論文

分散情報の安全性を考慮した再生成符号における最小ストレージ再生成符号の最適性に関する一検討

吉田隆弘

1　はじめに

分散ストレージ方式とは重要な情報であるオリジナル情報を n 個のノードに分散させて保管し，必要なときに k 個 ($k \leq n$) のノードの分散情報からオリジナル情報が復元できる方式である．よって，故障等によって一部のノードの分散情報が利用できなくなった場合でも，正常なノードが k 個以上存在していれば，それらのノードの分散情報からオリジナル情報が復元できるため信頼性が確保できる．このような方式は，リード・ソロモン符号のような最大距離分離 (MDS: Maximmum Distance Separable) 符号 [1] を利用することで実現できる．

また，故障したノードを修復できるほうが信頼性の観点からより望ましいため，故障ノードが修復可能な分散ストレージ方式を実現する再生成符号と呼ばれる符号クラスが提案された [2]．再生成符号における故障ノード修復機能とは，$k \leq d$ を満たす任意の d 個の故障していない正常なノードが生成する故障ノード修復用の情報 (以下では再生成情報と呼ぶ) から故障ノードの分散情報を復元する機能である．この再生成符号に対して，各ノードが記憶する分散情報の記憶容量 (以下ではストレージと呼ぶ) と故障ノードを修復するために必要な d 個の再生成情報の大きさ (以下では修復バンドワイズと呼ぶ) は，いずれも小さいほうが望ましいが両者にはトレードオフがあることが示されている [2]．このトレードオフにおいて，ストレージが最小となるときに修復バンドワイズを最小とする最小ストレージ再生成符号，及び修復バンドワイズが最小となるときにストレージを最小とする最小バンドワイズ再生成符号が提案されている [3, 4, 5, 6]．

さらに従来の再生成符号のクラスに対して，分散情報の情報漏洩量を考慮した制約条件を追加することで再生成符号のクラスを限定した 2 つの符号クラスが提案されている [7]．また，Rashmi らによって提案された最小ストレージ再生成符号と最小バンドワイズ再生成符号 [4] が，これら 2 つの符号クラスにそれぞれ含まれ，かつストレージと修復バンドワイズを共に最小とする最適な再生成符号であることが示されている [7]．しかし従来研究では，Rashmi らの最小ストレージ再生成符号に対する最適性の証明が示されていない．そこで本稿では，従来研究で示されていなかった Rashmi らの最小ストレージ再生成符号に対する最適性の証明を示す．

本稿の構成は以下のとおりである．2 章では，本稿の解析で主に用いるエントロピーや相互情報量の性質等の情報理論における基本事項について紹介する．3 章では従来示されている修復可能な分散ストレージ方式のモデル，分散情報の情報漏洩量を考慮した再生成符号の符号クラス，及び Rashmi らの最小ストレージ再生成符号の概要を紹介する．次に，4 章で Rashmi らが提案した最小ストレージ再生成符号が，3 章で紹介した符号クラスに含まれ，ストレージと修復バンドワイズを共に最小とする最適な再生成符号となることを示す．最後に 5 章でまとめる．

2　準備

本章では，再生成符号の定義や解析において，頻繁に利用する情報理論におけるエントロピーと相互情報量の定義，及びエントロピーと相互情報量の基本的性質 [8] について紹介する．

ここで，可算集合 $\mathcal{X}$ に値をとる確率変数を X とおき，確率変数 X の確率分布を

$$p_X(x) = \Pr\{X = x\},\ x \in \mathcal{X}, \tag{1}$$

とする．以下，任意の確率変数に対する確率分布を上記のように表す．また，任意の 2 つの整数 m, n に対して，長さ $n-m+1$ の任意の系列 $X_m, X_{m+1}, \cdots, X_n$ を X_m^n とおく場合がある．ただし，$n < m$ のときは空系列とする．

2.1　エントロピーとその基本的性質

確率変数 X のエントロピー $H(X)$ は，

$$H(X) = -\sum_{x\in\mathcal{X}} p_X(x)\log p_X(x) \tag{2}$$

として定義される[1]．また，可算集合 $\mathcal{X}_1\times\mathcal{X}_2\times\cdots\times\mathcal{X}_N$ に値をとり $(N\geq 2)$，同時確率分布

$$p_{X_1^N}(x_1^N) = \Pr\left\{X_1^N = x_1^N\right\},\quad x_1^N \in \mathcal{X}_1\times\mathcal{X}_2\times\cdots\times\mathcal{X}_N \tag{3}$$

を持つ N 個の確率変数の組 $(X_1, X_2, \cdots, X_N)$ に対するエントロピー

$$\begin{aligned} H\left(X_1^N\right) &= H(X_1, X_2, \cdots, X_N) \\ &= -\sum_{x_1\in\mathcal{X}_1}\cdots\sum_{x_N\in\mathcal{X}_N} p_{X_1^N}(x_1^N) \\ &\quad\times\log p_{X_1^N}(x_1^N) \end{aligned} \tag{4}$$

を同時エントロピーと呼ぶ．

可算集合 $\mathcal{X}\times\mathcal{Y}$ に値をとり，同時確率分布 $p_{XY}(x,y)$ を持つ 2 つの確率変数 X, Y に対し，Y が与えられたときの X の条件付きエントロピー $H(X\mid Y)$ は，

$$H(X\mid Y) = -\sum_{x\in\mathcal{X}}\sum_{y\in\mathcal{Y}} p_{XY}(x,y)\log p_{X|Y}(x\mid y) \tag{5}$$

として定義される．ここで，$p_{X|Y}(x\mid y)$ は条件 $Y=y$ のもとでの $X=x$ の条件付き確率分布で，次のように定義される．

$$p_{X|Y}(x\mid y) = \frac{p_{XY}(x,y)}{p_Y(y)}. \tag{6}$$

上記のエントロピー，同時エントロピー，及び条件付きエントロピーは，次のような性質を持つ．

定理 1. ([8, 補題 2.1.1]) エントロピーは常に非負値をとる．すなわち，任意の確率変数 X に対して，

$$H(X)\geq 0 \tag{7}$$

が成り立つ．□

定理 1 の非負性は，同時エントロピーと条件付きエントロピーについても同様に成り立つ．

定理 2. ([8, 定理 2.6.4]) エントロピーは一様分布のときに最大となる．すなわち，任意の確率変数 X に対して，

$$\log|\mathcal{X}| \geq H(X) \tag{8}$$

が成り立つ．等号は X が $\mathcal{X}$ 上で一様に分布している場合，かつその場合に限る．□

[1] 本稿を通じて対数の底は 2 とする．

このような性質は，同時エントロピーと条件付きエントロピーについても同様に成り立つ．

複数の確率変数に対して，次のようなチェイン則が成り立つ．

定理 3. ([8, 定理 2.5.1]) 任意の N 個の確率変数 $X_1, X_2, \cdots, X_N$ に対して，

$$H\left(X_1^N\right) = \sum_{i=1}^{N} H\left(X_i\mid X_1^{i-1}\right) \tag{9}$$

が成り立つ．□

2.2　相互情報量とその基本的性質

2 つの確率変数 X, Y に対して，X と Y の相互情報量 $I(X;Y)$ は，

$$\begin{aligned} I(X;Y) &= H(X) - H(X\mid Y) \\ &= \sum_{x\in\mathcal{X}}\sum_{y\in\mathcal{Y}} p_{XY}(x,y) \\ &\quad\times\log\frac{p_{XY}(x,y)}{p_X(x)p_Y(y)} \end{aligned} \tag{10}$$

として定義される．また，3 つの確率変数 X, Y, Z に対して，Z が与えられたときの X と Y の条件付き相互情報量 $I(X;Y\mid Z)$ は，

$$I(X;Y\mid Z) = H(X\mid Z) - H(X\mid Y,Z) \tag{11}$$

として定義される．

上記の相互情報量と条件付き相互情報量は，次のような性質を持つ．

定理 4. ([8, 定理 2.4.1]) 相互情報量と条件付き相互情報量は対称性を持つ．すなわち，任意の確率変数 X, Y, Z に対して，

$$I(X;Y) = I(Y;X), \tag{12}$$

$$I(X;Y\mid Z) = I(Y;X\mid Z) \tag{13}$$

が成り立つ．□

定理 4 より，明らかに，

$$\begin{aligned} H(X) - H(X|Y) &= H(Y) - H(Y|X), \\ H(X|Z) - H(X|YZ) &= H(Y|Z) - H(Y|XZ) \end{aligned}$$

が成立する．

エントロピーと同様に，相互情報量，及び条件付き相互情報量は常に非負値をとる．すなわち，以下の定理が成立する．

定理 5. ([8, 定理 2.6.3]) 任意の確率変数 X, Y, Z に対して,

$$\begin{aligned} I(X;Y) &\geq 0, \\ I(X;Y \mid Z) &\geq 0 \end{aligned} \tag{14}$$

が成り立つ. □

定理 5 から, 以下の関係が成り立つ.

定理 6. ([8, 定理 2.6.5]) 任意の確率変数 X, Y, Z に対して,

$$H(X \mid Y) \leq H(X), \tag{15}$$

$$H(X \mid Y, Z) \leq H(X \mid Z) \tag{16}$$

が成り立つ. 式 (15) の等号は X と Y が互いに独立であるとき, かつそのときに限られる. また, 式 (16) の等号は Z が与えられたもとで X と Y が互いに独立であるとき, かつそのときに限られる. □

定理 6 は, 条件付きエントロピーに条件を加えることで, その量が減少することはあっても増加することはないことを示している.

3 従来研究

本章では, 従来の修復可能な分散ストレージ方式のモデルと分散情報の情報漏洩量を考慮した再生成符号の符号クラス [2, 7], 及び Rashmi らの最小ストレージ再生成符号 [4] を紹介する.

3.1 修復可能な分散ストレージ方式

修復可能な分散ストレージ方式は, n 個のノード $\mathrm{N}_1, \mathrm{N}_2, \ldots, \mathrm{N}_n$ とデータコレクター DC によって構成される. これら n 個のノードの集合を

$$\mathcal{N} = \{\mathrm{N}_1, \mathrm{N}_2, \ldots, \mathrm{N}_n\} \tag{17}$$

とおく. また, 各ノードに分散させて記憶するオリジナル情報を s で表し, オリジナル情報 s 全体の集合を $\mathcal{S}$ とおく. ただし, $\mathcal{S}$ は有限集合とする. このとき, S を $\mathcal{S}$ 上の確率変数とし, $s \in \mathcal{S}$ は $\mathcal{S}$ 上の一様分布 p_S に従って発生するものとする. すなわち,

$$p_S(s) = \frac{1}{|\mathcal{S}|}, \ \forall s \in \mathcal{S} \tag{18}$$

となる. 修復可能な分散ストレージ方式は, 以下のように定義できる.

