全性 ($\Leftarrow$ セキュアなネットワーク符号化)**
  - 山本博資, "(k, L, n) しきい値秘密分散システム", 1985
- **本稿の目的**
  - **セキュアネットワーク符号化のアルゴリズムを具体的に提示する**

    与えられた ネットワーク符号化 $\Rightarrow$ (強いランプ型の) セキュアなネットワーク符号化
  - **計算量の評価**

セキュアネットワーク符号化アルゴリズム

- **与えられたネットワーク符号化を**

  (強いランプ型の) セキュアネットワーク符号化に変換する方法

- **具体的には、与えられた盗聴条件 $\mathcal{G}$ に対し、**

  (強いランプ型) 秘密分散符号化の条件を満たす変換行列 F を構成する方法

  条件付き正則行列：$h \times h$ 行列 $F = [\boldsymbol{f}_1, \boldsymbol{f}_2, \boldsymbol{f}_3, \ldots, \boldsymbol{f}_h]$

- **符号化を行なう有限体 $\mathbf{F}_q$ のサイズが、$|\mathbf{F}_q| = q > 2M$ を満たすとき、**

  時間計算量：$O(h^3 M)$　　$(\approx\ O(h^2 M)\ \times\ O(h))$

  領域計算量：$O(h^2 L)$

- S.Jaggi, *et. al.*, "Polynomial time algorithms for multicast network code construction," 2005

- **M, L は、盗聴条件 $\mathcal{G}$ に依存して定まる値。　($\Longrightarrow$ h, L, M の値の内容を説明する)**

- $\boxed{h}$: h 次元情報ベクトル

$$(S^{h-r}R^r) = (\underbrace{S_1, \ldots, S_{h-r}}_{\text{情報シンボル}}, \underbrace{R_1, \ldots, R_r}_{\text{乱数}}) \in \mathbf{F}_q^h$$

- 符号化 : 符号シンボル (符号語) W

  任意の (リンク) ベクトル $\boldsymbol{g} \in \mathbf{F}_q^h$ に対し、

$$W(\boldsymbol{g}) = (S^{h-r}R^r)F^{-1}\boldsymbol{g}$$

  ただし、F は $h \times h$ の (条件付き) 正則行列 : $F = [\boldsymbol{f}_1, \ldots, \boldsymbol{f}_h]$

- 復号化 :

  正則行列 $\boxed{F}$ と 線型独立な任意の h 個の $\boxed{\boldsymbol{g}_1, \ldots, \boldsymbol{g}_h}$ と

  それらで定まる h 個の $\boxed{W(\boldsymbol{g}_1), \ldots, W(\boldsymbol{g}_h)}$ という取得情報から、

  情報ベクトルは、以下のように求まる。

$$(S^{h-r}R^r) = (W(\boldsymbol{g}_1), \ldots, W(\boldsymbol{g}_h))[\boldsymbol{g}_1, \ldots, \boldsymbol{g}_h]^{-1}F$$

- **盗聴条件** $\mathcal{G}$
  - **盗聴パターン** G_ℓ

    盗聴される r_ℓ **本** $(< h)$ **のリンクに付随するリンクベクトル** $\boldsymbol{g}_{\ell,i}$ **の集合**

    $$G_\ell = \{\boldsymbol{g}_{\ell,1}, \ldots, \boldsymbol{g}_{\ell,r_\ell}\} \subset \mathbf{F}_q^h \quad \text{s.t.} \quad \text{rank}[\boldsymbol{g}_{\ell,1}, \ldots, \boldsymbol{g}_{\ell,r_\ell}] = r_\ell < h$$

    $$W_{\ell,i} = W(\boldsymbol{g}_{\ell,i}) = (S^{h-r}R^r)F^{-1}\boldsymbol{g}_{\ell,i}, \quad i = 1, \ldots, r_\ell$$

  - **全体で** N **通り の盗聴パターンを考える。**

    $$\mathcal{G} = \{G_1, \ldots, G_N\}$$

- **(強いランプ型) 秘密分散符号化の条件**

  盗聴条件 $\mathcal{G}$ **に対し、条件付き正則行列** $F = [\boldsymbol{f}_1, \ldots, \boldsymbol{f}_{h-r} | \ldots, \boldsymbol{f}_h]$ **は以下を満たす。**

  任意の盗聴パターン $G_\ell = \{\boldsymbol{g}_{\ell,1}, \ldots, \boldsymbol{g}_{\ell,r_\ell}\} \in \mathcal{G} = \{G_1, \ldots, G_N\}$ **と**

