修復可能な分散ストレージシステムにおけるランプ型秘密分散法

(最小バンドワイド再生成符号を用いたランプ型秘密分散法)

栗原 正純　　桑門 秀典
（電気通信大学）　（神戸大学）

電子情報通信学会 情報理論研究会, 岡山大学, 2011/07/21-22

(2011/7/20/11:44)

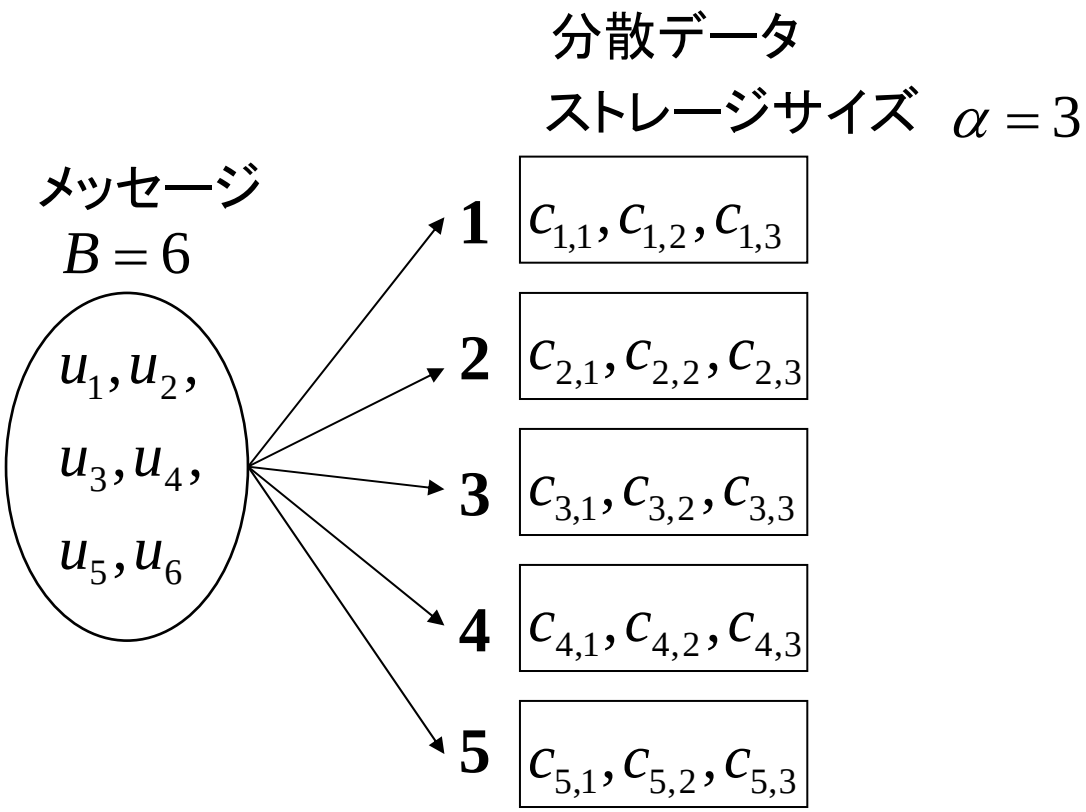
目次

はじめに（分散ストレージシステムの修復問題と再生成符号）

1. **分散ストレージシステムの修復問題**
   1. [2] Dimakis, Godfrey, Wu, Wainwright, Ramchandran, ”Network Coding for Distributed Storage Systems,”2010.
2. **「分散符号化」と「故障ノードの修復」**
3. **再生成符号** (Regenerating codes)
   1. **復元（復号）**:
      → メッセージの復元
   2. **修復（再生成）**:
      → 故障ノードの修復（システムの信頼性の維持）
      → つまり、
      故障ノードに保存されていたデータを再生成
4. **ストレージ と修復バンドワイドのトレードオフ**

（上記のことを図を用いて説明（6 頁））

分散ストレージシステム（安全性、信頼性の確保）



$$\alpha = k = d = 3,$$
$$\beta = 1,$$
$$B = 6$$

メッセージ

$u_1, u_2, u_3,$
u_4, u_5, u_6

分散符号化

ノード i

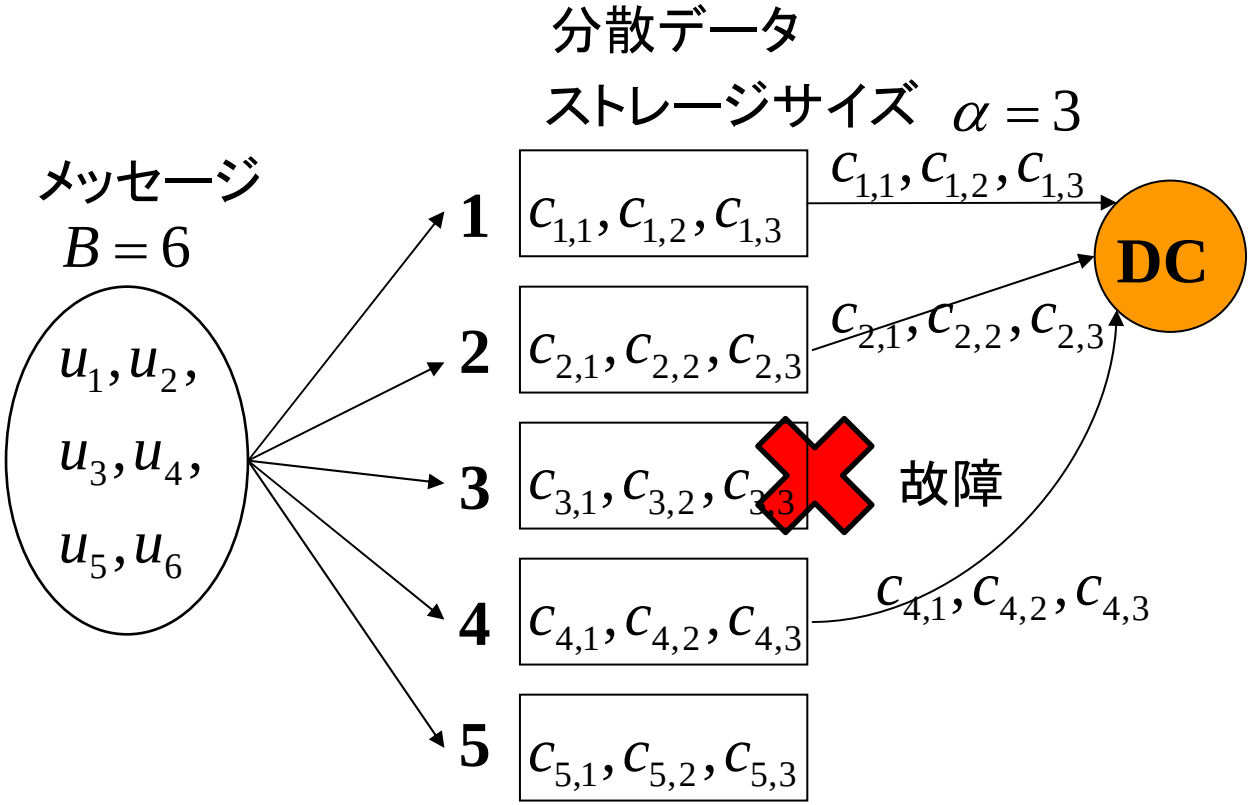
分散データ

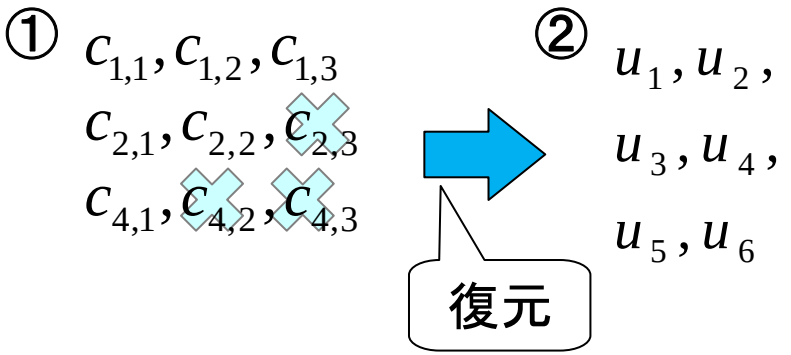
$c_{i,1}, c_{i,2}, c_{i,3}$

$$u_k, c_{j,k} \in GF(q)$$

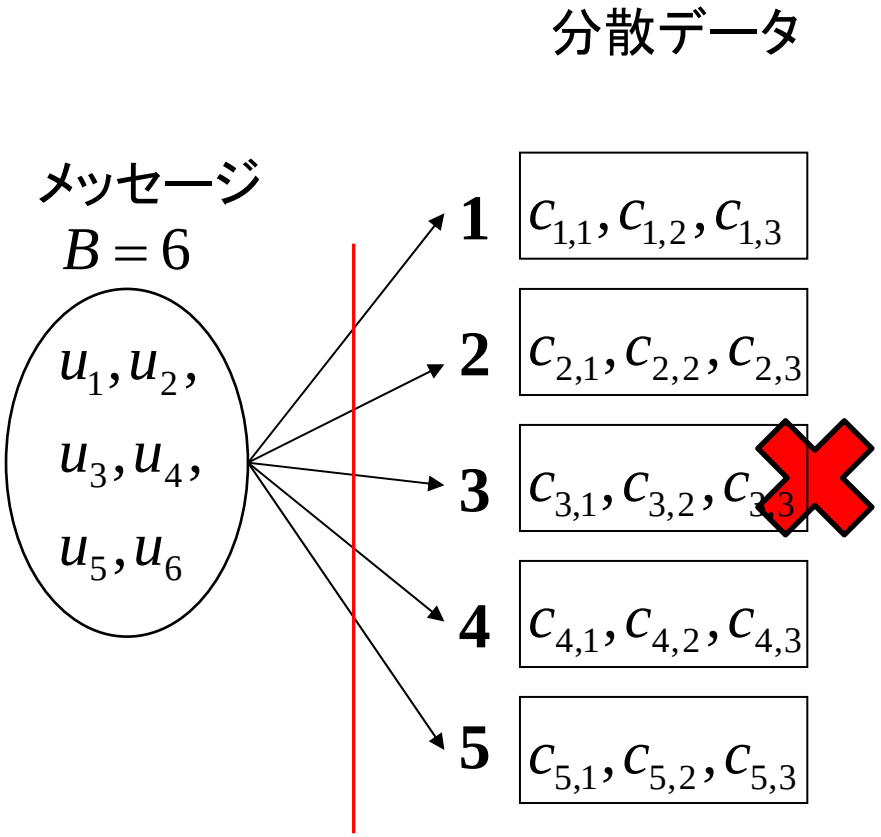
復元(復号)