定義 1. 4 つの有限集合 $\mathcal{N}$, $\mathcal{S}$, $\mathcal{U}$, $\mathcal{V}$, 4 つの関数 F, G, f, g, 及び $n > d \geq k$ を満たす正整数 n, k, d を公開情報とする. このとき, 次の 3 つのフェーズから構成される方式を $[n, k, d]$ 分散ストレージ方式 (DSS: Distributed Storage Systems) と呼ぶ.

<分散情報生成フェーズ>

管理者は, 関数 $F : \mathcal{S} \to \mathcal{U}^n$ を用いてオリジナル情報 $s \in \mathcal{S}$ に対する n 個の分散情報

$$(u_1, u_2, \ldots, u_n), \ u_j \in \mathcal{U}, \ 1 \leq j \leq n \tag{19}$$

を生成する [2]. すなわち, オリジナル情報 s から

$$F(s) = (u_1, u_2, \ldots, u_n), \ u_j \in \mathcal{U}, j = 1, 2, \ldots, n \tag{20}$$

を計算する. 次に, u_j を安全な通信路を用いてノード N_j に送信する. ノード N_j は, 受信した分散情報 u_j をそれぞれ記憶する.

<オリジナル情報復元フェーズ>

データコレクター DC は n 個のノードから k 個のノード $\mathrm{N}_{j_1}, \mathrm{N}_{j_2}, \ldots, \mathrm{N}_{j_k}$ を任意に選択し, 各ノードが記憶している分散情報を受信する. k 個の分散情報 $u_{j_1}, u_{j_2}, \ldots, u_{j_k}$ を受信した DC は, 関数 $G : \mathcal{U}^k \to \mathcal{S}$ を用いてオリジナル情報 $\hat{s} \in \mathcal{S}$ を復元する. すなわち, k 個の分散情報 $u_{j_1}, u_{j_2}, \ldots, u_{j_k}$ から

$$G(u_{j_1}, u_{j_2}, \ldots, u_{j_k}) = \hat{s} \tag{21}$$

を計算する.

<再生成フェーズ>

分散情報 $u_i \in \mathcal{U}$ を記憶していた故障ノード N_i を修復するために, 新たにノード N_i を設置する. 新たに設置されたノードは, 故障していないノードの中から d 個のノード $\mathrm{N}_{i_1}, \mathrm{N}_{i_2}, \ldots, \mathrm{N}_{i_d}$ を任意に選択する. 次に, 選択された各ノードは記憶している分散情報と関数 $f : \mathcal{U} \times \mathcal{N} \to \mathcal{V}$ を用いて, 再生成情報 $v_{i_j,i}$, $1 \leq j \leq d$ をそれぞれ生成する. すなわち,

$$f(u_{i_j}, \mathrm{N}_i) = v_{i_j,i}, \ 1 \leq j \leq d \tag{22}$$

を計算する. これら d 個の再生成情報は新規ノードに送信され, 新規ノードは関数 $g : \mathcal{V}^d \to \mathcal{U}$ を用いて分散情報 $\hat{u}_i \in \mathcal{U}$ を生成する. すなわち,

$$g(v_{i_1,i}, \ldots, v_{i_d,i}) = \hat{u}_i \tag{23}$$

を計算する. 新規ノード N_i はこの分散情報を $u_i = \hat{u}_i$ として記憶する. □

$[n, k, d]$ DSS において, オリジナル情報 s が確率的に発生することを仮定しているため, 各フェーズで生成される情報は全て $\mathcal{S}$ 上の一様分布と関数 F, G, f,

[2] ここで, 任意の集合 $\mathcal{A}$ と自然数 m に対して, $\mathcal{A}^m$ を集合 $\mathcal{A}$ の m 個の直積集合とする.

g に依存して定まる．ここで，$u_j, \hat{u}_j, 1 \leq j \leq n$ に対する確率変数を，それぞれ $U_j, \hat{U}_j$ とし，同様に $v_{j,i}$, $1 \leq i, j \leq n$ に対する確率変数を $V_{j,i}$ とする．また，$\alpha = \log|\mathcal{U}|$, $\beta = \log|\mathcal{V}|$ とおき，α をストレージ，$\gamma = d\beta$ を修復バンドワイズと呼ぶ．

3.2　従来の再生成符号のクラスとその性質

3.2.1　$[n,k,d]$ 再生成符号

定義 1 の $[n,k,d]$ DSS は，再生成符号と呼ばれる符号クラスによって効率的に実現できる [2]．この再生成符号のクラスに対する要件は，2 章で述べたエントロピー $H(\cdot)$ 及び条件付きエントロピー $H(\cdot|\cdot)$ を用いて定義できる．

定義 2. $[n,k,d]$ DSS において，以下の条件 (C1), (C2) を満たす関数の組 (F,G,f,g) を $[n,k,d]$ 再生成符号と呼ぶ．

(C1) 任意の k 個のノード $\mathrm{N}_{j_1}, \mathrm{N}_{j_2}, \ldots, \mathrm{N}_{j_k}$ に対して，

$$H(S \mid U_{j_1}, U_{j_2}, \ldots, U_{j_k}) = 0 \tag{24}$$

が成立する．

(C2) 任意の $d+1$ 個のノード $\mathrm{N}_i, \mathrm{N}_{i_1}, \mathrm{N}_{i_2}, \ldots, \mathrm{N}_{i_d}$ に対して，

$$H(\hat{U}_i | V_{i_1,i}, V_{i_2,i}, \ldots, V_{i_d,i}) = 0$$

が成立する．　□

上記の条件 (C1) は，任意の k 個の分散情報からオリジナル情報 s が一意に定まることを意味している．一方，条件 (C2) は故障ノード以外の任意の d 個のノードが生成する再生成情報から，故障ノードの分散情報が一意に定まることを意味している．

3.2.2　分散情報の情報漏洩量を考慮した $[n,k,d,k-1]$ 再生成符号

本節では，$[n,k,d]$ 再生成符号の符号クラスの条件に分散情報の情報漏洩量に対する制約条件を追加した再生成符号の符号クラスの 1 つである $[n,k,d,k-1]$ 再生成符号 [7] を紹介する．

$[n,k,d,k-1]$ 再生成符号は $[n,k,d]$ 再生成符号のクラスに含まれる限定されたクラスとなる．

定義 3. $[n,k,d]$ DSS において，以下の条件 (C1) から (C4) を満たす関数の組 (F,G,f,g) を $[n,k,d,k-1]$ 再生成符号と呼ぶ．

(C1) 任意の k 個のノード $\mathrm{N}_{j_1}, \mathrm{N}_{j_2}, \ldots, \mathrm{N}_{j_k}$ に対して，

$$H(S \mid U_{j_1}, U_{j_2}, \ldots, U_{j_k}) = 0 \tag{25}$$

が成立する．

(C2) 任意の $d+1$ 個のノード $\mathrm{N}_i, \mathrm{N}_{i_1}, \mathrm{N}_{i_2}, \ldots, \mathrm{N}_{i_d}$ に対して，

$$H(\hat{U}_i | V_{i_1,i}, V_{i_2,i}, \ldots, V_{i_d,i}) = 0 \tag{26}$$

が成立する．

(C3) $m < k$ を満たす任意の $m+1$ 個のノード $\mathrm{N}_j, \mathrm{N}_{j_1}, \mathrm{N}_{j_2}, \ldots, \mathrm{N}_{j_m}$ に対して，

$$H(U_j \mid U_{j_1}, U_{j_2}, \ldots, U_{j_m}) = H(U_j) \tag{27}$$

が成立する．

(C4) $k \leq l < d$ を満たす任意の $l+1$ 個のノード $\mathrm{N}_i, \mathrm{N}_{i_1}, \mathrm{N}_{i_2}, \ldots, \mathrm{N}_{i_l}$ に対して，

$$H(\hat{U}_i \mid V_{i_1,i}, V_{i_2,i}, \ldots, V_{i_l,i}) = \frac{d-l}{d-k+1} H(\hat{U}_i) \tag{28}$$

が成立する．　□

上記の条件 (C1) および (C2) は，定義 2 の条件 (C1) および (C2) とそれぞれ同じ条件になっている．また，条件 (C3) はノード N_j の分散情報以外の m 個の分散情報から，ノード N_j の分散情報に対する情報が全く洩れていないことを意味している．条件 (C4) はノード N_i を修復するための l 個 $(k \leq l)$ の再生成情報から，ノード N_i の分散情報に対する情報が $\frac{l-k+1}{d-k+1} H(\hat{U}_i)$ だけ洩れていることを意味している．

注意 1. $[n,k,d]$ DSS では任意の分散情報 u_j に対して，任意のノード N_i に対する再生成情報 $v_{j,i}$ が一意に定まるので，

$$H(V_{j,i} | U_j) = 0 \tag{29}$$

が成り立つ．これと条件 (C3) より，$m < k$ を満たす任意の $m+1$ 個のノード $\mathrm{N}_i, \mathrm{N}_{i_1}, \mathrm{N}_{i_2}, \ldots, \mathrm{N}_{i_l}$ に対して，

$$H(\hat{U}_i \mid V_{i_1,i}, V_{i_2,i}, \ldots, V_{i_m,i}) = H(\hat{U}_i) \tag{30}$$

となる．よって，$[n,k,d,k-1]$ 再生成符号は式 (30) を満たす．　□

注意1と条件(C3), (C4)より，$[n,k,d,k-1]$ 再生成符号において，任意の分散情報に関する情報は，$k-1$ 個の分散情報あるいは $k-1$ 個の再生成情報からでは一切洩れていないことが保証される．また，定義2及び定義3より，$[n,k,d]$ 再生成符号は，$[n,k,d,k-1]$ 再生成符号を含む広いクラスとなることがわかる．

次節では，従来研究で示されている $[n,k,d]$ 再生成符号におけるストレージと修復バンドワイズの性質を紹介する．

3.2.3 $[n,k,d]$ 再生成符号におけるストレージと修復バンドワイズ

再生成符号においてストレージ α と修復バンドワイズ γ は小さい方が望ましいが，$[n,k,d]$ 再生成符号においては両者にトレードオフがあることが示されている [2]．したがって，$[n,k,d]$ 再生成符号の符号クラスを考えると，両者を最小にする符号は存在しない．また，$[n,k,d]$ 再生成符号における α と γ のトレードオフに対して次の2つの端点が示されている [2]．

$$(\alpha_{\min}, \gamma_{\min}(\alpha_{\min})) = \left(\frac{\log|\mathcal{S}|}{k}, \frac{d\log|\mathcal{S}|}{k(d-k+1)}\right), \tag{31}$$

$$(\alpha_{\min}(\gamma_{\min}), \gamma_{\min}) = \left(\frac{2d\log|\mathcal{S}|}{k(2d-k+1)}, \frac{2d\log|\mathcal{S}|}{k(2d-k+1)}\right). \tag{32}$$