  任意の $\boldsymbol{f}_{i_1}, \ldots, \boldsymbol{f}_{i_{h-r_\ell}} \in \{\boldsymbol{f}_1, \ldots, \boldsymbol{f}_{h-r}\}$ **に対して、**

  $h \times h$ **行列** $Y_\ell^{(k)} := [\boldsymbol{f}_{i_1}, \ldots, \boldsymbol{f}_{i_{h-r_\ell}} \mid \boldsymbol{g}_{\ell,1}, \ldots, \boldsymbol{g}_{\ell,r_\ell}]$ **が正則になる。**

  ただし、 $r_\ell \geq r$**.**

- **安全性**

  任意の盗聴パターン $G_\ell \in \mathcal{G}$ **より得られる符号シンボル** $W_{\ell,1}, \ldots, W_{\ell,r_\ell}$ **と**

  任意の情報シンボル $\boldsymbol{S}_{i_1}, \ldots, \boldsymbol{S}_{i_{h-r_\ell}} \in \{\boldsymbol{S}_1, \ldots, \boldsymbol{S}_{h-r}\}$ **に対して、**

  $$H(\boldsymbol{S}_{i_1}, \ldots, \boldsymbol{S}_{i_{h-r_\ell}} | W_{\ell,1}, \ldots, W_{\ell,r_\ell}) = H(\boldsymbol{S}_{i_1}, \ldots, \boldsymbol{S}_{i_{h-r_\ell}})$$

  が成り立つ。ただし、 $r_\ell \geq r$**.**

- $\boxed{L}$: 盗聴条件 $\mathcal{G}$ に対し、条件付き正則行列 F を構成するために考慮する行列の総数

$$Y_\ell^{(k)} = \left[\boldsymbol{f}_{i_1}, \ldots, \boldsymbol{f}_{i_{h-r_\ell}} \mid \boldsymbol{g}_{\ell,1}, \ldots, \boldsymbol{g}_{\ell,r_\ell} \right]$$

  - 各 $\ell = 1, \ldots, N$ に対し、

    $\underbrace{\boldsymbol{f}_1, \ldots, \boldsymbol{f}_{h-r}}_{h-r}$ の中から $\underbrace{\boldsymbol{f}_{i_1}, \ldots, \boldsymbol{f}_{i_{h-r_\ell}}}_{h-r_\ell}$ を取り出す組合せ数を、

    $$d_\ell = \binom{h-r}{h-r_\ell}$$

    とする。ただし、$r_\ell \geq r$.

  - すべての $\ell = 1, \ldots, N$ と 行列 F 自身も含めた、

    F を構成するために考慮すべき行列の総数を、

    $$L = \sum_{\ell=1}^{N} d_\ell + 1$$

    とする。(盗聴条件 $\mathcal{G}$ に依存して定まる値)

- $\boxed{M}$: $\boldsymbol{f}_1, \boldsymbol{f}_2, \ldots, \boldsymbol{f}_{h-r}$ の中のある $\boldsymbol{f}_m$ のみに着目したとき、

  L 個の全部の行列の中で $\boldsymbol{f}_m$ を含む行列の総数 $(M \leq L)$

  $$\mathrm{Y}_\ell^{(k)} = \left[\boldsymbol{f}_{i_1}, \ldots, \boldsymbol{f}_m, \ldots, \boldsymbol{f}_{i_{h-r_\ell}} \mid \boldsymbol{g}_{\ell,1}, \ldots, \boldsymbol{g}_{\ell,r_\ell}\right]$$

  - 各 $\ell = 1, \ldots, N$ に対し、

    $\underbrace{\{\boldsymbol{f}_1, \ldots, \boldsymbol{f}_{h-r}\} \setminus \{\boldsymbol{f}_m\}}_{h-r-1}$ の中から $h - r_\ell - 1$ 個を取り出す組合せ数を、

    $$D_\ell = \tbinom{h-r-1}{h-r_\ell-1}$$

    とする。ただし、$r_\ell \geq r$.

  - すべての $\ell = 1, \ldots, N$ と 行列 F 自身も含めた、$\boldsymbol{f}_m$ を含む行列の総数を、

    $$M = \textstyle\sum_{\ell=1}^{N} D_\ell + 1$$

    とする。(盗聴条件 $\mathcal{G}$ に依存して定まる値)

- 一般に、$\boxed{N \leq M \leq L}$ が成り立つ。

セキュアネットワーク符号化アルゴリズム

- 与えられた盗聴条件 $\mathcal{G} = \{G_1, \ldots, G_N\}$ に対し、条件付き正則行列

$$F = \left[\boldsymbol{f}_1, \ldots, \boldsymbol{f}_m, \ldots, \boldsymbol{f}_{h-r} \mid \boldsymbol{f}_{h-r+1}, \ldots, \boldsymbol{f}_h\right]$$