復元のためにアクセスするノード数 $k=3$





故障ノードの修復問題(システムの信頼性の維持)



「アクセスできない」
と仮定する

故障ノードの修復

1. 故障したノードを新しいノードに置き換える。

2. そして、故障ノードが保存していた分散データの複製を保存したい。
（再生成）

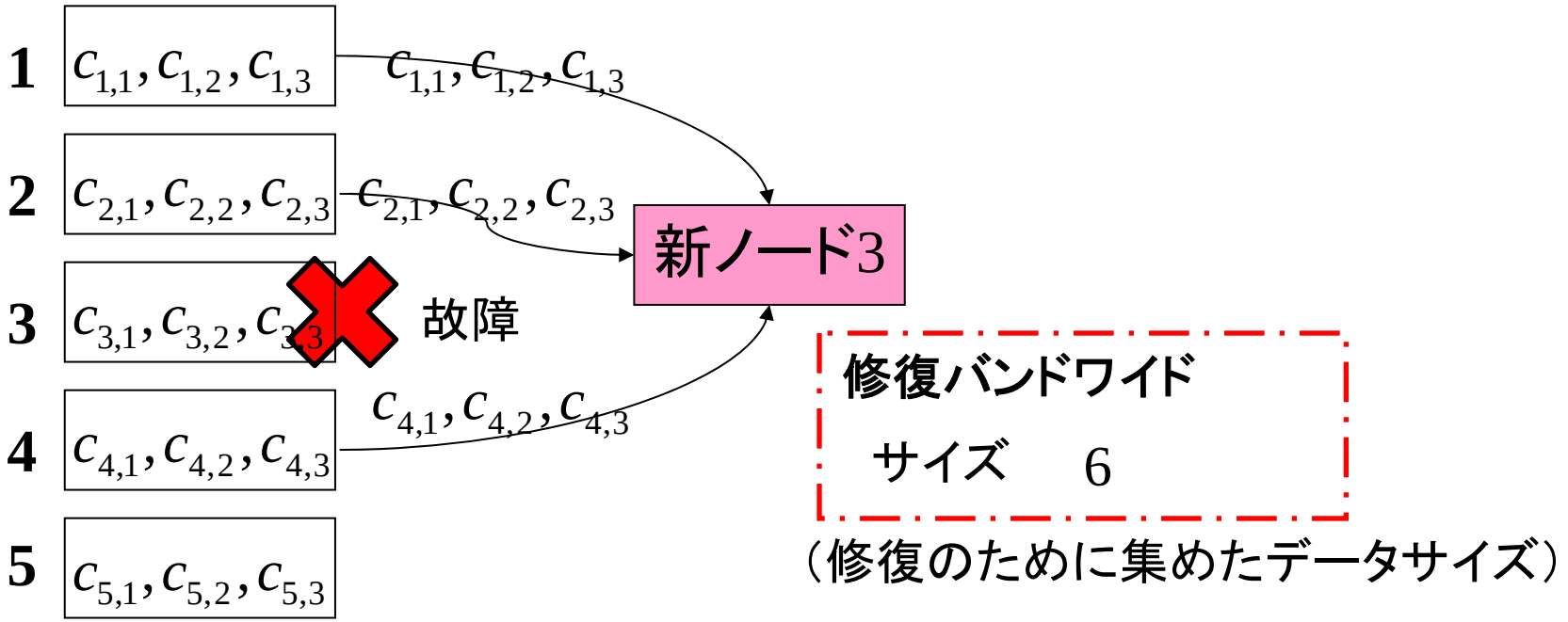
ただし、再び、ソースから分散データを受信することはできないと仮定する。

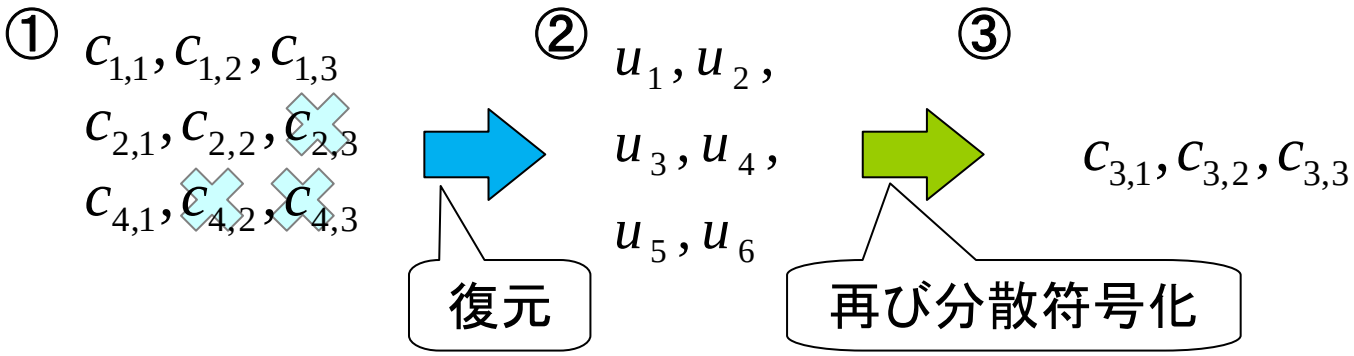
修復(復元を利用した自明な方法)