ここで，α の最小値を $\alpha_{\min}$ とし，そのときの γ の最小値を $\gamma_{\min}(\alpha_{\min})$ とおいた．同様に γ の最小値を $\gamma_{\min}$ とし，そのときの α の最小値を $\alpha_{\min}(\gamma_{\min})$ とおいた．本稿では，式(31)を達成する $[n,k,d]$ 再生成符号，すなわちストレージが最小となるときに修復バンドワイズを最小とする $[n,k,d]$ 再生成符号を $[n,k,d]$ 最小ストレージ再生成符号 (MSR 符号: Minimum Storage Regenerating Codes) と呼ぶ．一方，式(32)を達成する $[n,k,d]$ 再生成符号，すなわち修復バンドワイズが最小となるときにストレージを最小とする $[n,k,d]$ 再生成符号を $[n,k,d]$ 最小バンドワイズ再生成符号 (MBR 符号: Minimum Bandwidth Regenerating Codes) と呼ぶ．これら2つの $[n,k,d]$ 再生成符号の構成法が，従来研究によって提案されている [3, 4, 5, 6]．Rashmi らは $[n,k,d]$ MSR 符号と $[n,k,d]$ MBR 符号の一般的な構成法として，Product-Matrix に基づく $[n,k,d]$ PM-MSR 符号 (Product-Matrix MSR 符号)，及び $[n,k,d]$ PM-MBR 符号 (Product-Matrix MBR 符号) を提案している [4]．

3.3 $[n,k,d]$ PM-MSR 符号

本節では，Rashmi らが提案した $[n,k,d]$ PM-MSR 符号の概要を紹介する [3]．

3.3.1 準備

$[n,k,d]$ PM-MSR 符号では $2k-2=d<n$ を満たす任意の正整数 n, k, d に対して，

$$\mathcal{S} = \mathbb{F}_q^{k(k-1)}, \tag{33}$$

$$\mathcal{U} = \mathbb{F}_q^{k-1}, \tag{34}$$

$$\mathcal{V} = \mathbb{F}_q, \tag{35}$$

とおく．ここで，$\mathbb{F}_q$ を位数 q の有限体とした．ただし，q は $n(k-1)\le q$ を満たす素数べきとする．

さらに，各ノード N_j, $1\le j\le n$ にそれぞれ一対一対応する d 次元ベクトル $\psi_j\in\mathbb{F}_q^d$，及び $k-1$ 次元ベクトル $\psi'_j\in\mathbb{F}_q^{k-1}$ を

$$\psi_j = \left(1, x_j, x_j^2, \ldots, x_j^{d-1}\right)^t = \left(\psi'_j, x_j^{k-1}\psi'_j\right)^t, \tag{36}$$

$$\psi'_j = \left(1, x_j, x_j^2, \ldots, x_j^{k-2}\right)^t, \quad x_j\in\mathbb{F}_q,\ 1\le j\le n \tag{37}$$

とし，

$$\mathcal{N}=\{\mathrm{N}_1,\mathrm{N}_2,\ldots,\mathrm{N}_n\}=\{\psi'_1,\psi'_2,\ldots,\psi'_n\} \tag{38}$$

とおく．ただし，x_j は0以外の値で，$j\ne j'$ を満たす任意の j, j' に対して $x_j\ne x_{j'}$ を満たすように定める．また，記号 t は転置を表す．このとき，$n\times d$ 行列

$$\Psi=\begin{bmatrix}\psi_1 & \psi_2 & \cdots & \psi_n\end{bmatrix}^t \tag{39}$$

の任意の d 行が一次独立となり，$n\times(k-1)$ 行列

$$\Psi'=\begin{bmatrix}\psi'_1 & \psi'_2 & \cdots & \psi'_n\end{bmatrix}^t \tag{40}$$

の任意の $k-1$ 行が一次独立となる．

次に，オリジナル情報によって定められるオリジナル情報行列 Ω を

$$\Omega=\begin{bmatrix}A\\B\end{bmatrix} \tag{41}$$

[3] $[n,k,d]$ PM-MSR 符号は，$2k-2\le d<n$ を満たす任意の n, k, d に対して構成できるが，本稿では $2k-2=d$ の場合のみを考える．

と定義する．ここで，A, B はそれぞれ $\mathbb{F}_q$ の値を要素とする $(k-1)\times(k-1)$ 対称行列で，

$$A = \begin{bmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,k-1} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,k-1} \\ \vdots & \vdots & \ddots & \vdots \\ a_{k-1,1} & a_{k-1,2} & \cdots & a_{k-1,k-1} \end{bmatrix},$$

$$B = \begin{bmatrix} b_{1,1} & b_{1,2} & \cdots & b_{1,k-1} \\ b_{2,1} & b_{2,2} & \cdots & b_{2,k-1} \\ \vdots & \vdots & \ddots & \vdots \\ b_{k-1,1} & b_{k-1,2} & \cdots & b_{k-1,k-1} \end{bmatrix}$$

とおく．このとき，$1 \le i,j \le k-1$ に対して $a_{i,j} = a_{j,i}$, $b_{i,j} = b_{j,i}$ が成り立つので，オリジナル情報行列 Ω における独立な要素の数は $k(k-1)$ 個となり，オリジナル情報 s と Ω を一対一対応させることができる．以降，s と Ω は等価なものであるとする．このオリジナル情報行列 Ω と式 (39) の行列 Ψ によって定まる $n\times(k-1)$ 行列 $\Psi\Omega$ を Product-Matrix と呼ぶ．

以下では，$[n,k,d]$ PM-MSR 符号の各フェーズの処理を紹介する．

3.3.2　分散情報生成フェーズ

管理者はオリジナル情報 s からオリジナル情報行列 Ω を定め，各ノード N_j, $1 \le j \le n$ の分散情報 $u_j \in \mathbb{F}_q^{k-1}$ を次のように計算する．

$$\begin{aligned} F(s) &= (u_1, u_2, \ldots, u_n) \\ &= \left(\psi_1^t\Omega, \psi_2^t\Omega, \ldots, \psi_n^t\Omega\right). \end{aligned} \tag{42}$$

3.3.3　オリジナル情報復元フェーズ

DC は任意の k 個のノード N_{j_h}, $1 \le h \le k$ を選択し，各ノードの分散情報 u_{j_h} から $k\times k$ 行列 Q を以下のように計算する．

$$\begin{aligned} Q &= \begin{bmatrix} u_{j_1}^t \\ u_{j_2}^t \\ \vdots \\ u_{j_k}^t \end{bmatrix} \begin{bmatrix} \psi'_{j_1} & \psi'_{j_2} & \cdots & \psi'_{j_k} \end{bmatrix} \\ &= \begin{bmatrix} u_{j_1}^t\psi'_{j_1} & u_{j_1}^t\psi'_{j_2} & \cdots & u_{j_1}^t\psi'_{j_k} \\ u_{j_2}^t\psi'_{j_1} & u_{j_2}^t\psi'_{j_2} & \cdots & u_{j_2}^t\psi'_{j_k} \\ \vdots & \vdots & \ddots & \vdots \\ u_{j_k}^t\psi'_{j_1} & u_{j_k}^t\psi'_{j_2} & \cdots & u_{j_k}^t\psi'_{j_k} \end{bmatrix}. \end{aligned} \tag{43}$$

ここで，

$$\Psi'_{\mathrm{rec}} = \begin{bmatrix} \psi'_{j_1} & \psi'_{j_2} & \cdots & \psi'_{j_k} \end{bmatrix}^t, \tag{44}$$

$$\Lambda_{\mathrm{rec}} = \begin{bmatrix} x_{j_1}^{k-1} & & & 0 \\ & x_{j_2}^{k-1} & & \\ & & \ddots & \\ 0 & & & x_{j_k}^{k-1} \end{bmatrix} \tag{45}$$

とおくと[4]，式 (36), (41), (42) より

$$Q = \begin{bmatrix} \Psi'_{\mathrm{rec}}A(\Psi'_{\mathrm{rec}})^t + \Lambda_{\mathrm{rec}}\Psi'_{\mathrm{rec}}B(\Psi'_{\mathrm{rec}})^t \end{bmatrix} \tag{46}$$

が成り立ち，$\Psi'_{\mathrm{rec}}A(\Psi'_{\mathrm{rec}})^t$ と $\Psi'_{\mathrm{rec}}B(\Psi'_{\mathrm{rec}})^t$ はそれぞれ $k\times k$ 対称行列となる．

次に，

$$\tilde{A} = \Psi'_{\mathrm{rec}}A(\Psi'_{\mathrm{rec}})^t, \tag{47}$$

$$\tilde{B} = \Psi'_{\mathrm{rec}}B(\Psi'_{\mathrm{rec}})^t \tag{48}$$

とし，行列 Q, $\tilde{A}$, $\tilde{B}$ の第 h 行 l 列要素をそれぞれ $q_{h,l}$, $\tilde{a}_{h,l}$, $\tilde{b}_{h,l}$ とおく $(1 \le h,l \le k)$．このとき，$1 \le h,l \le k$ を満たす任意の h, l に対して，

$$q_{h,l} = \tilde{a}_{h,l} + x_{j_h}^{k-1}\tilde{b}_{h,l}, \tag{49}$$

$$\begin{aligned} q_{l,h} &= \tilde{a}_{l,h} + x_{j_l}^{k-1}\tilde{b}_{l,h} \\ &= \tilde{a}_{h,l} + x_{j_l}^{k-1}\tilde{b}_{h,l} \end{aligned} \tag{50}$$

が成り立つ．よって，行列 Q と公開情報から行列 $\tilde{A}$, $\tilde{B}$ の対角要素を除く全ての要素 $\tilde{a}_{h,l}$, $\tilde{b}_{h,l}$, $h \ne l$ が定まる．ここで，$1 \le h \le k$ に対して，$\tilde{A}$, $\tilde{B}$ の対角要素を除いた第 h 行成分をそれぞれ

$$\tilde{A}(h) = \begin{bmatrix} \tilde{a}_{h,1} \\ \tilde{a}_{h,2} \\ \vdots \\ \tilde{a}_{h,h-1} \\ \tilde{a}_{h,h+1} \\ \vdots \\ \tilde{a}_{h,k} \end{bmatrix}^t, \tag{51}$$

$$\tilde{B}(h) = \begin{bmatrix} \tilde{b}_{h,1} \\ \tilde{b}_{h,2} \\ \vdots \\ \tilde{b}_{h,h-1} \\ \tilde{b}_{h,h+1} \\ \vdots \\ \tilde{b}_{h,k} \end{bmatrix}^t \tag{52}$$