は、以下の計算量で求まる。

符号化を行なう有限体 $\mathbf{F}_q$ のサイズが、$|\mathbf{F}_q| = q > 2M$ を満たすとき、

時間計算量：$O(h^3M)$　$(\approx O(h^2M) \times (h-r))$

領域計算量：$O(h^2L)$

ここで、$N \leq M \leq L$ が成り立つ。

- **準備**
- **初期設定**
- **前処理： アルゴリズム** I
- **本処理： アルゴリズム** IIb

「線型独立な列ベクトルを順次追加し、条件を満たす正則行列を構成する」という手法ではなく、「最初に、適当な正則行列を用意し、その正則性を維持しながら列ベクトルを更新し、条件を満たす正則行列を構成する」という手法をとる。

- **準備**：L 個の $h \times h$ 正則行列 $Y_\ell^{(k)}$ を準備する。(領域計算量 $O(h^2 L)$)

  ◦ $L-1$ 個の $\ell = 1, \ldots, N, \quad k = 1, \ldots, d_\ell$ に対し、

$$Y_\ell^{(k)} = \left[\boldsymbol{y}_{\ell,1}^{(k)}, \ldots, \boldsymbol{y}_{\ell,h}^{(k)} \right] \left(= \left[\boldsymbol{f}_{i_1^{(k)}}, \ldots, \boldsymbol{f}_{i_{h-r_\ell}^{(k)}} | \boldsymbol{g}_{\ell,1}, \ldots, \boldsymbol{g}_{\ell,r_\ell} \right] \right)$$

  ◦ 条件付き正則行列 F：$\ell = N+1, \quad k = 1 (= d_{N+1})$ に対し、

$$Y_{N+1}^{(1)} = \left[\boldsymbol{y}_{N+1,1}^{(1)}, \ldots, \boldsymbol{y}_{N+1,h}^{(1)} \right] \left(= [\boldsymbol{f}_1, \ldots, \boldsymbol{f}_{h-r} | \boldsymbol{f}_{h-r+1}, \ldots, \boldsymbol{f}_h] = F \right)$$

- **初期設定**：L 個の正則行列 $Y_\ell^{(k)}$ を以下のように初期設定する。

$\ell = 1, \ldots, N+1, \quad k = 1, \ldots, d_\ell$ に対し、

$$Y_\ell^{(k)} = \left[\boldsymbol{y}_{\ell,1}^{(k)}, \ldots, \boldsymbol{y}_{\ell,h-r_\ell}^{(k)} | \boldsymbol{y}_{\ell,-r_\ell+1}^{(k)}, \ldots, \boldsymbol{y}_{\ell,h}^{(k)} \right] := \begin{bmatrix} 1 & & \boldsymbol{O} \\ & \ddots & \\ \boldsymbol{O} & & 1 \end{bmatrix}$$

- **前処理**：**(アルゴリズムI (基底構成アルゴリズム))**

$L-1$ **個の正則行列** $Y_\ell^{(k)}$ **に** **盗聴パターン** $G_\ell = \{\boldsymbol{g}_{\ell,1}, \ldots, \boldsymbol{g}_{\ell,r_\ell}\} \in \mathcal{G}$ **を反映させる。**

すなわち、 $\ell = 1, \ldots, N, \quad k = 1, \ldots, d_\ell$ **に対し、**

$$Y_\ell^{(k)} = \left[\boldsymbol{y}_{\ell,1}^{(k)}, \ldots, \boldsymbol{y}_{\ell,h-r_\ell}^{(k)} | \boldsymbol{y}_{\ell,-r_\ell+1}^{(k)}, \cdots, \boldsymbol{y}_{\ell,h}^{(k)}\right]$$

$$\Downarrow$$

$$Y_\ell^{(k)} = \left[\boldsymbol{y}_{\ell,1}^{(k)}, \ldots, \boldsymbol{y}_{\ell,h-r_\ell}^{(k)} | \boldsymbol{g}_{\ell,1}, \cdots, \boldsymbol{g}_{\ell,r_\ell}\right]$$

- **本処理**：**(アルゴリズム** IIb **)**　$F = \left[\boldsymbol{f}_1, \boldsymbol{f}_2, \ldots, \boldsymbol{f}_m, \ldots, \boldsymbol{f}_{h-r} \mid \ldots, \boldsymbol{f}_h\right]$