分散データ

ストレージサイズ $\alpha = 3$

修復するためにアクセスするノード数 $d = 3$





修復(自明でない方法):再生成用データ

$d = 3$

分散データ
ストレージサイズ $\alpha = 3$

符号化

$c_{i,1}, c_{i,2}, c_{i,3}$ 分散データ → $d_{f,i}$ 再生成用データ
サイズ β

1 $c_{1,1}, c_{1,2}, c_{1,3}$

2 $c_{2,1}, c_{2,2}, c_{2,3}$

3 $c_{3,1}, c_{3,2}, c_{3,3}$ 故障

4 $c_{4,1}, c_{4,2}, c_{4,3}$

5 $c_{5,1}, c_{5,2}, c_{5,3}$

$d_{3,1}$, $d_{3,2}$, $d_{3,4}$ → 新ノード3

修復バンドワイド
サイズ $d\beta = 3 \times 1 = 3$

$u_k, c_{j,k}, d_{l,m} \in GF(q)$

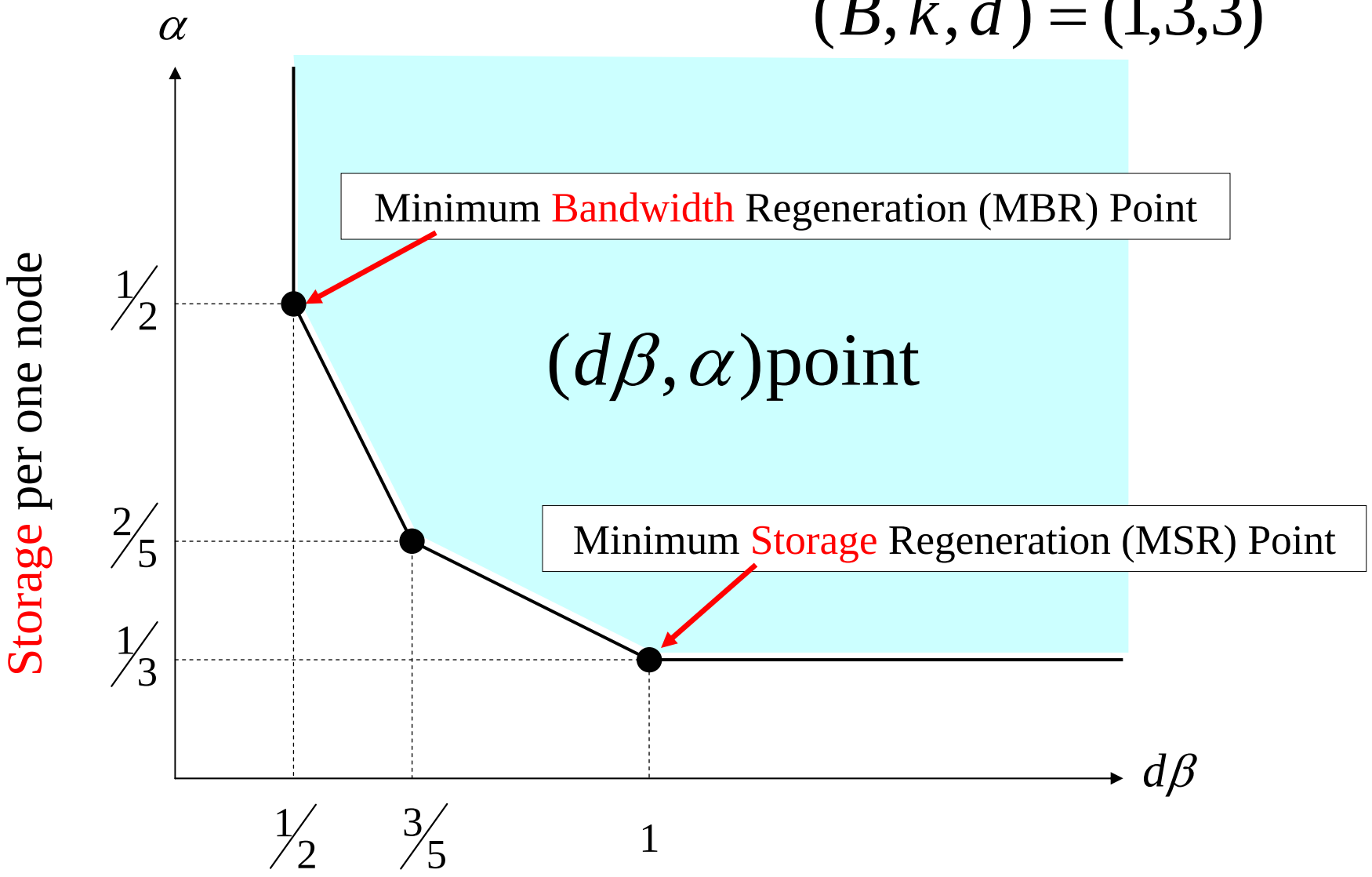
① 再生成用データ ②

$d_{3,1}, d_{3,2}, d_{3,4}$ → $c_{3,1}, c_{3,2}, c_{3,3}$

再生成(符号化処理)

Optimal Tradeoff curve between repair bandwidth $d\beta$ and storage α

$$(B, k, d) = (1,3,3)$$



再生成符号

1. **ストレージ α と 修復バンドワイド $d\beta$ のトレードオフ**
   1. **修復バンドワイドを最小**:
      → **最小バンドワイド再生成符号**
      (Minimum Bandwidth Regenerating(MBR) codes)
   2. **ストレージを最小**:
      → **最小ストレージ再生成符号**
      (Minimum Storage Regenerating(MSR) codes)
2. **一般的な再生成符号の一構成方法（最初の）**
   1. [7] Rashmi, Shah, and Kumar, "Optimal Exact-Regenerating Codes for Distributed Storage at the MSR and MBR Points via a Product-Matrix Construction," 2010.

目的（提案）

1. **本発表の目的（提案）**:
   最小バンドワイド再生成 (MBR) **符号を用いたランプ型秘密分散法**
   1. Rashmi-Shah-Kumar MBR **符号** [7] **の特別な場合**
      （[6] **とは異なる符号）**
   2. **（拡張符号** [9] **の特別な場合）**

2. **関連研究**:
   1. [1, Pawar, Rouayheb and Ramchandran] **：**
      最小バンドワイド再生成 (MBR) **符号を用いた秘密分散法**
      1. Secrecy Capacity $C_S(\alpha, d\beta)$
      2. **「**[5, Subramanian, *et.al.*] **の秘密分散法」 と**
         「[6, Rashmi, *et.al.*] **の最小バンドワイド再生成符号」 の組合せ**
   2. [8,9] **：**
      最小ストレージ再生成 (MSR) **符号を用いた秘密分散法**
      1. Rashmi-Shah-Kumar MSR **符号** [7]（[6] **とは異なる符号）**
      2. Rashmi-Shah-Kumar MSR **符号** [7] **の拡張符号**