[4] 式 (45) の右辺は，$k\times k$ の対角行列を表している．以降も対角行列を同様の表記で表す．

が成り立つ．ここで，$1 \leq h \leq k$ に対し，

$$\Psi'_{\mathrm{rec}}(h) = \begin{bmatrix} \psi'_{j_1} \\ \psi'_{j_2} \\ \vdots \\ \psi'_{j_{h-1}} \\ \psi'_{j_{h+1}} \\ \vdots \\ \psi'_{j_k} \end{bmatrix}^t \quad (53)$$

とおいた．式 (40) の Ψ' の任意の $k-1$ 行が一次独立となるので，$(k-1) \times (k-1)$ 行列 $\Psi'_{\mathrm{rec}}(h)$ にはそれぞれ逆行列 $(\Psi'_{\mathrm{rec}}(h))^{-1}$ が存在し，$\tilde{A}(h)$, $\tilde{B}(h)$ にそれぞれ $(\Psi'_{\mathrm{rec}}(h))^{-1}$ を右から掛けることで，

$$\tilde{A}(h)\left(\Psi'_{\mathrm{rec}}(h)\right)^{-1} = \left(\psi'_{j_h}\right)^t A, \quad (54)$$

$$\tilde{B}(h)\left(\Psi'_{\mathrm{rec}}(h)\right)^{-1} = \left(\psi'_{j_h}\right)^t B \quad (55)$$

が成り立ち，$\Psi'_{\mathrm{rec}}A$, $\Psi'_{\mathrm{rec}}B$ が得られる．Ψ' の性質より Ψ'_{rec} の任意の $k-1$ 行が一次独立となるので，同様に逆行列を用いることで A, B が得られ，オリジナル情報行列

$$\Omega = \begin{bmatrix} A \\ B \end{bmatrix} \quad (56)$$

が定まる．よって，オリジナル情報行列 Ω と等価なオリジナル情報 s が得られる．以上の処理が関数 G の中で行われる計算となる．

3.3.4 再生成フェーズ

ここで，

$$\Psi_{\mathrm{rep}} = \begin{bmatrix} \psi_{i_1} & \psi_{i_2} & \cdots & \psi_{i_d} \end{bmatrix}^t \quad (57)$$

とおく．新規ノード N_i に選択された d 個のノード N_{i_l}, $1 \leq l \leq d$ は，それぞれ再生成情報

$$f(u_{i_l}, \mathrm{N}_i) = u_{i_l}^t \psi'_i = v_{i_l,i}, \ 1 \leq l \leq d \quad (58)$$

を計算する．

次に，関数 g の中で行われる計算を示す．$[n,k,d]$ PM-MSR 符号では，修復後の分散情報 $\hat{u}_i$ は元の分散情報 u_i と全く同じ情報に再生成するので，

$$u_i = g(v_{i_1,i}, v_{i_2,i}, \ldots, v_{i_d,i}) \quad (59)$$

となる．新規ノード N_i が受信する d 個の再生成情報 $v_{i_l,i}$, $1 \leq l \leq d$ に対して，

$$\begin{aligned} \begin{bmatrix} v_{i_1,i} \\ v_{i_2,i} \\ \vdots \\ v_{i_d,i} \end{bmatrix} &= \begin{bmatrix} u_{i_1}^t \psi'_i \\ u_{i_2}^t \psi'_i \\ \vdots \\ u_{i_d}^t \psi'_i \end{bmatrix} \\ &= \begin{bmatrix} \psi_{i_1}^t \Omega \psi'_i \\ \psi_{i_2}^t \Omega \psi'_i \\ \vdots \\ \psi_{i_d}^t \Omega \psi'_i \end{bmatrix} \\ &= \Psi_{\mathrm{rep}} \Omega \psi'_i \end{aligned} \quad (60)$$

が成り立つ．2 つ目の等号は式 (42), 3 つ目の等号は式 (57) を用いた．また，式 (39) の Ψ の任意の d 行が一次独立となるので，Ψ_{rep} には逆行列 Ψ_{rep}^{-1} が存在する．よって，d 個の再生成情報と逆行列 Ψ_{rep}^{-1} を用いることで，

$$\begin{aligned} \Psi_{\mathrm{rep}}^{-1} \begin{bmatrix} v_{i_1,i} \\ v_{i_2,i} \\ \vdots \\ v_{i_d,i} \end{bmatrix} &= \Psi_{\mathrm{rep}}^{-1} \Psi_{\mathrm{rep}} \Omega \psi'_i \\ &= \Omega \psi'_i \\ &= \begin{bmatrix} A \\ B \end{bmatrix} \psi'_i \\ &= \begin{bmatrix} A\psi'_i \\ B\psi'_i \end{bmatrix} \end{aligned} \quad (61)$$

となり，$A\psi_i$, $B\psi_i$ が得られる．ここで，3 番目の等号は式 (41) を用いた．次に，$A\psi_i$, $B\psi_i$ を用いて，

$$\begin{aligned} (A\psi'_i)^t + x_i^{k-1} (B\psi'_i)^t &= (\psi'_i)^t A + x_i^{k-1} (\psi'_i)^t B \\ &= \psi_i^t \Omega \\ &= u_i^t \end{aligned} \quad (62)$$

を計算することで u_i を得る．ここで，1 番目の等号は行列 A, B が対称行列であること，2 番目の等号は式 (36), (41), 3 番目の等号は式 (42) を用いた．以上の処理が関数 g の中で行われる計算となる．

4 最適な $[n,k,d,k-1]$ 再生成符号

本章では，3.3 節で述べた $[n,k,d]$ PM-MSR 符号がストレージと修復バンドワイズを最小にする最適な $[n,k,d,k-1]$ 再生成符号となることを示す．具体的には，4.1 節で $[n,k,d,k-1]$ 再生成符号におけるストレージと修復バンドワイズの下界をそれぞれ導出し，4.2 節で $[n,k,d]$ PM-MSR 符号がそれらの下界を達成する $[n,k,d,k-1]$ 再生成符号となることを示す．

4.1 $[n,k,d,k-1]$ 再生成符号におけるストレージと修復バンドワイズの下界

ここで，分散情報 U_j, $1 \le j \le n$ に対して次のような仮定をおく．

仮定 1. 全ての分散情報のエントロピーが等しい．すなわち $1 \le i,j \le n$ に対して，

$$H(U_i) = H(\hat{U}_i) = H(U_j) \tag{63}$$

が成立する． □

$[n,k,d,k-1]$ 再生成符号に対するストレージの下界を以下の定理で示す．

定理 7. 仮定 1 を満たす任意の $[n,k,d,k-1]$ 再生成符号において，

$$\alpha \ge \frac{\log|\mathcal{S}|}{k} \tag{64}$$

が成立する． □

(証明) オリジナル情報の確率分布 p_S が一様分布であること，及び $[n,k,d,k-1]$ 再生成符号が満たすべき条件 (C1) より，任意の k 個のノード N_{j_h}, $1 \le h \le k$ に対して，

$$H(S) - H(S|U_{j_1}, U_{j_2}, \ldots, U_{j_k}) = \log|\mathcal{S}| \tag{65}$$

が成り立つ．また，定理 4 より，

$$\begin{aligned} & H(S) - H(S|U_{j_1}, U_{j_2}, \ldots, U_{j_k}) \\ &= H(U_{j_1}, U_{j_2}, \ldots, U_{j_k}) \\ &\quad - H(U_{j_1}, U_{j_2}, \ldots, U_{j_k}|S) \end{aligned} \tag{66}$$

となるので，式 (65), (66) より，

$$\begin{aligned} \log|\mathcal{S}| &= H(U_{j_1}, U_{j_2}, \ldots, U_{j_k}) \\ &\quad - H(U_{j_1}, U_{j_2}, \ldots, U_{j_k}|S) \\ &\le H(U_{j_1}, U_{j_2}, \ldots, U_{j_k}) \end{aligned} \tag{67}$$

が成り立つ．ここで，不等号は定理 1 を用いた．同様に任意の k 個のノードに対して，

$$\begin{aligned} & H(U_{j_1}, U_{j_2}, \ldots, U_{j_k}) \\ &= \sum_{h=1}^{k} H(U_{j_h}|U_{j_1}, U_{j_2}, \ldots, U_{j_{h-1}}) \\ &= \sum_{h=1}^{k} H(U_{j_h}) \\ &= kH(U_j) \\ &\le k\alpha \end{aligned} \tag{68}$$

が任意の $1 \le j \le n$ で成り立つ．1 番目の等号は定理 3，2 番目の等号は条件 (C3)，3 番目の等号は仮定 1，不等号は α の定義及び定理 2 を用いた．よって，式 (67)，(68) より，$1 \le j \le n$ に対して，

$$\begin{aligned} \alpha &\ge H(U_j) \\ &\ge \frac{\log|\mathcal{S}|}{k} \end{aligned} \tag{69}$$

が成り立ち，定理が証明される． □

次に，$[n,k,d,k-1]$ 再生成符号に対する修復バンドワイズの下界を以下の定理で示す．

定理 8. 仮定 1 を満たす任意の $[n,k,d,k-1]$ 再生成符号において，

$$\gamma \ge \frac{d\log|\mathcal{S}|}{k(d-k+1)} \tag{70}$$

が成立する． □

(証明) ここで，

$$\bar{V}_{j_h,j} = (V_{j_1,j}, \ldots, V_{j_{h-1},j}, V_{j_{h+1},j}, \ldots, V_{j_d,j}) \tag{71}$$

とおく．このとき，任意の $d+1$ 個のノード N_i, N_{i_1}, N_{i_2}, …, N_{i_d} に対して，

$$\begin{aligned} \gamma &\ge H(V_{j_1,j}, V_{j_2,j}, \ldots, V_{j_d,j}) \\ &= \sum_{h=1}^{d} H(V_{j_h,j}|V_{j_1,j}, \ldots, V_{j_{h-1},j}) \\ &\ge \sum_{h=1}^{d} H(V_{j_h,j}|\bar{V}_{j_h,j}) \end{aligned} \tag{72}$$

が成り立つ．1 番目の不等号は定理 2 と γ の定義，等号は定理 3，2 番目の不等号は定理 6 を用いた．また，$1 \le h \le d$ と $1 \le j \le n$ を満たす任意の h,j に対して，

$$\begin{aligned} & H(V_{j_h,j}|\bar{V}_{j_h,j}) \\ &= H(\hat{U}_j|\bar{V}_{j_h,j}) - H(\hat{U}_j|V_{j_h,j}, \bar{V}_{j_h,j}) \\ &\quad + H(V_{j_h,j}|\hat{U}_j, \bar{V}_{j_h,j}) \\ &\ge H(\hat{U}_j|\bar{V}_{j_h,j}) \\ &= \frac{1}{d-k+1} H(\hat{U}_j) \\ &= \frac{1}{d-k+1} H(U_j) \\ &\ge \frac{\log|\mathcal{S}|}{k(d-k+1)} \end{aligned} \tag{73}$$

が成り立つ．1 番目の等号は定理 4，1 番目の不等号は条件 (C2) と定理 1，2 番目の等号は条件 (C4)，3 番目の等号は仮定 1，2 番目の不等号は式 (69) を用いた．したがって，式 (72), (73) より，

$$\gamma \ge \frac{d\log|\mathcal{S}|}{k(d-k+1)} \tag{74}$$

が成立し，定理が証明される． □

4.2 $[n,k,d]$ PM-MSR 符号の最適性

3.3 節で述べた $[n,k,d]$ PM-MSR 符号が定理 7 と定理 8 の下界の両方を達成する最適な $[n,k,d,k-1]$ 再生成符号であることを以下の定理で示す.