  各 $m = 1, \ldots, h-r$ **に対し、**$\boldsymbol{f}_m$ **を構成する手続きを繰り返し行なう。**

  - $\boldsymbol{f}_m$ **に関与する** M **個の行列** $Y_\ell^{(k)}$ **：**

$$\mathrm{Y}_\ell^{(k)} = \left[\cdots, \boldsymbol{y}^{(k)}_{\ell, i^{(k)}_{\ell,m}}, \cdots \middle| \boldsymbol{g}_{\ell,1}, \ldots, \boldsymbol{g}_{\ell,r_\ell}\right], \quad \ell = 1, \ldots, N,\ k \in D_\ell(m)$$

$$\mathrm{Y}_{N+1}^{(1)} = \left[\cdots, \boldsymbol{y}^{(k)}_{\ell, i^{(1)}_{N+1,m}}, \cdots \middle| \boldsymbol{f}_{h-r+1}, \ldots, \boldsymbol{f}_h\right] (= F), \quad \ell = N+1$$

  - M **個の乱数** $\alpha_\ell^{(k)} \in \mathbf{F}_q$ **を用いて、**$\boldsymbol{f}_m$ **の候補を構成する。(時間計算量** $O(hM)$**)**

$$\boldsymbol{f}_m := \sum_{\ell=1}^{N+1} \sum_{k \in D_\ell(m)} \alpha_\ell^{(k)} \boldsymbol{y}^{(k)}_{\ell, i^{(k)}_{\ell,m}}$$

アルゴリズムの概要 $(5/5)$

○ それぞれの行列 $Y_\ell^{(k)}$ の成分 $\boldsymbol{y}^{(k)}_{\ell,i^{(k)}_{\ell,m}}$ を $\boldsymbol{f}_m$ に交換し、

正則かどうかをチェックする。(時間計算量 $O(hM)$)

$$\left[\cdots,\boldsymbol{y}^{(k)}_{\ell,i^{(k)}_{\ell,m}},\cdots|\boldsymbol{g}_{\ell,1},\ldots,\boldsymbol{g}_{\ell,r_\ell}\right]\Rightarrow\left[\cdots,\boldsymbol{f}_m,\cdots|\boldsymbol{g}_{\ell,1},\ldots,\boldsymbol{g}_{\ell,r_\ell}\right]$$

$$\left[\cdots,\boldsymbol{y}^{(k)}_{\ell,i^{(k)}_{\ell,m}},\cdots|\boldsymbol{f}_{h-r+1},\ldots,\boldsymbol{f}_h\right]\Rightarrow\left[\cdots,\boldsymbol{f}_m,\cdots|\boldsymbol{f}_{h-r+1},\ldots,\boldsymbol{f}_h\right]$$

○ そして、M 個すべての行列が正則ならば、「$\boldsymbol{f}_m$ の構成」に **成功** 。

$m := m+1$ とする。 $\Longrightarrow$ 時間計算量 $O(h^2M)\times 1$

○ 他方、M 個のすべての行列が正則でないならば、ならば「$\boldsymbol{f}_m$ の構成」に **失敗** 。

再度、$\boldsymbol{f}_m$ の候補を構成する。 $\Longrightarrow$ 時間計算量 $O(h^2M)\times$ (失敗回数)

● 符号化を行なう有限体 $\mathbf{F}_q$ のサイズが、$|\mathbf{F}_q| = q > \underline{2}M$ ならば、

「失敗する確率は、$\underline{1/2}$ より小さい」ことが言える。 $\Longrightarrow$ 時間計算量 $O(h^2M)\times\underline{2}$

結論

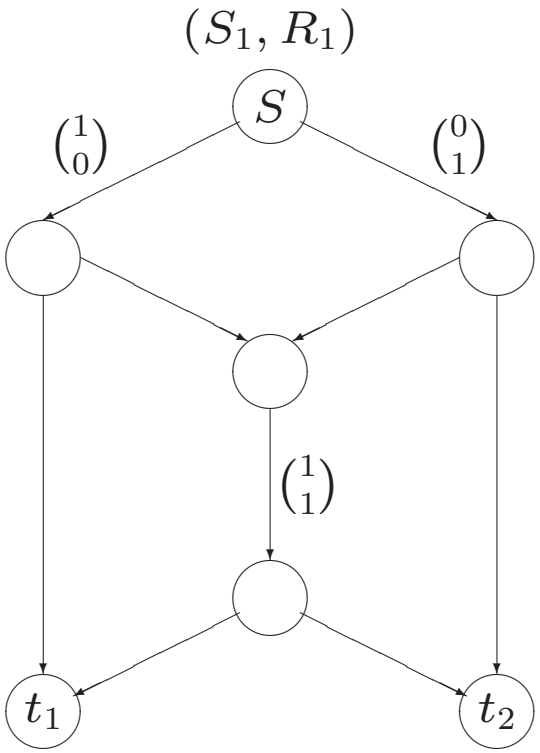
符号化を行なう有限体$\mathbf{F}_q$のサイズが、$|\mathbf{F}_q| > 2M$ を満たすとき、