（上記のことを図を用いて説明（3 **頁））**

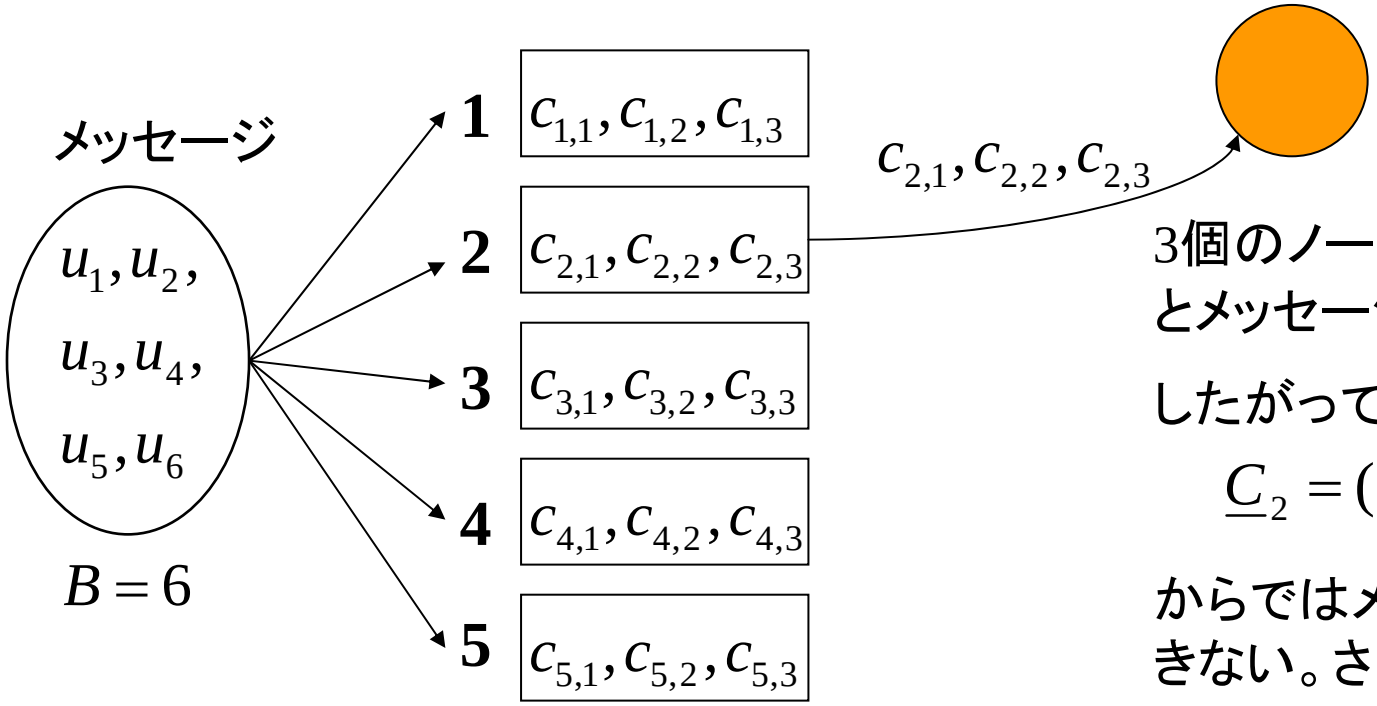
再生成符号を用いた秘密分散法（分散データ）

$(k,d)=(3,3)$

秘密情報： $\underline{S}=(u_1,u_2,u_3)$

乱数： $\underline{R}=(u_4,u_5,u_6)$

$$H(\underline{S}\,|\,\underline{C}_i)=H(\underline{S})$$



3個のノードにアクセスしないとメッセージを復元できない。

したがって、1個の分散データ

$$\underline{C}_2=(c_{2,1},c_{2,2},c_{2,3})$$

からではメッセージを復元できない。さらに、

$$H(\underline{S}\,|\,\underline{C}_2)=H(\underline{S})$$

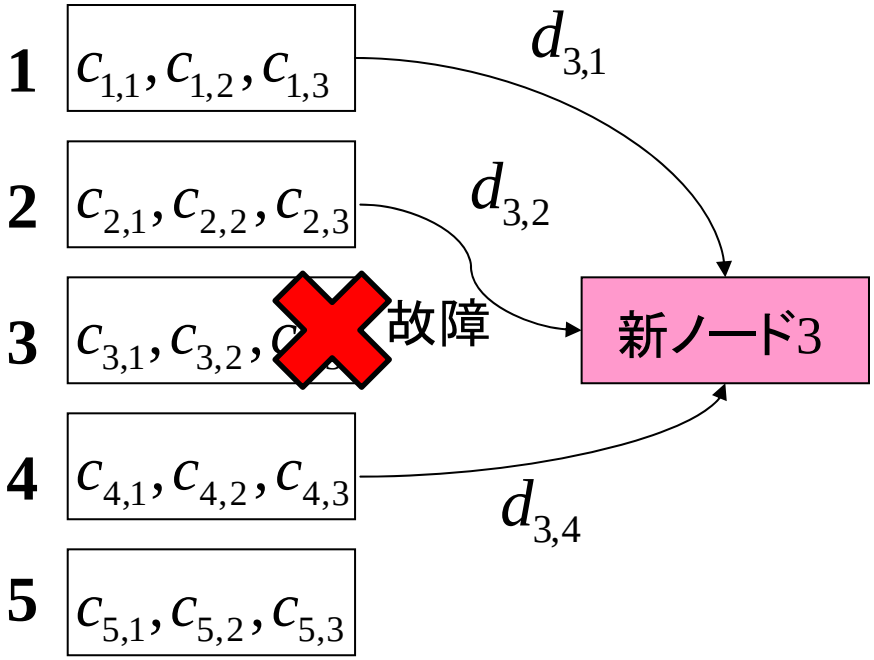
が成り立つ。

再生成符号を用いた秘密分散法（再生成用データ） $(k,d)=(3,3)$

秘密情報： $\underline{S}=(u_1,u_2,u_3)$

乱数： $\underline{R}=(u_4,u_5,u_6)$

$$H(\underline{S}\,|\,\underline{D}_i)=H(\underline{S})$$



再生成用データ

$$\underline{D}_3=(d_{3,1},d_{3,2},d_{3,4})$$

に対し、

$$H(\underline{S}\,|\,\underline{D}_3)=H(\underline{S})$$

が成り立つ。

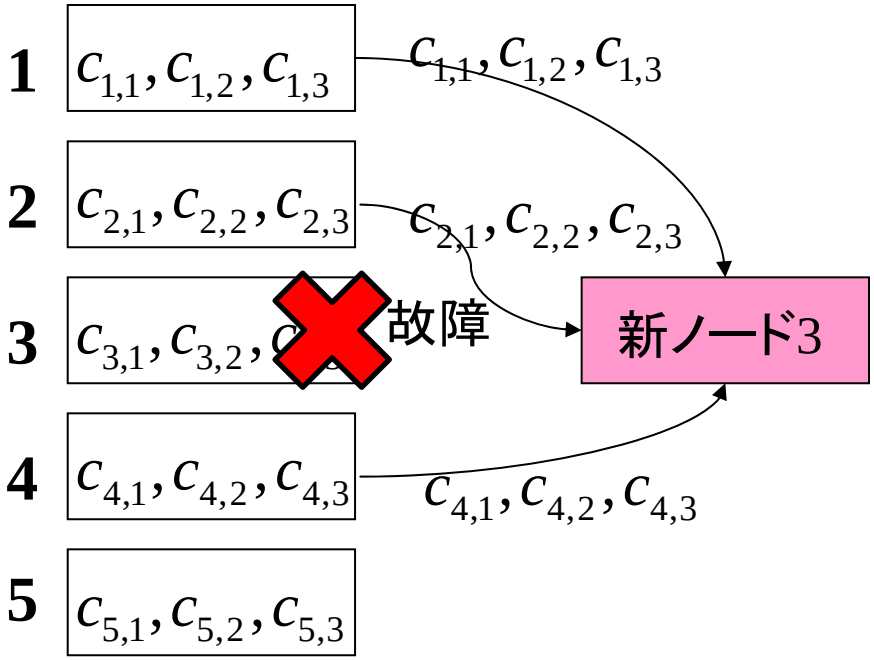
再生成符号を用いると、秘密情報が全くもれることなく、分散データを再生成できる。

復元を利用した自明な方法による修復の場合

秘密情報： $\underline{S} = (u_1, u_2, u_3)$

乱数： $\underline{R} = (u_4, u_5, u_6)$

$$H(\underline{S} \mid \underline{C}_1 \underline{C}_2 \underline{C}_4) = 0$$



① $\underline{C}_1 = (c_{1,1}, c_{1,2}, c_{1,3})$
$\underline{C}_2 = (c_{2,1}, c_{2,2}, c_{2,3})$
$\underline{C}_4 = (c_{4,1}, c_{4,2}, c_{4,3})$

↓ 復元

② $u_1, u_2, u_3,$
u_4, u_5, u_6

↓ 再び分散符号化

③ $c_{3,1}, c_{3,2}, c_{3,3}$

最小バンドワイド再生成 (MBR) 符号 [7] の設定

1. **パラメータ** $(n, k, d, \alpha, \beta, B)$
   - n : ストレージノードの個数（分散データの個数）
   - k : 復元のためにアクセスするノードの個数
   - d : 修復のためにアクセスするノードの個数
   - α : 分散データのサイズ
   - β : 再生成用データのサイズ ($\beta = 1$)
   - B : メッセージのサイズ

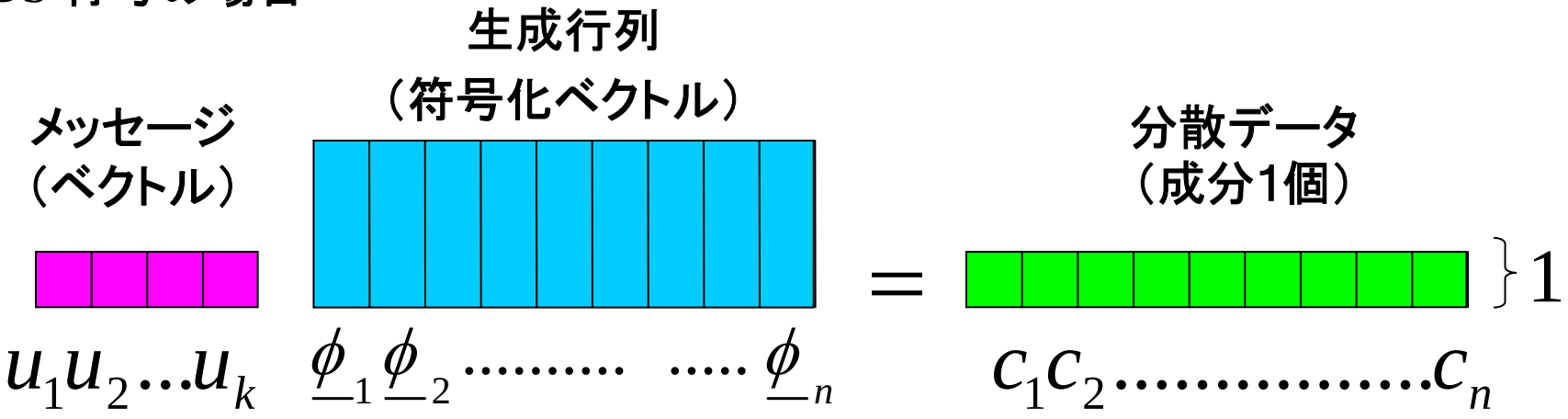
2. **パラメータ設定 (主要なものは、α によって定まる)**

$$
\begin{aligned}
k &= d = \alpha, \\
B &= \frac{\alpha(\alpha+1)}{2}, \\
\beta &= 1, \\
n &> |GF(q)|.
\end{aligned}
$$

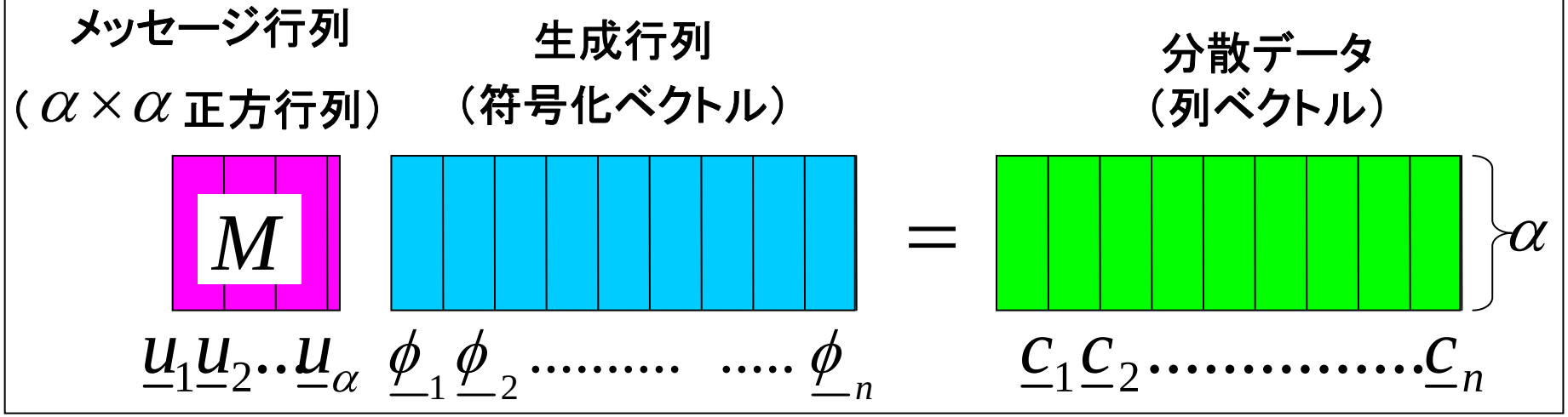
（MBR 符号の符号化の様子を図を用いて説明（1 頁））

MBR 符号の符号化の様子

MDS 符号の場合



MBR 符号の場合



メッセージ行列（MBR 符号 [7]）

1. メッセージ行列 M は，$\alpha \times \alpha$ **対称行列**：

$$M = \begin{bmatrix} u_{1,1} & u_{1,2} & \cdots & u_{1,\alpha} \\ u_{2,1} & u_{2,2} & \cdots & u_{2,\alpha} \\ \vdots & \vdots & \ddots & \vdots \\ u_{\alpha,1} & u_{\alpha,2} & \cdots & u_{\alpha,\alpha} \end{bmatrix}$$

（異なる成分の個数） $= \frac{\alpha(\alpha+1)}{2} = B =$ **（メッセージのサイズ）**

分散データ（MBR 符号 [7]）

1. **ノード i の符号化ベクトル $\underline{\phi}_i \in \mathbb{F}_q^\alpha$:**

$$\underline{\phi}_i = \left[1, x_i, x_i^2, \ldots, x_i^{\alpha-1}\right]^t \in \mathbb{F}_q^\alpha$$

ノード $i \in \{1, 2, \ldots, n\}$ に対し、非零な有限体の要素 $x_i \in \mathbb{F}_q$ を対応させ、かつ、 $x_i \neq x_j$ if $i \neq j$.