定理 9. $[n,k,d]$ PM-MSR 符号は，ストレージと修復バンドワイズが最小の最適な $[n,k,d,k-1]$ 再生成符号となる. □

(証明) まず，$[n,k,d]$ PM-MSR 符号のストレージと修復バンドワイズが定理 7 と定理 8 の下界とそれぞれ一致することを示す．$[n,k,d]$ PM-MSR 符号で分散情報の生成に用いられるオリジナル情報行列 Ω の任意の列において，他の列のどの成分に対しても互いに独立となる成分が 1 つ以上存在するので，d 次元ベクトル ψ_j を Ω の各列にそれぞれ掛けて得られる分散情報の各成分は互いに独立となる．また，Ω において互いに独立となる成分はそれぞれ $\mathbb{F}_q$ 上の一様分布に従うので，分散情報の各成分も同様に $\mathbb{F}_q$ 上の一様分布に従う．また，$[n,k,d]$ PM-MSR 符号において，元の分散情報 u_j と修復後の分散情報 $\hat{u}_j$ は等価であるので,

$$H(\hat{U}_j) = H(U_j) \tag{75}$$

となる．以上より，

$$\begin{aligned} H(U_j) &= H(\hat{U}_j) \\ &= (k-1)\log q \\ &= \log|\mathcal{U}| \\ &= \alpha, \quad 1 \le j \le n \end{aligned} \tag{76}$$

が成立する．よって，$[n,k,d]$ PM-MSR 符号は仮定 1 を満たす．また，再生成情報の集合が $\mathcal{V} = \mathbb{F}_q$ であることから，

$$\begin{aligned} \gamma &= d\beta \\ &= d\log q \end{aligned} \tag{77}$$

が成り立つ．一方，オリジナル情報の集合が $\mathbb{F}_q^{k(k-1)}$ なので，定理 7 の下界は $(k-1)\log q$ となり α と下界が一致する．また，$d = 2k-2$ なので，定理 8 の下界は，$d\log q$ となり γ と下界が一致する.

以下では，$[n,k,d]$ PM-MSR 符号が定義 3 で定義される $[n,k,d,k-1]$ 再生成符号であることを示す．すなわち，条件 (C1), (C2), (C3), (C4) を全て満たすことを示す.

$[n,k,d]$ PM-MSR 符号は $[n,k,d]$ 再生成符号なので，条件 (C1) と (C2) を満たしている.

次に，条件 (C3) を満たすことを示す．式 (41) のオリジナル情報行列における，$(k-1)\times(k-1)$ 行列 A, B の第 1 列成分をそれぞれ $\mathbf{a}_1$, $\mathbf{b}_1$ とおき，第 2 列から第 $k-1$ 列目までの行列をそれぞれ $\overline{\mathbf{a}}_1$, $\overline{\mathbf{b}}_1$ とおく．また，$\mathbf{a}_1$, $\mathbf{b}_1$, $\overline{\mathbf{a}}_1$, $\overline{\mathbf{b}}_1$ に対応する確率変数をそれぞれ $\mathbf{A}_1$, $\mathbf{B}_1$, $\overline{\mathbf{A}}_1$, $\overline{\mathbf{B}}_1$ とする．このとき，定理 4 より，任意の k 個のノード $\mathrm{N}_j, \mathrm{N}_{j_1}, \mathrm{N}_{j_2}, \ldots, \mathrm{N}_{j_{k-1}}$ に対して,

$$\begin{aligned} &H(U_j \mid U_{j_1}, U_{j_2}, \ldots, U_{j_{k-1}}) \\ &\quad = H(\mathbf{A}_1, \overline{\mathbf{A}}_1, \mathbf{B}_1, \overline{\mathbf{B}}_1 \mid U_{j_1}, \ldots, U_{j_{k-1}}) \\ &\qquad -H(\mathbf{A}_1, \overline{\mathbf{A}}_1, \mathbf{B}_1, \overline{\mathbf{B}}_1 \mid U_{j_1}, \ldots, U_{j_{k-1}}, U_j) \\ &\qquad +H(U_j \mid U_{j_1}, \ldots, U_{j_{k-1}}, \mathbf{A}_1, \overline{\mathbf{A}}_1, \mathbf{B}_1, \overline{\mathbf{B}}_1) \end{aligned}$$

が成り立つ．$[n,k,d]$ PM-MSR 符号は任意の k 個の分散情報からオリジナル情報行列を求めることができるので,

$$H(\mathbf{A}_1, \overline{\mathbf{A}}_1, \mathbf{B}_1, \overline{\mathbf{B}}_1 \mid U_{j_1}, \ldots, U_{j_{k-1}}, U_j) = 0 \tag{78}$$

となる．また，オリジナル情報行列から分散情報が一意に定まるので,

$$H(U_j \mid U_{j_1}, \ldots, U_{j_{k-1}}, \mathbf{A}_1, \overline{\mathbf{A}}_1, \mathbf{B}_1, \overline{\mathbf{B}}_1) = 0 \tag{79}$$

が成り立つ．したがって,

$$\begin{aligned} &H(U_j \mid U_{j_1}, U_{j_2}, \ldots, U_{j_{k-1}}) \\ &\quad = H(\mathbf{A}_1, \overline{\mathbf{A}}_1, \mathbf{B}_1, \overline{\mathbf{B}}_1 \mid U_{j_1}, \ldots, U_{j_{k-1}}) \end{aligned} \tag{80}$$

を得る．式 (80) の右辺は定理 3 より，

$$\begin{aligned} &H(\mathbf{A}_1, \overline{\mathbf{A}}_1, \mathbf{B}_1, \overline{\mathbf{B}}_1 \mid U_{j_1}, U_{j_2}, \ldots, U_{j_{k-1}}) \\ &\quad = H(\mathbf{A}_1, \mathbf{B}_1 \mid U_{j_1}, \ldots, U_{j_{k-1}}) \\ &\qquad +H(\overline{\mathbf{A}}_1, \overline{\mathbf{B}}_1 \mid U_{j_1}, \ldots, U_{j_{k-1}}, \mathbf{A}_1, \mathbf{B}_1) \end{aligned} \tag{81}$$

となる．ここで，$u_{j_1}, u_{j_2}, \ldots, u_{j_{k-1}}, \mathbf{a}_1, \mathbf{b}_1$ を既知の情報として，既知の情報から $\overline{\mathbf{a}}_1, \overline{\mathbf{b}}_1$ を求めることを考える．$[n,k,d]$ PM-MSR 符号における分散情報の生成方法より，既知の情報から

$$\begin{aligned} &\begin{bmatrix} u_{j_1} \\ u_{j_2} \\ \vdots \\ u_{j_{k-1}} \end{bmatrix} - \begin{bmatrix} \Psi'_{[j]}\mathbf{a}_1 + \Lambda_{[j]}\Psi'_{[j]}\mathbf{b}_1 \end{bmatrix} \\ &\quad = \begin{bmatrix} \Psi'_{[j]}A + \Lambda_{[j]}\Psi'_{[j]}B \end{bmatrix} \\ &\qquad - \begin{bmatrix} \Psi'_{[j]}\mathbf{a}_1 + \Lambda_{[j]}\Psi'_{[j]}\mathbf{b}_1 \end{bmatrix} \\ &\quad = \begin{bmatrix} \Psi'_{[j]}\overline{\mathbf{a}}_1 + \Lambda_{[j]}\Psi'_{[j]}\overline{\mathbf{b}}_1 \end{bmatrix} \end{aligned} \tag{82}$$

が計算できる．ここで，

$$\Psi'_{[j]} = \begin{bmatrix} \psi'_{j_1} & \psi'_{j_2} & \cdots & \psi'_{j_{k-1}} \end{bmatrix}^t, \quad (83)$$

$$\Lambda_{[j]} = \begin{bmatrix} x_{j_1}^{k-1} & & & 0 \\ & x_{j_2}^{k-1} & & \\ & & \ddots & \\ 0 & & & x_{j_{k-1}}^{k-1} \end{bmatrix} \quad (84)$$

とおいた．また，行列 A, B が対称行列なので，

$$a_{i,j} = a_{j,i},\ b_{i,j} = b_{j,i},\quad 1 \le i, j \le k-1 \quad (85)$$

が成り立ち，既知の情報である $\mathbf{a}_1, \mathbf{b}_1$ から行列 $\overline{\mathbf{a}}_1, \overline{\mathbf{b}}_1$ の第 1 行成分が一意に定まる．すなわち，既知の情報から $a_{1,2}, a_{1,3}, \ldots, a_{1,k-1}$, $b_{1,2}, b_{1,3}, \ldots, b_{1,k-1}$ が一意に定まる．よって，既知の情報から

$$\begin{aligned} &\Psi'_{[j]}\overline{\mathbf{a}}_1 + \Lambda_{[j]}\Psi'_{[j]}\overline{\mathbf{b}}_1 - \Delta(\mathbf{a}_1) - \Lambda_{[j]}\Delta(\mathbf{b}_1) \\ &\quad = \Psi''_{[j]}\widetilde{\mathbf{a}}_1 + \Lambda_{[j]}\Psi''_{[j]}\widetilde{\mathbf{b}}_1 \end{aligned} \quad (86)$$