時間計算量：$O(h^3 M)$　　$(\approx O(h^2 M) \times (h - r))$

領域計算量：$O(h^2 L)$

をもつ(強いランプ型の)セキュアネットワーク符号化アルゴリズムの概略を説明した。

例：セキュアネットワーク符号化 (しきい値 $= 1$) $(1/2)$



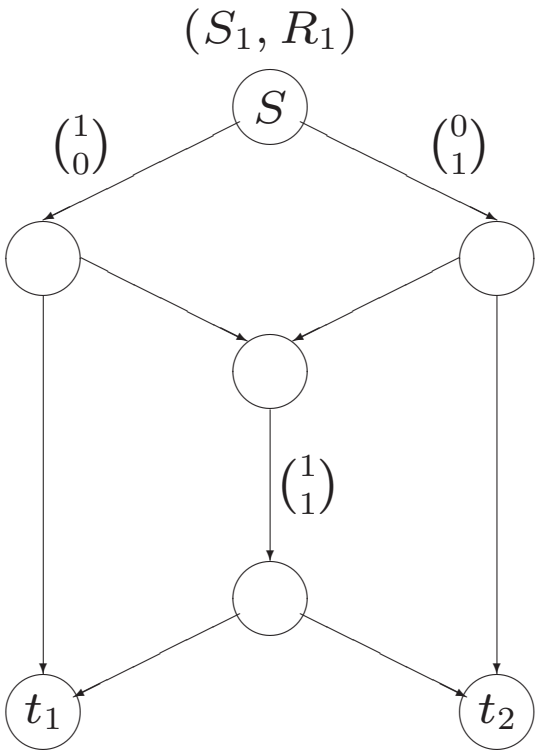
- $(S_1, R_1) \in \mathbf{F}_3^2$：情報ベクトル
  S_1：情報シンボル (等確率に生起)
  R_1：一様乱数
- $F = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ の場合

$$
\begin{aligned}
(S_1, R_1)F^{-1}\binom{1}{0} &= S_1 \\
(S_1, R_1)F^{-1}\binom{0}{1} &= R_1 \\
(S_1, R_1)F^{-1}\binom{1}{1} &= S_1 + R_1
\end{aligned}
$$

- $F = \begin{bmatrix} 1 & 1 \\ 2 & 0 \end{bmatrix}$ の場合 (セキュア変換行列)

$$
\begin{aligned}
(S_1, R_1)F^{-1}\binom{1}{0} &= R_1 \\
(S_1, R_1)F^{-1}\binom{0}{1} &= 2S_1 + R_1 \\
(S_1, R_1)F^{-1}\binom{1}{1} &= 2S_1 + 2R_1
\end{aligned}
$$

例：セキュアネットワーク符号化 (しきい値 $= 1$) $(2/2)$



- **盗聴パターン** G_ℓ, $\ell = 1, 2, 3$

$$G_1 = \left\{ \binom{1}{0} \right\}$$

$$G_2 = \left\{ \binom{0}{1} \right\}$$

$$G_3 = \left\{ \binom{1}{1} \right\}$$

- **盗聴条件** $\mathcal{G}$

$$\mathcal{G} = \{G_1, G_2, G_3\}$$

- **条件付き正則行列**

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

- **準備 1**：L 個の $h \times h$ 正則行列 $Y_\ell^{(k)}$ を準備する。(領域計算量 $O(h^2 L)$)

  ◦ $L-1$ 個の $\ell = 1, \ldots, N, \quad k = 1, \ldots, d_\ell$ に対し、

  $$Y_\ell^{(k)} = \left[\boldsymbol{y}_{\ell,1}^{(k)}, \ldots, \boldsymbol{y}_{\ell,h}^{(k)} \right] \left(= \left[\boldsymbol{f}_{i_1^{(k)}}, \ldots, \boldsymbol{f}_{i_{h-r_\ell}^{(k)}} | \boldsymbol{g}_{\ell,1}, \ldots, \boldsymbol{g}_{\ell,r_\ell} \right] \right)$$