2. **ノード i の分散データ $\underline{C}_i \in \mathbb{F}_q^\alpha$: （分散符号化）**

$$\underline{C}_i = \begin{bmatrix} c_{i,1} \\ c_{i,2} \\ c_{i,3} \\ \vdots \\ c_{i,\alpha} \end{bmatrix} = \begin{bmatrix} u_{1,1} & u_{1,2} & \cdots & u_{1,\alpha} \\ u_{2,1} & u_{2,2} & \cdots & u_{2,\alpha} \\ \vdots & \vdots & \ddots & \vdots \\ u_{\alpha,1} & u_{\alpha,2} & \cdots & u_{\alpha,\alpha} \end{bmatrix} \begin{bmatrix} 1 \\ x_i \\ x_i^2 \\ \vdots \\ x_i^{\alpha-1} \end{bmatrix} \in \mathbb{F}_q^\alpha$$

復元（MBR 符号 [7]）

1. $k = \alpha$ 個のノード（分散データ）にアクセスすることで復元できる.
2. なぜなら、α 個の符号化ベクトルを並べた $\alpha \times \alpha$ 正方行列 の行列式は、Vandermonde の行列式であるから.
3. この場合、復元のために、サイズ α^2 の分散データをダウンロードすることを仮定している.

- しかし，ランプ型秘密分散法の性能評価より，
  ダウンロードする分散データのサイズは，
  メッセージサイズ $B = \dfrac{\alpha(\alpha+1)}{2}$ で，
  必要十分であることが明らかになる．

修復（MBR 符号 [7]）

1. **故障ノード $f \in \{1, 2, ..., n\}$ の修復 :**
   故障していない任意の $d = \alpha$ 個の各ノード $h_1, h_2, \ldots, h_\alpha$ でサイズ $\beta = 1$ の再生成用データ

$$d_{f,h_p} = \underline{C}_{h_p}^t \underline{\phi}_f \in \mathbb{F}_q,\ 1 \le p \le \alpha$$

を生成し，ダウンロードし，再生成用データのベクトル

$$\underline{D}_f = \left[d_{f,h_1}, d_{f,h_2}, \cdots, d_{h_{f,\alpha}} \right]^t$$

を得る。そして，$\underline{D}_f$ から $\underline{C}_f$ を一意に再生成できる:

$$\underline{C}_f = \begin{bmatrix} \underline{\phi}_{h_1}^t \\ \vdots \\ \underline{\phi}_{h_\alpha}^t \end{bmatrix}^{-1} \underline{D}_f.$$

- **（この関係から，$\underline{C}_f$ から $\underline{D}_f$ も一意に決定できる. ）**

MBR 符号を用いた秘密分散法（安全性条件）の設定（その 1/2）

1. MBR 符号の設定: パラメータ α → (k, d, B)
2. **秘密分散法の設定**: パラメータ μ . ただし，$\mu < k$.
   μ → L_S (秘密情報のサイズ)
3. 秘密情報 $\underline{S} \in \mathbb{F}_q^{L_S}$: $L_S = H(\underline{S})$
   1. 任意の k 個 の分散データ $\underline{C}_{i_1}, \ldots, \underline{C}_{i_k}$ に対し，

$$H(\underline{S}|\underline{C}_{i_1}, \ldots, \underline{C}_{i_k}) = 0.$$

   2. 任意の μ 個 の再生成用データ $\underline{D}_{i_1}, \ldots, \underline{D}_{i_\mu}$ に対し，

$$H(\underline{S}|\underline{D}_{i_1}, \ldots, \underline{D}_{i_\mu}) = H(\underline{S}).$$

- （再生成用データと分散データの関係より，
  一般に，$H(\underline{S}|\underline{D}_{i_1}, \ldots, \underline{D}_{i_\mu}) \leq H(\underline{S}|\underline{C}_{i_1}, \ldots, \underline{C}_{i_\mu})$
  が成り立つ．）

Secrecy Capacity $C_S(\alpha, d\beta)$ [1, Pawar, *et.al.*]

1. **定義（(k,μ) で定まる.）**

$$C_s(\alpha, d\beta) := \sup H(\underline{S})$$
$$H(\underline{S}|\underline{C}_{i_1}, \ldots, \underline{C}_{i_k}) = 0, \ \forall i_1, \ldots, i_k \in \{1, \ldots, n\}$$
$$H(\underline{S}|\underline{D}_{i_1}, \ldots, \underline{D}_{i_\mu}) = H(\underline{S}), \ \forall i_1, \ldots, i_\mu \in \{1, \ldots, n\}$$

2. **上界** [1, Theorem 1] ← $(\alpha, \beta, k, d, \mu)$ **で定まる**.

$$C_s(\alpha, d\beta) \le \sum_{i=\mu+1}^{k} \min\{(d-i+1)\beta, \alpha\}$$

- **パラメータ** ν : $\mu \le \nu \le k$
  MBS **符号のパラメータ** (α, β, k, d) **に対し，**

$$g(\nu) := \sum_{i=\nu+1}^{k} \min\{(d-i+1)\beta, \alpha\}$$

とする.

ランプ型秘密分散法（安全性条件）の設定（その 2/2）

1. **秘密情報** $\underline{S} \in \mathbb{F}_q^{L_S}$
   （パラメータ ν **は，**$0 \le \nu \le k$ **を動く）**
   1. **任意の** ν **個の分散データ** $\underline{D}_{i_1}, \ldots, \underline{D}_{i_\nu}$ **に対し，**

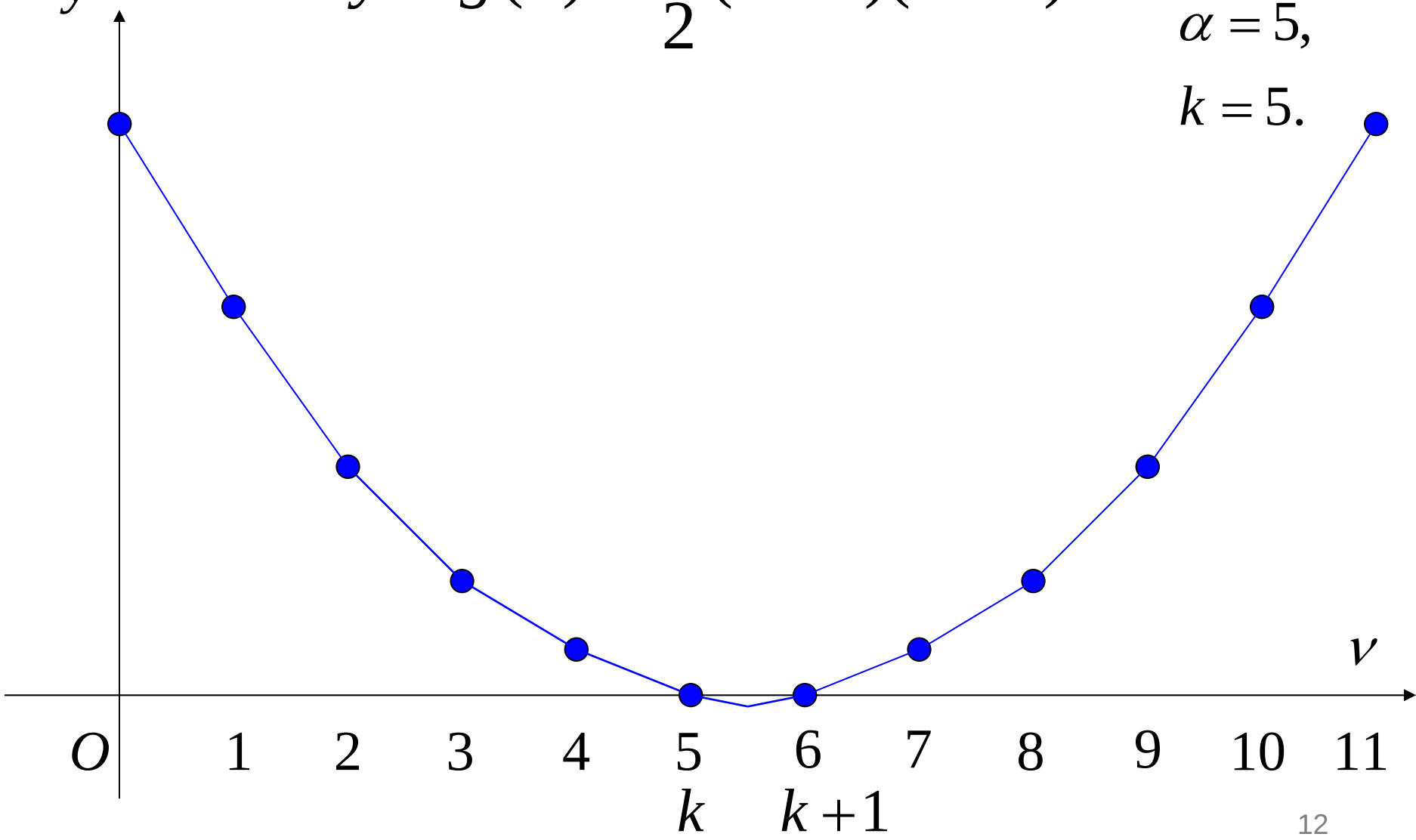
$$H(\underline{S}|\underline{D}_{i_1}, \ldots, \underline{D}_{i_\nu}) = \begin{cases} H(\underline{S}), & (0 \le \nu \le \mu) \\ \dfrac{g(\nu)}{L_S} H(\underline{S}), & (\mu + 1 \le \nu < k) \\ 0, & (k \le \nu) \end{cases}$$