が計算できる．ここで，$\Delta(\mathbf{a}_1)$, $\Delta(\mathbf{b}_1)$, $\Psi''_{[j]}$ を，それぞれ $(k-1)\times(k-2)$ 行列

$$\Delta(\mathbf{a}_1) = \begin{bmatrix} a_{1,2} & a_{1,3} & \cdots & a_{1,k-1} \\ a_{1,2} & a_{1,3} & \cdots & a_{1,k-1} \\ \vdots & \vdots & \ddots & \vdots \\ a_{1,2} & a_{1,3} & \cdots & a_{1,k-1} \end{bmatrix}, \quad (87)$$

$$\Delta(\mathbf{b}_1) = \begin{bmatrix} b_{1,2} & b_{1,3} & \cdots & b_{1,k-1} \\ b_{1,2} & b_{1,3} & \cdots & b_{1,k-1} \\ \vdots & \vdots & \ddots & \vdots \\ b_{1,2} & b_{1,3} & \cdots & b_{1,k-1} \end{bmatrix}, \quad (88)$$

$$\Psi''_{[j]} = \begin{bmatrix} x_{j_1} & x_{j_1}^2 & \cdots & x_{j_1}^{k-2} \\ x_{j_2} & x_{j_2}^2 & \cdots & x_{j_2}^{k-2} \\ \vdots & \vdots & \ddots & \vdots \\ x_{j_{k-1}} & x_{j_{k-1}}^2 & \cdots & x_{j_{k-1}}^{k-2} \end{bmatrix} \quad (89)$$

とし，$\widetilde{\mathbf{a}}_1, \widetilde{\mathbf{b}}_1$ を，それぞれ $(k-2)\times(k-2)$ 対称行列

$$\widetilde{\mathbf{a}}_1 = \begin{bmatrix} a_{2,2} & a_{2,3} & \cdots & a_{2,k-1} \\ a_{3,2} & a_{3,3} & \cdots & a_{3,k-1} \\ \vdots & \vdots & \ddots & \vdots \\ a_{k-1,2} & a_{k-1,3} & \cdots & a_{k-1,k-1} \end{bmatrix} \quad (90)$$

$$\widetilde{\mathbf{b}}_1 = \begin{bmatrix} b_{2,2} & b_{2,3} & \cdots & b_{2,k-1} \\ b_{3,2} & b_{3,3} & \cdots & b_{3,k-1} \\ \vdots & \vdots & \ddots & \vdots \\ b_{k-1,2} & b_{k-1,3} & \cdots & b_{k-1,k-1} \end{bmatrix} \quad (91)$$

とおいた．式 (86) の右辺に右から $(k-2)\times(k-1)$ 行列 $(\Psi''_{[j]})^t$ を掛けることで，$(k-1)\times(k-1)$ 行列

$$Q' = \Psi''_{[j]}\widetilde{\mathbf{a}}_1(\Psi''_{[j]})^t + \Lambda_{[j]}\Psi''_{[j]}\widetilde{\mathbf{b}}_1(\Psi''_{[j]})^t \quad (92)$$

を得る．また，$(k-2)\times(k-1)$ 行列 $(\Psi''_{[j]})^t$ の任意の 1 列を除いた $k-2$ 列は一次独立となるので，それらを並べた $(k-2)\times(k-2)$ 行列には逆行列が存在する．よって，3.3.3 節の行列 Q から行列 A, B を求める計算と同様に，$(k-1)\times(k-1)$ 行列 Q' から行列 $\widetilde{\mathbf{a}}_1, \widetilde{\mathbf{b}}_1$ を一意に求めることができる．以上の議論より，既知の情報 $u_{j_1}, u_{j_2}, \ldots, u_{j_{k-1}}, \mathbf{a}_1, \mathbf{b}_1$ から $\overline{\mathbf{a}}_1, \overline{\mathbf{b}}_1$ を一意に求めることができ，

$$H(\overline{\mathbf{A}}_1, \overline{\mathbf{B}}_1 \mid U_{j_1}, \ldots, U_{j_{k-1}}, \mathbf{A}_1, \mathbf{B}_1) = 0 \quad (93)$$

が成立する．よって，式 (80), (81), (93) より，

$$\begin{aligned} &H(U_j \mid U_{j_1}, U_{j_2}, \ldots, U_{j_{k-1}}) \\ &\quad = H(\mathbf{A}_1, \mathbf{B}_1 \mid U_{j_1}, \ldots, U_{j_{k-1}}) \end{aligned} \quad (94)$$

を得る．また，定理 6 より，

$$H(U_j \mid U_{j_1}, U_{j_2}, \ldots, U_{j_{k-1}}) \le H(U_j) \quad (95)$$

が成り立つので，式 (94), (95) より，

$$\begin{aligned} &H(\mathbf{A}_1, \mathbf{B}_1 \mid U_{j_1}, U_{j_2}, \ldots, U_{j_{k-1}}) \\ &\quad = H(U_j \mid U_{j_1}, \ldots, U_{j_{k-1}}) \\ &\quad \le H(U_j) \end{aligned} \quad (96)$$

を得る．一方，$\mathbf{a}_1, \mathbf{b}_1$ の各成分は互いに独立に $\mathbb{F}_q$ 上の一様分布に従って生成されること，及び分散情報がオリジナル情報から一意に定まることより，

$$H(\mathbf{A}_1, \mathbf{B}_1) = 2(k-1)\log q, \quad (97)$$

$$H(U_{j_1}, \ldots, U_{j_{k-1}} \mid \overline{\mathbf{A}}_1, \overline{\mathbf{B}}_1, \mathbf{A}_1, \mathbf{B}_1) = 0 \quad (98)$$

がそれぞれ成り立つ．よって，式 (96) の左辺に対して，

$$\begin{aligned} &H(\mathbf{A}_1, \mathbf{B}_1 \mid U_{j_1}, U_{j_2}, \ldots, U_{j_{k-1}}) \\ &\quad = H(\mathbf{A}_1, \mathbf{B}_1) - H(U_{j_1}, U_{j_2}, \ldots, U_{j_{k-1}}) \\ &\qquad + H(U_{j_1}, \ldots, U_{j_{k-1}} \mid \mathbf{A}_1, \mathbf{B}_1) \\ &\quad = 2(k-1)\log q - H(U_{j_1}, U_{j_2}, \ldots, U_{j_{k-1}}) \\ &\qquad + H(U_{j_1}, \ldots, U_{j_{k-1}} \mid \mathbf{A}_1, \mathbf{B}_1) \\ &\qquad - H(U_{j_1}, \ldots, U_{j_{k-1}} \mid \overline{\mathbf{A}}_1, \overline{\mathbf{B}}_1, \mathbf{A}_1, \mathbf{B}_1) \\ &\quad = 2(k-1)\log q - H(U_{j_1}, U_{j_2}, \ldots, U_{j_{k-1}}) \\ &\qquad + H(\overline{\mathbf{A}}_1, \overline{\mathbf{B}}_1 \mid \mathbf{A}_1, \mathbf{B}_1) \\ &\qquad - H(\overline{\mathbf{A}}_1, \overline{\mathbf{B}}_1 \mid \mathbf{A}_1, \mathbf{B}_1, U_{j_1}, \ldots, U_{j_{k-1}}) \\ &\quad = 2(k-1)\log q - H(U_{j_1}, U_{j_2}, \ldots, U_{j_{k-1}}) \\ &\qquad + H(\overline{\mathbf{A}}_1, \overline{\mathbf{B}}_1 \mid \mathbf{A}_1, \mathbf{B}_1) \\ &\quad \ge 2(k-1)\log q - (k-1)^2 \log q \\ &\qquad + H(\overline{\mathbf{A}}_1, \overline{\mathbf{B}}_1 \mid \mathbf{A}_1, \mathbf{B}_1) \end{aligned} \quad (99)$$

が成立する．1番目と3番目の等号は定理4，2番目の等号は式(97), (98)，4番目の等号は式(93)，不等号は定理2を用いた．オリジナル情報行列の定義より，行列 A, B の第1列成分 $\mathbf{a}_1, \mathbf{b}_1$ は，行列 $\overline{\mathbf{a}}_1, \overline{\mathbf{b}}_1$ の第1行成分を除く成分とそれぞれ互いに独立に生成される．すなわち，

$$H(\overline{\mathbf{A}}_1, \overline{\mathbf{B}}_1 \mid \mathbf{A}_1, \mathbf{B}_1) = (k-2)(k-1)\log q \quad (100)$$

が成り立つので，式(99), (100)より，

$$\begin{aligned} H(\mathbf{A}_1, \mathbf{B}_1 \mid U_{j_1}, U_{j_2}, \ldots, U_{j_{k-1}}) &\geq 2(k-1)\log q - (k-1)^2 \log q \\ &\quad +(k-2)(k-1)\log q \\ &= (k-1)\log q \\ &= H(U_j) \end{aligned} \quad (101)$$

を得る．最後の等号は式(76)を用いた．したがって，式(96), (101)より，

$$H(U_j \mid U_{j_1}, U_{j_2}, \ldots, U_{j_{k-1}}) = H(U_j) \quad (102)$$

が成立する．また，定理6と式(102)より，

$$\begin{aligned} H(U_j) &\geq H(U_j \mid U_{j_1}, U_{j_2}, \ldots, U_{j_m}) \\ &\geq H(U_j \mid U_{j_1}, U_{j_2}, \ldots, U_{j_{k-1}}) \\ &= H(U_j),\ m < k \end{aligned} \quad (103)$$

が成り立つので，

$$H(U_j \mid U_{j_1}, U_{j_2}, \ldots, U_{j_m}) = H(U_j),\ \ m < k \quad (104)$$

を得る．よって条件(C3)を満たすことが証明された．

最後に，条件(C4)を満たすことを示す．$[n, k, d]$ PM-MSR符号において，元の分散情報 u_j と修復後の分散情報 $\hat{u}_j$ は等価であるので，一般性を失うことなく $U_j = \hat{U}_j$ と仮定できる．よって，$k \leq l < d$ を満たす任意の $l+1$ 個のノード N_i, N_{i_1}, N_{i_2}, …, N_{i_l} に対して，

$$\begin{aligned} &H(U_i \mid V_{i_1,i}, V_{i_2,i}, \ldots, V_{i_l,i}) \\ &\quad = \frac{d-l}{d-k+1} H(U_i) \end{aligned} \quad (105)$$