  ◦ 条件付き正則行列 F：$\ell = N+1, \quad k = 1 (= d_{N+1})$ に対し、

  $$Y_{N+1}^{(1)} = \left[\boldsymbol{y}_{N+1,1}^{(1)}, \ldots, \boldsymbol{y}_{N+1,h}^{(1)} \right] \left(= \left[\boldsymbol{f}_1, \ldots, \boldsymbol{f}_{h-r} | \boldsymbol{f}_{h-r+1}, \ldots, \boldsymbol{f}_h \right] = F \right)$$

- **準備 2**：m と ℓ に関する添字集合 $D_\ell(m)$ を準備する。

  各 $m = 1, \ldots, h-r$ と 各 $\ell = 1, \ldots, N+1$ に対し、

  $$D_\ell(m) := \left\{ k \in \{1, \ldots, d_\ell\} | m \in \{i_1^{(k)}, \ldots, i_{h-r_\ell}^{(k)}\} (\subset \{1, \ldots, h-r\}) \right\}$$

  $$\left(Y_\ell^{(k)} = \left[\boldsymbol{f}_{i_1^{(k)}}, \ldots, \boldsymbol{f}_m, \ldots, \boldsymbol{f}_{i_{h-r_\ell}^{(k)}} | \boldsymbol{g}_{\ell,1}, \ldots, \boldsymbol{g}_{\ell,r_\ell} \right] \right)$$

  $M = \sum_{\ell=1}^{N+1} |D_\ell(m)| = \sum_{\ell=1}^{N+1} D_\ell$. **ただし、** $D_{N+1} = 1$.

前処理：アルゴリズム I (基底構成アルゴリズム)

Input : $G = \{\boldsymbol{g}_1, \boldsymbol{g}_2, \ldots, \boldsymbol{g}_n\}$
Output: Y, X, and I

Initial: $X = Y := E$, $I := \{1, 2, \ldots, h\}$, and $k := 1$.
Step 1) Input: $G = \{\boldsymbol{g}_1, \boldsymbol{g}_2, \ldots, \boldsymbol{g}_n\}$.
Step 2) if $^{\exists} j \in I$ such that $(\boldsymbol{g}_k, \boldsymbol{x}_j) \neq 0$, then goto 3), else goto 5).
Step 3) for some j such that $(\boldsymbol{g}_k, \boldsymbol{x}_j) \neq 0$,

$$
\begin{aligned}
\boldsymbol{y}_j &:= \boldsymbol{g}_k \\
\boldsymbol{x}_j &:= (\boldsymbol{y}_j, \boldsymbol{x}_j)^{-1} \boldsymbol{x}_j \\
\boldsymbol{x}_i &:= \boldsymbol{x}_i - (\boldsymbol{y}_j, \boldsymbol{x}_i)\boldsymbol{x}_j \text{ for all } i = 1, \ldots, h \text{ s.t.} i \neq j \\
I &:= I \setminus \{j\}
\end{aligned}
$$

Step 4) if $I = \emptyset$, then goto 6), else goto 5).
Step 5) $k := k + 1$. if $k > n$, then goto 6), else goto 2).
Step 6) Output: X, Y, and I and halt.

本処理：アルゴリズム IIb

Input : $X_\ell^{(k)}, Y_\ell^{(k)}, I_\ell^{(k)}$ for all $\ell = 1, \ldots, N$ and $k = 1, \ldots, d_\ell$
Output : $X_{N+1}^{(1)}, Y_{N+1}^{(1)}, I_{N+1}^{(1)}$

Initial: $h_2 := h - r$, $X_{N+1}^{(1)} = Y_{N+1}^{(1)} := E$, $I_{N+1}^{(1)} := \{1, \ldots, h\}$, and $m := 1$.
Step 1) Input: $X_\ell^{(k)}, Y_\ell^{(k)}, I_\ell^{(k)}$ for all $\ell = 1, \ldots, N$ and $k = 1, \ldots, d_\ell$
Step 2) for each $\ell = 1, \ldots, N+1$ and $k \in D_\ell(m)$,

$$i_\ell^{(k)} = i_{\ell,m}^{(k)} := \min I_\ell^{(k)} \tag{1}$$

Step 3) Choose $\alpha_\ell^{(k)} \in \mathbf{F}_q$ for all $\ell = 1, \ldots, N+1$ and $k \in D_\ell(m)$, and set

$$\boldsymbol{f} = \boldsymbol{f}_m := \sum_{\ell=1}^{N+1} \sum_{k \in D_\ell(m)} \alpha_\ell^{(k)} \boldsymbol{y}_{\ell, i_\ell^{(k)}}^{(k)} \tag{2}$$

Step 4) if $(\boldsymbol{f}, \boldsymbol{x}_{\ell, i_\ell^{(k)}}^{(k)}) \neq 0$ for all $\ell = 1, \ldots, N+1$ and $k \in D_\ell(m)$, then goto 5), else goto 3).