が成り立つ．ただし，$(\alpha, \beta, k, d) = (\alpha, 1, \alpha, \alpha)$ **より，**

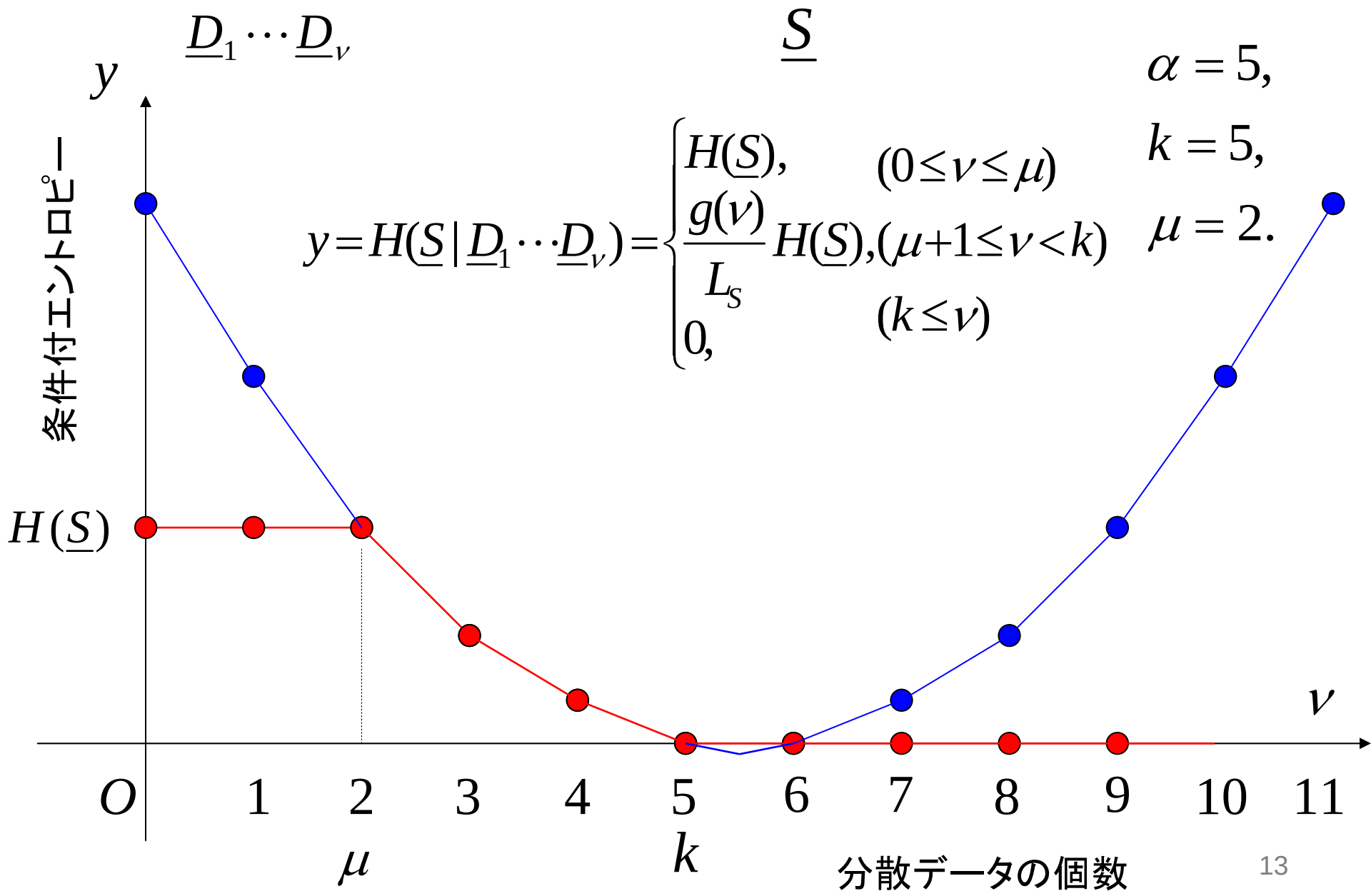
$$g(\nu) = \frac{1}{2}(\nu - k)(\nu - (k+1)).$$

（上記のことを図を用いて説明（4 頁））

$$y = g(\nu) = \frac{1}{2}(\nu - 5)(\nu - 6)$$



再生成用データが与えられた下での秘密情報の条件付エントロピー



再生成用データが与えられた下での秘密情報の条件付エントロピー

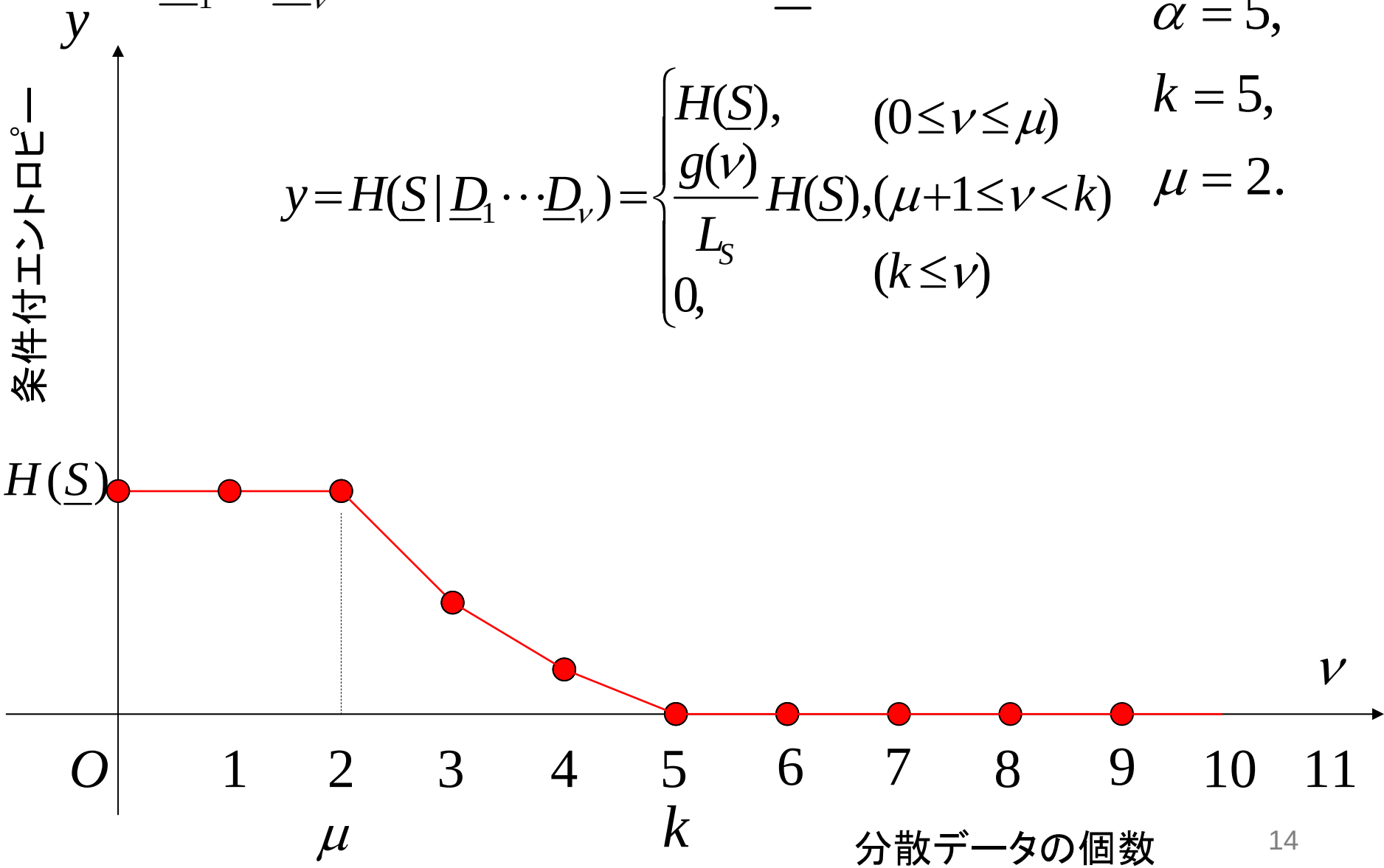
$\underline{D}_1 \cdots \underline{D}_\nu$ $\underline{S}$

$$y = H(\underline{S} \mid \underline{D}_1 \cdots \underline{D}_\nu) = \begin{cases} H(\underline{S}), & (0 \le \nu \le \mu) \\ \dfrac{g(\nu)}{L_S} H(\underline{S}), & (\mu+1 \le \nu < k) \\ 0, & (k \le \nu) \end{cases}$$