を示せばよい．定理4より，任意の $d+1$ 個のノード N_i, N_{i_1}, N_{i_2}, …, N_{i_d} に対して，

$$\begin{aligned} &H(U_i \mid V_{i_1,i}, V_{i_2,i}, \ldots, V_{i_l,i}) \\ &\quad = H(V_{i_{l+1},i}, \ldots, V_{i_d,i} \mid V_{i_1,i}, \ldots, V_{i_l,i}) \\ &\qquad -H(V_{i_{l+1},i}, \ldots, V_{i_d,i} \mid V_{i_1,i}, \ldots, V_{i_l,i}, U_i) \\ &\qquad +H(U_i \mid V_{i_1,i}, \ldots, V_{i_d,i}),\ \ k \leq l < d \end{aligned} \quad (106)$$

が成り立つ．また，$[n, k, d]$ PM-MSR符号が条件(C2)を満たしていることから，

$$H(U_i \mid V_{i_1,i}, V_{i_2,i}, \ldots, V_{i_d,i}) = 0 \quad (107)$$

が成り立つ．ここで，$k \leq l < d$ を満たす任意の l に対して，

$$\mathbf{z}_{[l]} = (z_1, z_2, \ldots, z_l)^t \in \mathbb{F}_q^l, \quad (108)$$

$$\overline{\mathbf{z}}_{[l]} = (z_{l+1}, z_{l+2}, \ldots, z_d)^t \in \mathbb{F}_q^{d-l}, \quad (109)$$

$$\begin{bmatrix} \mathbf{z}_{[l]} \\ \overline{\mathbf{z}}_{[l]} \end{bmatrix} = \Omega \psi_i' \in \mathbb{F}_q^d \quad (110)$$

とおき，$\mathbf{z}_{[l]}, \overline{\mathbf{z}}_{[l]}$ に対応する確率変数を，それぞれ $\mathbf{Z}_{[l]}$, $\overline{\mathbf{Z}}_{[l]}$ とする．このとき，3.3.4節の再生成フェーズの計算より，l 個の再生成情報 $v_{i_1,i}, \ldots, v_{i_l,i}$ に対して，

$$\begin{aligned} \begin{bmatrix} v_{i_1,i} \\ v_{i_2,i} \\ \vdots \\ v_{i_l,i} \end{bmatrix} &= \begin{bmatrix} \psi_{i_1}^t \\ \psi_{i_2}^t \\ \vdots \\ \psi_{i_l}^t \end{bmatrix} \begin{bmatrix} \mathbf{z}_{[l]} \\ \overline{\mathbf{z}}_{[l]} \end{bmatrix} \\ &= \begin{bmatrix} \psi_{i_1}^t \\ \psi_{i_2}^t \\ \vdots \\ \psi_{i_l}^t \end{bmatrix} \begin{bmatrix} z_1 \\ z_2 \\ \vdots \\ z_d \end{bmatrix} \end{aligned} \quad (111)$$

が成り立つので，$\mathbf{z}_{[l]}, \overline{\mathbf{z}}_{[l]}$ から任意の再生成情報が一意に定まる．すなわち，

$$H(V_{i_{l+1},i}, \ldots, V_{i_d,i} \mid \mathbf{Z}_{[l]}, \overline{\mathbf{Z}}_{[l]}) = 0 \quad (112)$$

が成り立つ．一方，3.3.4節の再生成フェーズにおける分散情報 u_i の生成過程で任意の d 個の再生成情報から $\mathbf{z}_{[l]}, \overline{\mathbf{z}}_{[l]}$ が一意に定まる．すなわち，

$$H(\mathbf{Z}_{[l]}, \overline{\mathbf{Z}}_{[l]} \mid V_{i_1,i}, \ldots, V_{i_d,i}) = 0 \quad (113)$$

が成り立つので，定理1と定理6より

$$H(\mathbf{Z}_{[l]}, \overline{\mathbf{Z}}_{[l]} \mid V_{i_1,i}, \ldots, V_{i_d,i}, U_i) = 0 \quad (114)$$

も同様に成り立つ．したがって，

$$\begin{aligned} &H(V_{i_{l+1},i}, \ldots, V_{i_d,i} \mid V_{i_1,i}, \ldots, V_{i_l,i}, U_i) \\ &\quad = H(\mathbf{Z}_{[l]}, \overline{\mathbf{Z}}_{[l]} \mid V_{i_1,i}, \ldots, V_{i_l,i}, U_i) \\ &\qquad -H(\mathbf{Z}_{[l]}, \overline{\mathbf{Z}}_{[l]} \mid V_{i_1,i}, \ldots, V_{i_d,i}, U_i) \\ &\qquad +H(V_{i_{l+1},i}, \ldots, V_{i_d,i} \mid V_{i_1,i}, \ldots, V_{i_l,i}, \\ &\qquad\qquad U_i, \mathbf{Z}_{[l]}, \overline{\mathbf{Z}}_{[l]}) \\ &\quad \leq H(\mathbf{Z}_{[l]}, \overline{\mathbf{Z}}_{[l]} \mid V_{i_1,i}, \ldots, V_{i_l,i}, U_i) \\ &\qquad +H(V_{i_{l+1},i}, \ldots, V_{i_d,i} \mid \mathbf{Z}_{[l]}, \overline{\mathbf{Z}}_{[l]}) \\ &\quad = H(\mathbf{Z}_{[l]}, \overline{\mathbf{Z}}_{[l]} \mid V_{i_1,i}, \ldots, V_{i_l,i}, U_i) \\ &\quad \leq H(\mathbf{Z}_{[l]}, \overline{\mathbf{Z}}_{[l]} \mid V_{i_1,i}, \ldots, V_{i_{k-1},i}, U_i) \end{aligned} \quad (115)$$

が成立する．1番目の等号は定理4，1番目の不等号は式(114)と定理6，2番目の等号は式(112)，2番目の不等号は$k \leq l$であることと定理6を用いた．ここで，$k-1$個の再生成情報$v_{i_1,i}, v_{i_2,i}, \ldots, v_{i_{k-1},i}$と分散情報$u_i$を既知の情報として，既知の情報から$\mathbf{z}_{[l]}$，$\overline{\mathbf{z}}_{[l]}$を求めることを考える．式(62)，(110)より，分散情報u_iに対して，

$$\begin{aligned} u_i^t &= (A\psi_i')^t + x_i^{k-1}(B\psi_i')^t \\ &= \begin{bmatrix} z_1 & z_2 & \cdots & z_{k-1} \end{bmatrix} \\ &\quad + x_i^{k-1}\begin{bmatrix} z_k & z_{k+1} & \cdots & z_d \end{bmatrix} \end{aligned} \quad (116)$$

が成り立つ．よって，式(111)，(116)より，

$$\begin{bmatrix} v_{i_1,i} \\ v_{i_2,i} \\ \vdots \\ v_{i_{k-1},i} \\ u_i \end{bmatrix} = \begin{bmatrix} \Psi_{[i]}' & \Lambda_{[i]}\Psi_{[i]}' \\ I & x_i^{k-1}I \end{bmatrix} \begin{bmatrix} z_1 \\ z_2 \\ \vdots \\ z_d \end{bmatrix} \quad (117)$$

を得る．ここで，Iを$(k-1)\times(k-1)$単位行列とし，

$$\Psi_{[i]}' = \begin{bmatrix} \psi_{i_1} & \psi_{i_2} & \cdots & \psi_{i_{k-1}} \end{bmatrix}^t, \quad (118)$$

$$\Lambda_{[i]} = \begin{bmatrix} x_{i_1}^{k-1} & & & 0 \\ & x_{i_2}^{k-1} & & \\ & & \ddots & \\ 0 & & & x_{i_{k-1}}^{k-1} \end{bmatrix} \quad (119)$$

とおいた．式(117)右辺の$d\times d$行列

$$\begin{bmatrix} \Psi_{[i]}' & \Lambda_{[i]}\Psi_{[i]}' \\ I & x_i^{k-1}I \end{bmatrix}$$

の行列式は，

$$\begin{aligned} &\begin{vmatrix} \Psi_{[i]}' & \Lambda_{[i]}\Psi_{[i]}' \\ I & x_i^{k-1}I \end{vmatrix} \\ &= (-1)^{(k-1)(k+1)} \prod_{j=1}^{k-1}(x_{ij}^{k-1} - x_i^{k-1}) \\ &\quad \times \prod_{1\leq h<h'\leq k-1}(x_{i_{h'}} - x_{i_h}) \end{aligned} \quad (120)$$

となり，

$$\begin{aligned} x_{i_h}^{k-1} &\neq x_i^{k-1}, \\ x_{i_h}^{k-1} &\neq x_{i_{h'}}^{k-1}, \quad 1 \leq h < h' \leq k-1 \end{aligned} \quad (121)$$

であることから，

$$\begin{vmatrix} \Psi_{[i]}' & \Lambda_{[i]}\Psi_{[i]}' \\ I & x_i^{k-1}I \end{vmatrix} \neq 0 \quad (122)$$

が成り立つ．よって，$d\times d$行列

$$\begin{bmatrix} \Psi_{[i]}' & \Lambda_{[i]}\Psi_{[i]}' \\ I & x_i^{k-1}I \end{bmatrix}$$

には逆行列が存在する．この逆行列を式(117)左辺の左から掛けることで，$\mathbf{z}_{[l]}$, $\overline{\mathbf{z}}_{[l]}$が一意に定まるので，

$$H(\mathbf{Z}_{[l]}, \overline{\mathbf{Z}}_{[l]} \,|\, V_{i_1,i}, \ldots, V_{i_{k-1},i}, U_i) = 0 \quad (123)$$

が成り立つ．したがって，定理1，及び式(115)，(123)より，

$$H(V_{i_{l+1},i}, \ldots, V_{i_d,i} \,|\, V_{i_1,i}, \ldots, V_{i_l,i}, U_i) = 0 \quad (124)$$

を得る．また，定理2，定理3，定理6より，

$$\begin{aligned} &H(V_{i_{l+1},i}, \ldots, V_{i_d,i} \mid V_{i_1,i}, \ldots, V_{i_l,i}) \\ &\quad = \sum_{h=l+1}^{d} H(V_{i_h,i} \mid V_{i_1,i}, \ldots, V_{i_{h-1},i}) \\ &\quad \leq \sum_{h=l+1}^{d} H(V_{i_h,i}) \\ &\quad \leq (d-l)\log q \end{aligned} \quad (125)$$

が成り立つ．よって，式(106)，(107)，(124)，(125)より，

$$\begin{aligned} &(d-l)\log q \\ &\quad \geq H(U_i \mid V_{i_1,i}, V_{i_2,i}, \ldots, V_{i_l,i}) \\ &\quad = H(V_{i_{l+1},i}, \ldots, V_{i_d,i} \mid V_{i_1,i}, \ldots, V_{i_l,i}) \end{aligned} \quad (126)$$