Step 5) for each $\ell = 1, \ldots, N+1$ and $k \in D_\ell(m)$,

$$
\begin{aligned}
\boldsymbol{y}^{(k)}_{\ell,i^{(k)}_\ell} &:= \boldsymbol{f} \\
\boldsymbol{x}^{(k)}_{\ell,i^{(k)}_\ell} &:= (\boldsymbol{y}^{(k)}_{\ell,i^{(k)}_\ell}, \boldsymbol{x}^{(k)}_{\ell,i^{(k)}_\ell})^{-1} \boldsymbol{x}^{(k)}_{\ell,i^{(k)}_\ell} \\
\boldsymbol{x}^{(k)}_{\ell,i} &:= \boldsymbol{x}^{(k)}_{\ell,i} - (\boldsymbol{y}^{(k)}_{\ell,i^{(k)}_\ell}, \boldsymbol{x}^{(k)}_{\ell,i}) \boldsymbol{x}^{(k)}_{\ell,i^{(k)}_\ell} \\
&\qquad \text{for all } i = 1, \ldots, h \text{ s.t.} i \neq i^{(k)}_\ell \\
I^{(k)}_\ell &:= I^{(k)}_\ell \setminus \{i^{(k)}_\ell\}
\end{aligned}
$$

Step 6) $m := m + 1$. if $m > h_2$, then goto 7), else goto 2).

Step 7) Output: $X^{(1)}_{N+1}$, $Y^{(1)}_{N+1}$, and $I^{(1)}_{N+1}$ and halt.

失敗する確率について $(1/5)$

- 新しい $\boldsymbol{f}_m$ に関与する M 個の正則行列：$\ell = 1, \ldots, N+1, \quad k \in D_\ell(m)$

$$Y_\ell^{(k)} = \left[\cdots \ \boldsymbol{y}^{(k)}_{\ell, i^{(k)}_{\ell,m}} \ \cdots \right]$$

- M 個の乱数 $\alpha_\ell^{(k)}$ を用いて、$\boldsymbol{f}_m$ の候補を構成する。

$$\boldsymbol{f}_m := \sum_{\ell=1}^{N+1} \sum_{k \in D_\ell(m)} \alpha_\ell^{(k)} \boldsymbol{y}^{(k)}_{\ell, i^{(k)}_{\ell,m}}$$

- M 個ある組 (ℓ, k) の中で、失敗した一つの組 $(\ell, k) = (p_1, p_2)$ に着目する。

$$\boldsymbol{y}^{(p_2)}_{p_1, i^{(p_2)}_{p_1,m}} \quad \Longrightarrow \quad \boldsymbol{f}_m$$

$$Y_{p_1}^{(p_2)} = \left[\cdots \ \boldsymbol{y}^{(p_2)}_{p_1, i^{(p_2)}_{p_1,m}} \ \cdots \right] \quad \Longrightarrow \quad [\cdots \ \boldsymbol{f}_m \ \cdots] : \begin{cases} \text{正則} & : \ \text{成功} \\ \text{正則でない} & : \ \boxed{\text{失敗}} \end{cases}$$

失敗する確率について $(2/5)$

○ **失敗** : (p_1, p_2) では、$[\cdots \ \boldsymbol{f}_m \ \cdots]$ が正則でない。

$\boldsymbol{f}_m$ は他の $h-1$ 個の成分ベクトル $\boldsymbol{y}_{p_1,i}^{(p_2)},\ i \neq i_{p_1,m}^{(p_2)}$ で表わされる。

$$\boldsymbol{f}_m = \sum_{\substack{i=1 \\ i \neq i_{p_1,m}^{(p_2)}}}^{h} \gamma_i \boldsymbol{y}_{p_1,i}^{(p_2)} \qquad (a)$$

ここで、 $\gamma_i \in \mathbf{F}_q$.

失敗する確率について $(3/5)$

- 一方、構成した $\boldsymbol{f}_m$ から (p_1, p_2) の項を抜き出す。

$$\begin{aligned}\boldsymbol{f}_m &= \sum_{\ell=1}^{N+1} \sum_{k \in D_\ell(m)} \alpha_\ell^{(k)} \boldsymbol{y}^{(k)}_{\ell, i^{(k)}_{\ell,m}} \\ &= \alpha_{p_1}^{(p_2)} \boldsymbol{y}^{(p_2)}_{p_1, i^{(p_2)}_{p_1,m}} + \underline{\sum_{\ell=1}^{N+1} \sum_{\substack{k \in D_\ell(m) \\ (\ell,k) \neq (p_1,p_2)}} \alpha_\ell^{(k)} \boldsymbol{y}^{(k)}_{\ell, i^{(k)}_{\ell,m}}} \qquad \in \mathbf{F}_q^h\end{aligned}$$