$\alpha = 5,$

$k = 5,$

$\mu = 2.$



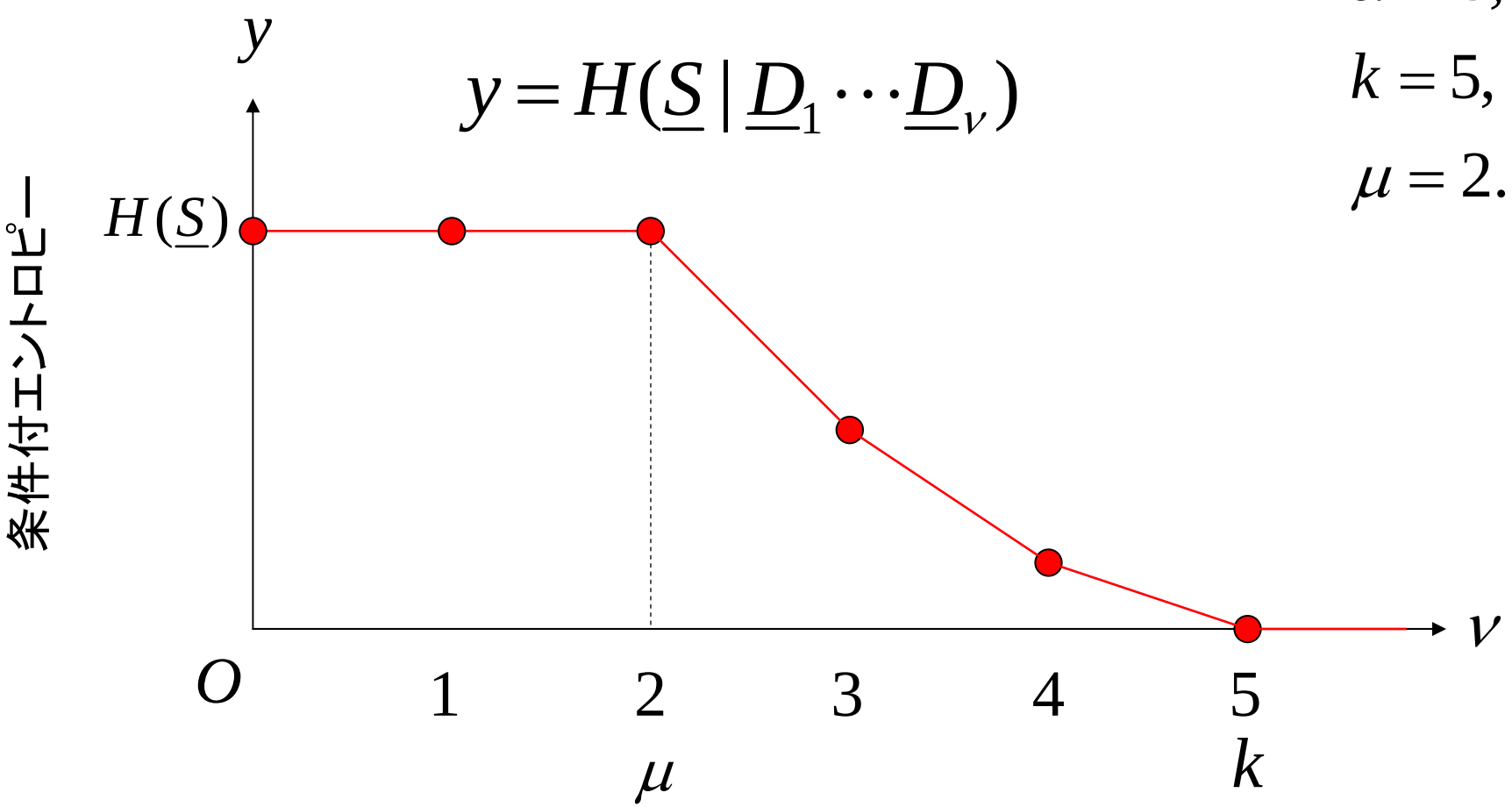
再生成用データが与えられた下での秘密情報の条件付エントロピー

$\underline{D}_1 \cdots \underline{D}_\nu$ $\underline{S}$

$\alpha = 5,$

$k = 5,$

$\mu = 2.$



秘密分散法の安全性条件に対応した符号の構成法（メッセージ行列内での秘密情報と乱数の配置）

1. サイズ B のメッセージの構成を**乱数**と**秘密情報**に分ける。
2. パラメータ μ → L_S：秘密情報のサイズ
   1. **乱数** $\underline{R} \in \mathbb{F}_q^{B-L_S}$
   2. **秘密情報** $\underline{S} \in \mathbb{F}_q^{L_S}$
3. たとえば、$(\alpha, \mu) = (5, 2)$ と設定するとき、メッセージ行列を

$$M = \begin{bmatrix} u_{1,1} & u_{1,2} & u_{1,3} & u_{1,4} & u_{1,\alpha} \\ u_{2,1} & u_{2,2} & u_{2,3} & u_{2,4} & u_{2,\alpha} \\ u_{3,1} & u_{3,2} & u_{3,3} & u_{3,4} & u_{3,\alpha} \\ u_{4,1} & u_{4,2} & u_{4,3} & u_{4,4} & u_{4,\alpha} \\ u_{\alpha,1} & u_{\alpha,2} & u_{\alpha,3} & u_{\alpha,4} & u_{\alpha,\alpha} \end{bmatrix}$$

と設定する．

（主対角線を含む $\mu = 2$ 個の対角線上に乱数を配置）

MBR 符号における 分散データ と 再生成用データ の安全性

① 分散データ

定理 7 任意の ν 個 の分散データ $\underline{C}_{i_1}, \ldots, \underline{C}_{i_\nu}$ に対し、

$$H(\underline{S}|\underline{C}_{i_1}, \ldots, \underline{C}_{i_\nu}) = \begin{cases} H(\underline{S}), & (0 \le \nu \le \mu) \\ \dfrac{g(\nu)}{L_S} H(\underline{S}), & (\mu + 1 \le \nu < k) \\ 0, & (k \le \nu) \end{cases}$$

が成り立つ。

② 再生成用データ

定理 9 任意の ν 個 の再生成用データ $\underline{D}_{i_1}, \ldots, \underline{D}_{i_\nu}$ に対し、

$$H(\underline{S}|\underline{D}_{i_1}, \ldots, \underline{D}_{i_\nu}) = H(\underline{S}|\underline{C}_{i_1}, \ldots, \underline{C}_{i_\nu})$$

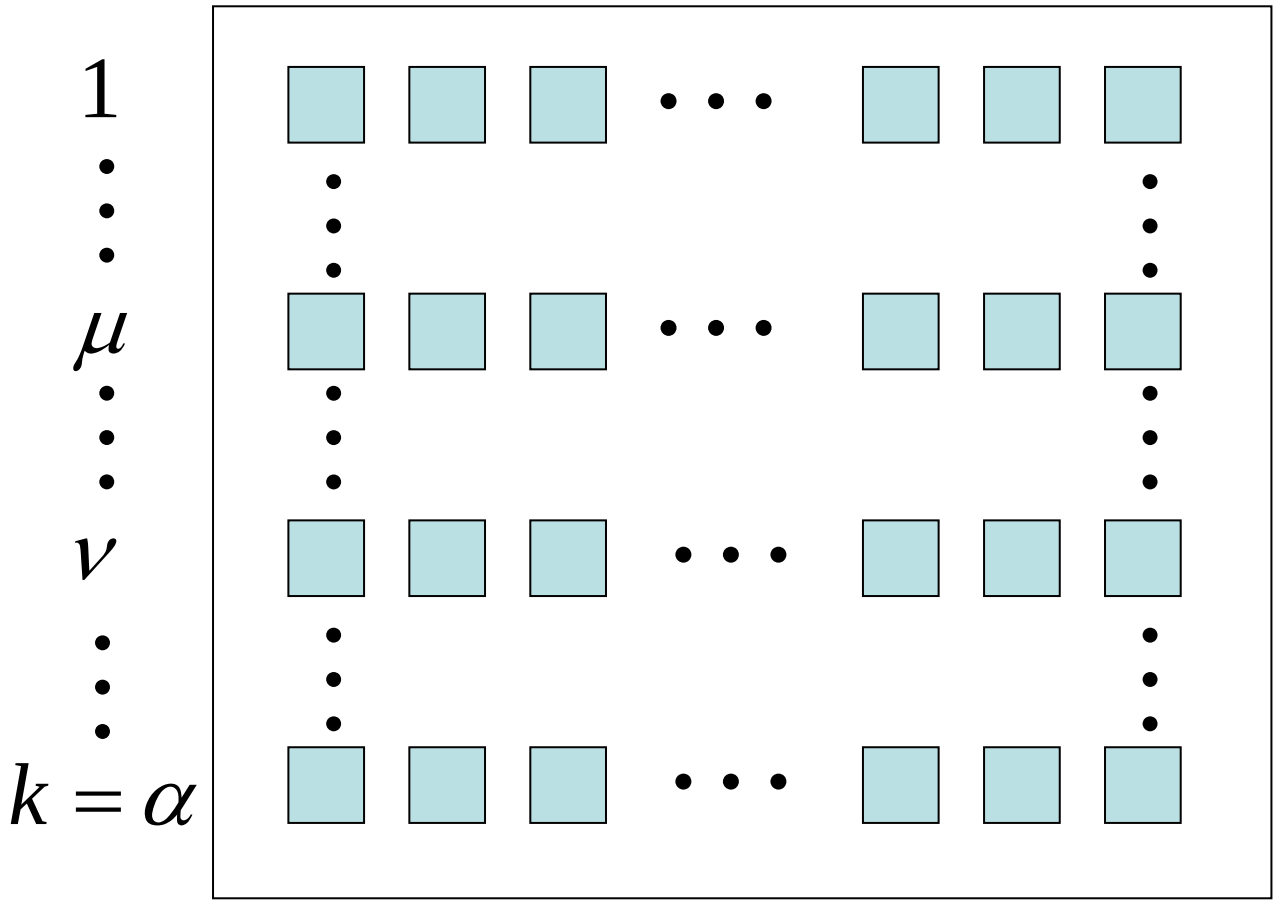
が成り立ことより、同様にして，

$$H(\underline{S}|\underline{D}_{i_1}, \ldots, \underline{D}_{i_\nu}) = \begin{cases} H(\underline{S}), & (0 \le \nu \le \mu) \\ \dfrac{g(\nu)}{L_S} H(\underline{S}), & (\mu + 1 \le \nu < k) \\ 0, & (k \le \nu) \end{cases}$$

が成り立つ。 （証明のポイントを図を用いて説明（3 頁））

定理7，9の証明のポイント（線形従属） その1/3

$i:\quad \underline{C}_i = (c_{i,1}, c_{i,2}, c_{i,3}, \cdots, \cdots, c_{i,8}, c_{i,9}, c_{i,\alpha})$