となり，式(115)と同様に考えることで，

$$\begin{aligned} &H(V_{i_{l+1},i}, \ldots, V_{i_d,i} \mid V_{i_1,i}, \ldots, V_{i_l,i}) \\ &\quad = H(\mathbf{Z}_{[l]}, \overline{\mathbf{Z}}_{[l]} \mid V_{i_1,i}, \ldots, V_{i_l,i}) \\ &\qquad -H(\mathbf{Z}_{[l]}, \overline{\mathbf{Z}}_{[l]} \mid V_{i_1,i}, \ldots, V_{i_d,i}) \\ &\qquad +H(V_{i_{l+1},i}, \ldots, V_{i_d,i} \mid V_{i_1,i}, \ldots, V_{i_l,i}, \\ &\qquad\qquad \mathbf{Z}_{[l]}, \overline{\mathbf{Z}}_{[l]}) \\ &\quad = H(\mathbf{Z}_{[l]}, \overline{\mathbf{Z}}_{[l]} \mid V_{i_1,i}, \ldots, V_{i_l,i}) \\ &\quad = H(\overline{\mathbf{Z}}_{[l]} \mid V_{i_1,i}, \ldots, V_{i_l,i}) \\ &\qquad +H(\mathbf{Z}_{[l]} \mid V_{i_1,i}, \ldots, V_{i_l,i}, \overline{\mathbf{Z}}_{[l]}) \end{aligned} \quad (127)$$

を得る．1番目の等号は定理4，2番目の等号は式(112)，(113)，最後の等号は定理3を用いた．ここで，$v_{i_1,i}$, …, $v_{i_l,i}$, $\overline{\mathbf{z}}_{[l]}$を既知の情報として，既知の情報から$\mathbf{z}_{[l]}$を求めることを考える．$[n,k,d]$ PM-MSR符号にお

ける再生成情報の生成方法より，

$$\begin{bmatrix} v_{i_1,i} \\ v_{i_2,i} \\ \vdots \\ v_{i_l,i} \end{bmatrix} - \begin{bmatrix} x_{i_1}^l & x_{i_1}^{l+1} & \cdots & x_{i_1}^{d-1} \\ x_{i_2}^l & x_{i_2}^{l+1} & \cdots & x_{i_2}^{d-1} \\ \vdots & \vdots & \ddots & \vdots \\ x_{i_l}^l & x_{i_l}^{l+1} & \cdots & x_{i_l}^{d-1} \end{bmatrix} \begin{bmatrix} z_{l+1} \\ z_{l+2} \\ \vdots \\ z_d \end{bmatrix}$$
$$= \begin{bmatrix} 1 & x_{i_1} & x_{i_1}^2 & \cdots & x_{i_1}^{l-1} \\ 1 & x_{i_2} & x_{i_2}^2 & \cdots & x_{i_2}^{l-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_{i_l} & x_{i_l}^2 & \cdots & x_{i_l}^{l-1} \end{bmatrix} \begin{bmatrix} z_1 \\ z_2 \\ \vdots \\ z_l \end{bmatrix} \tag{128}$$

が成り立ち，式 (128) の左辺は既知の情報から計算できる．また，式 (128) 右辺の $l \times l$ 行列

$$\begin{bmatrix} 1 & x_{i_1} & x_{i_1}^2 & \cdots & x_{i_1}^{l-1} \\ 1 & x_{i_2} & x_{i_2}^2 & \cdots & x_{i_2}^{l-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_{i_l} & x_{i_l}^2 & \cdots & x_{i_l}^{l-1} \end{bmatrix}$$

の行列式は Vandermonde の行列式となり，$1 \le h < h' \le l$ に対して，$x_{i_h} \neq x_{i_{h'}}$ なので，

$$\begin{aligned} \begin{vmatrix} 1 & x_{i_1} & x_{i_1}^2 & \cdots & x_{i_1}^{l-1} \\ 1 & x_{i_2} & x_{i_2}^2 & \cdots & x_{i_2}^{l-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_{i_l} & x_{i_l}^2 & \cdots & x_{i_l}^{l-1} \end{vmatrix} &= \prod_{1 \le h < h' \le l} (x_{i_{h'}} - x_{i_h}) \\ &\neq 0 \end{aligned} \tag{129}$$

が成り立つ．よって，この $l \times l$ 行列には逆行列が存在する．この逆行列を式 (128) の左辺に左から掛けることで，既知の情報から $\mathbf{z}_{[l]}$ が一意に定まる．すなわち，

$$H(\mathbf{Z}_{[l]} \mid V_{i_1,i}, \ldots, V_{i_l,i}, \overline{\mathbf{Z}}_{[l]}) = 0 \tag{130}$$

が成り立つので，式 (126)，(127)，(130) より，

$$\begin{aligned} (d-l)\log q &\ge H(U_i \mid V_{i_1,i}, V_{i_2,i}, \ldots, V_{i_l,i}) \\ &= H(\overline{\mathbf{Z}}_{[l]} \mid V_{i_1,i}, \ldots, V_{i_l,i}) \end{aligned} \tag{131}$$

を得る．一方，$(\mathbf{z}_{[l]}, \overline{\mathbf{z}}_{[l]})$ の各成分は，相異なるオリジナル情報の成分をそれぞれ含んでいるので互いに独立となり，

$$H(\mathbf{Z}_{[l]}) = l \log q, \tag{132}$$
$$H(\overline{\mathbf{Z}}_{[l]}) = (d-l)\log q, \tag{133}$$
$$H(\mathbf{Z}_{[l]} \mid \overline{\mathbf{Z}}_{[l]}) = H(\mathbf{Z}_{[l]}) \tag{134}$$

が成り立つ．また，$\mathbf{z}_{[l]}, \overline{\mathbf{z}}_{[l]}$ から任意の再生成情報が一意に定まるので，

$$H(V_{i_1,i}, \ldots, V_{i_l,i} \mid \mathbf{Z}_{[l]}, \overline{\mathbf{Z}}_{[l]}) = 0 \tag{135}$$

が成り立つ．したがって，

$$\begin{aligned} &H(\overline{\mathbf{Z}}_{[l]} \mid V_{i_1,i}, \ldots, V_{i_l,i}) \\ &= H(\overline{\mathbf{Z}}_{[l]}) - H(V_{i_1,i}, \ldots, V_{i_l,i}) \\ &\quad + H(V_{i_1,i}, \ldots, V_{i_l,i} \mid \overline{\mathbf{Z}}_{[l]}) \\ &= (d-l)\log q - H(V_{i_1,i}, \ldots, V_{i_l,i}) \\ &\quad + H(V_{i_1,i}, \ldots, V_{i_l,i} \mid \overline{\mathbf{Z}}_{[l]}) \\ &\quad - H(V_{i_1,i}, \ldots, V_{i_l,i} \mid \mathbf{Z}_{[l]}, \overline{\mathbf{Z}}_{[l]}) \\ &= (d-l)\log q - H(V_{i_1,i}, \ldots, V_{i_l,i}) \\ &\quad + H(\mathbf{Z}_{[l]} \mid \overline{\mathbf{Z}}_{[l]}) \\ &\quad - H(\mathbf{Z}_{[l]} \mid V_{i_1,i}, \ldots, V_{i_l,i}, \overline{\mathbf{Z}}_{[l]}) \\ &= (d-l)\log q - H(V_{i_1,i}, \ldots, V_{i_l,i}) \\ &\quad + H(\mathbf{Z}_{[l]} \mid \overline{\mathbf{Z}}_{[l]}) \\ &= (d-l)\log q - H(V_{i_1,i}, \ldots, V_{i_l,i}) + l \log q \\ &\ge (d-l)\log q - l \log q + l \log q \\ &= (d-l)\log q \end{aligned} \tag{136}$$

が成立する．1 番目と 3 番目の等号は定理 4，2 番目の等号は式 (132)，(135)，4 番目の等号は式 (130)，5 番目の等号は式 (132)，(134)，不等号は定理 2 を用いた．よって，$d = 2k-2$ であること，及び式 (131)，(136) より，$k \le l < d$ に対して，

$$\begin{aligned} &H(U_i \mid V_{i_1,i}, V_{i_2,i}, \ldots, V_{i_l,i}) \\ &= (d-l)\log q \\ &= \frac{(d-l)(k-1)}{2(k-1)-(k-1)} \log q \\ &= \frac{d-l}{d-k+1} H(U_i) \end{aligned} \tag{137}$$

が成立する．よって条件 (C4) を満たすことが証明された． □

5 まとめ

本稿では，Rashmi らによって提案された $[n,k,d]$ PM-MSR 符号がストレージと修復バンドワイズを最小にする最適な $[n,k,d,k-1]$ 再生成符号となることを証明した．今後の課題としては，一般の $d(\ge 2k-2)$ に対する $[n,k,d]$ PM-MSR 符号の最適性の証明などが挙げられる．

謝辞

本研究の一部は，横浜商科大学学術研究会助成金の援助による．

参考文献

[1] F.J. MacWilliams, and N.J.A. Sloane, The Theory of Error-Correcting Codes, North-Holland Pub. Co, Sole distributors for the U.S.A. and Canada, Elsevier/North-Holland, 1977.

[2] A.G. Dimakis, P.B. Godfrey, Y. Wu, M.J. Wainwright, and K. Ramchandran, "Network Coding for Distributed Storage Systems," IEEE Transactions on Information Theory, vol.56, no.9, pp.4539–4551, Sept. 2010.

[3] C. Suh, and K. Ramchandran, "Exact-Repair MDS Code Construction Using Interference Alignment," IEEE Transactions on Information Theory, vol.57, no.3, pp.1425–1442, March 2011.

[4] 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," IEEE Transactions on Information Theory, vol.57, no.8, pp.5227–5239, Aug. 2011.

[5] N.B. Shah, K.V. Rashmi, P.V. Kumar, and K. Ramchandran, "Distributed Storage Codes With Repair-by-Transfer and Nonachievability of Interior Points on the Storage-Bandwidth Tradeoff," IEEE Transactions on Information Theory, vol.58, no.3, pp.1837–1852, March 2012.

[6] N.B. Shah, K.V. Rashmi, P.V. Kumar, and K. Ramchandran, "Interference Alignment in Regenerating Codes for Distributed Storage: Necessity and Code Constructions," IEEE Transactions on Information Theory, vol.58, no.4, pp.2134–2158, Apr. 2012.

[7] 吉田隆弘，地主創，松嶋敏泰，"分散情報の安全性を考慮した再生成符号のモデル化とその最適性に関する一検討," 電子情報通信学会技術研究報告. IT, 情報理論，vol.113，no.153，pp.27–32，2013.

[8] T. Cover, and J. Thomas, Elements of Information Theory 2nd Edition, Wiley-Interscience, 2006.