- $\underline{Y^{(p_2)}_{p_1}}$ は正則行列より、上式の右辺の第二項は以下のように書ける。

$$\underline{\sum_{\ell=1}^{N+1} \sum_{\substack{k \in D_\ell(m) \\ (\ell,k) \neq (p_1,p_2)}} \alpha_\ell^{(k)} \boldsymbol{y}^{(k)}_{\ell, i^{(k)}_{\ell,m}}} = \sum_{i=1}^{h} \beta_i \boldsymbol{y}^{(p_2)}_{p_1,i} \qquad \in \mathbf{F}_q^h$$

ここで、 $\beta_i \in \mathbf{F}_q$.

- そこで、$\sum_{i=1}^{h} \beta_i \boldsymbol{y}^{(p_2)}_{p_1,i}$ を上記の $\boldsymbol{f}_m$ の式に代入すると、

失敗する確率について $(4/5)$

$$
\begin{aligned}
\boldsymbol{f}_m &= \alpha_{p_1}^{(p_2)} \boldsymbol{y}^{(p_2)}_{p_1, i^{(p_2)}_{p_1,m}} + \sum_{i=1}^{h} \beta_i \boldsymbol{y}^{(p_2)}_{p_1,i} \\
&= (\alpha_{p_1}^{(p_2)} + \beta_{i^{(p_2)}_{p_1,m}}) \boldsymbol{y}^{(p_2)}_{p_1, i^{(p_2)}_{p_1,m}} + \sum_{\substack{i=1 \\ i \neq i^{(p_2)}_{p_1,m}}}^{h} \beta_i \boldsymbol{y}^{(p_2)}_{p_1,i} \qquad (b)
\end{aligned}
$$

- **ベクトル $\boldsymbol{f}_m$ を表す2つの式 (a) と (b) より、$(b) = (a)$ とすると、**

$$
(\alpha_{p_1}^{(p_2)} + \beta_{i^{(p_2)}_{p_1,m}}) \boldsymbol{y}^{(p_2)}_{p_1, i^{(p_2)}_{p_1,m}} + \sum_{\substack{i=1 \\ i \neq i^{(p_2)}_{p_1,m}}}^{h} \beta_i \boldsymbol{y}^{(p_2)}_{p_1,i} = \sum_{\substack{i=1 \\ i \neq i^{(p_2)}_{p_1,m}}}^{h} \gamma_i \boldsymbol{y}^{(p_2)}_{p_1,i}
$$

- **右辺を左辺に移項する：**

$$
(\alpha_{p_1}^{(p_2)} + \beta_{i^{(p_2)}_{p_1,m}}) \boldsymbol{y}^{(p_2)}_{p_1, i^{(p_2)}_{p_1,m}} + \sum_{\substack{i=1 \\ i \neq i^{(p_2)}_{p_1,m}}}^{h} (\beta_i - \gamma_i) \boldsymbol{y}^{(p_2)}_{p_1,i} = 0
$$

失敗する確率について $(5/5)$

- $Y_{p_1}^{(p_2)}$ は正則行列、すなわち、$\boldsymbol{y}_{p_1,1}^{(p_2)}, \ldots, \boldsymbol{y}_{p_1,h}^{(p_2)}$ は線型独立であるから、$(\alpha_{p_1}^{(p_2)} + \beta_{i_{p_1,m}^{(p_2)}}) = 0.$

$$\alpha_{p_1}^{(p_2)} = -\beta_{i_{p_1,m}^{(p_2)}} \in \mathbf{F}_q$$

- 組 (p_1, p_2) が失敗するのは、$\alpha_{p_1}^{(p_2)}$ の値として、$-\beta_{i_{p_1,m}^{(p_2)}} \in \mathbf{F}_q$ が選ばれた場合のみである。

  ゆえに、$(\ell, k) = (p_1, p_2)$ において失敗する確率は $\boxed{1/q}$ である。

- 決定した M 個の $\alpha_\ell^{(k)}\mathbf{F}_q,\ \ell = 1, \ldots, N+1, \quad k \in D_\ell(m)$ に対し、
  失敗する組 (ℓ, k) が 1 組でも存在する確率は、たかだか

$$\boxed{M \times \frac{1}{q} < M \times \frac{1}{2M} < \frac{1}{2}}$$

  ただし、$|\mathbf{F}_q| = q > 2M.$

参考 WEB

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