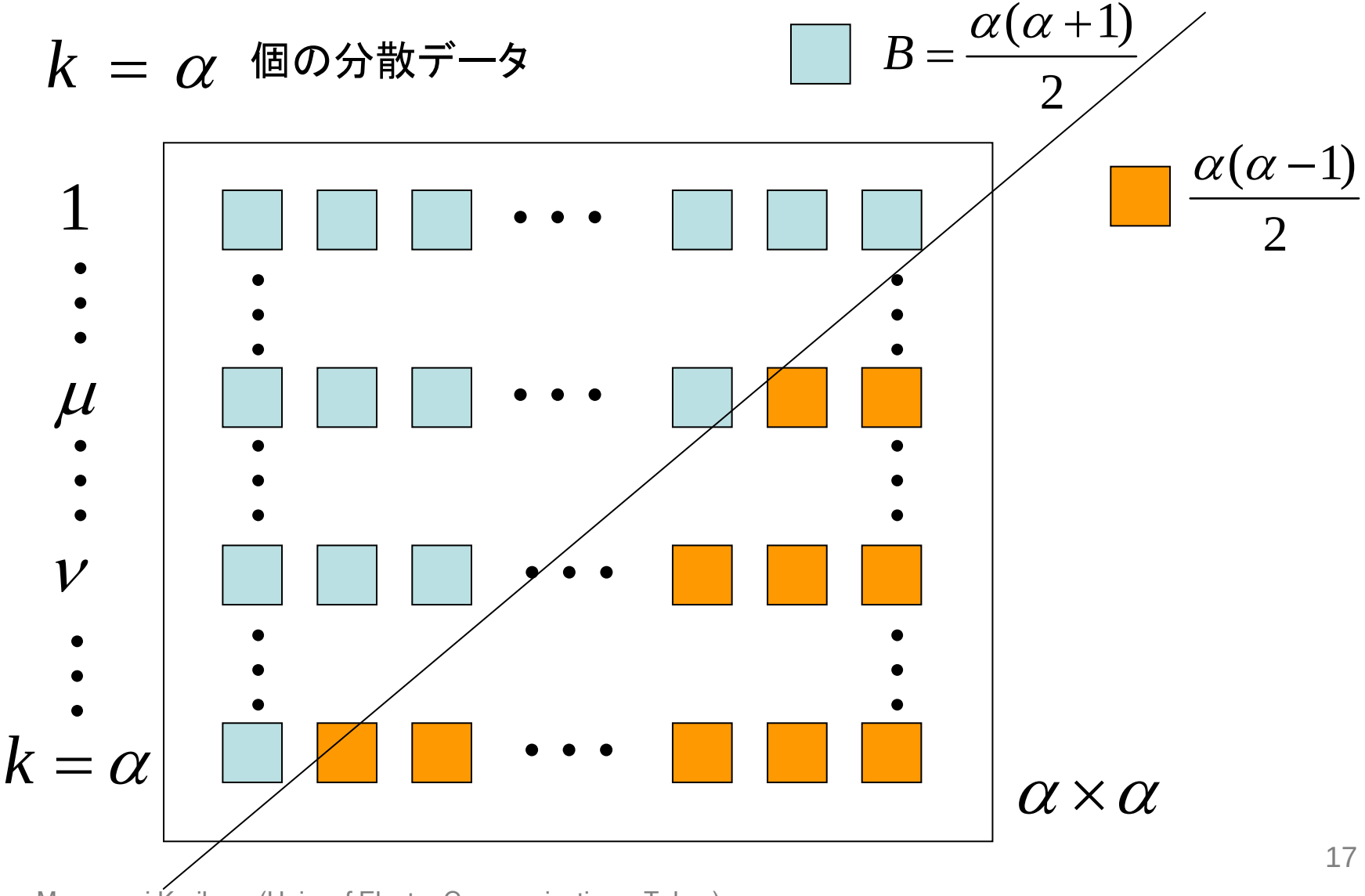
α 個の分散データ

メッセージサイズ

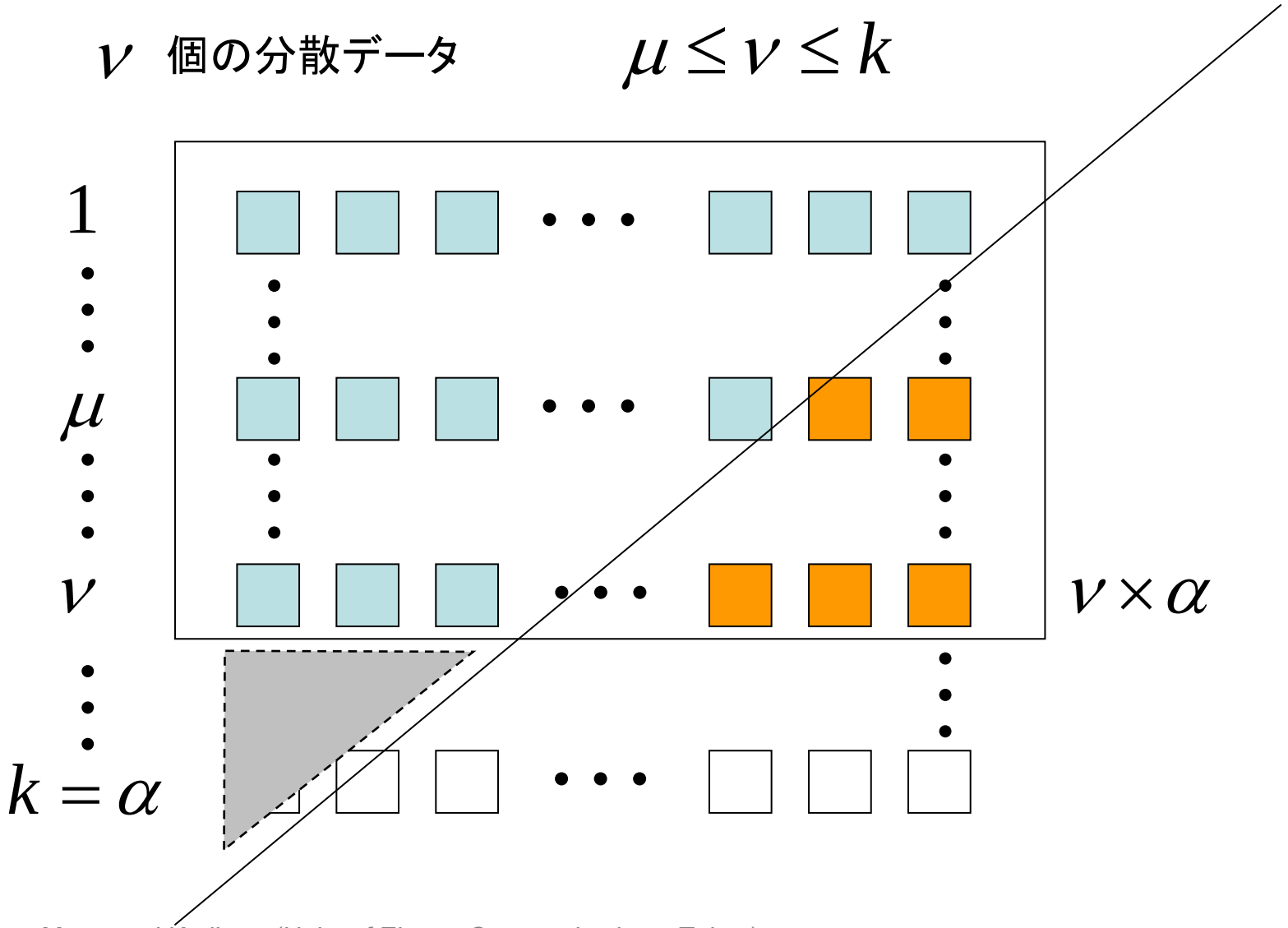
$$B = \frac{\alpha(\alpha+1)}{2}$$

$\alpha \times \alpha$

定理7，9の証明のポイント（線形従属） その2/3



定理7，9の証明のポイント（線形従属） その3/3



結論

本発表では，
修復可能な分散ストレージシステムにおける，

1. 最小バンドワイド再生成 (MBR) 符号を基にした
   ランプ型秘密分散法の構成方法を提案し，
2. その安全性の性能を示した（評価した）。

主な参考文献

- [1] S.Pawar, S.E.Rouayheb and K.Ramchandran, “On Secure Distributed Data Storage Under Repair Dynamics,” http://arxiv.org/abs/1003.0488, arXiv:1003.0488v2, 2010.
- [2] A.G.Dimakis, P.B.Godfrey, Y.Wu, M.J.Wainwright and K.Ramchandran, ”Network Coding for Distributed Storage Systems,” IEEE Trans. on Information Theory, vol.56, no.9, pp.4539–4551, Sept. 2010.
- [5] S.Subramanian and S.W.McLaughlin, “MDS codes on the erasure-erasure wiretap channle,” http://arxiv.org/abs/0902.3286, arXiv:0902.3286v1, 2009.
- [6] K.V.Rashmi, N.B.Shah, P.V.Kumar and K.Ramchandran, “Explicit Construction of Optimal Exact Regenerating Codes for Distributed Storage,” in Proc. Forty-Seventh Annual Allerton Conference, Allerton House, UIUC, Illinois, USA, September 30 – October 2, 2009, pp.1243–1249, 2009.
- [7] K.V.Rashmi, N.B.Shah, and P.V.Kumar, “Optimal Exact-Regenerating Codes for Distributed Storage at the MSR and MBR Points via a Product-Matrix Construction,” http://arxiv.org/abs/1005.4178
- [8] **栗原正純**, **桑門秀典**, “**分散ストレージにおける再生成符号と秘密分散について**,” **信学技報**, IT2010-56(2011-01), pp.13-18, Jan. 2011.
- [9] **栗原正純**, **桑門秀典**, “Rashmi-Shah-Kumar **再生成符号の拡張と秘密分散について**,” **信学技報**, IT2010-114(2011-03), pp.303-310, Mar. 2011.