早稲田大学

博士学位論文

分散ストレージ符号化の一般化に関する研究

A Study on Generalization of Coding for Distributed Storage System

2018 年 2 月

鎌塚 明

Akira KAMATSUKA

早稲田大学

博士学位論文

分散ストレージ符号化の一般化に関する研究

A Study on Generalization of Coding for Distributed Storage System

2018 年 2 月

早稲田大学大学院 基幹理工学研究科

数学応用数理専攻 情報理論研究

鎌塚 明

Akira KAMATSUKA

目次

図目次

表目次

第 1 章

序論

1.1　研究背景

近年，記録ストレージの大容量化や，各種クラウドサービスの発展に伴い，企業および個人が保有する大量のデータを安全かつ効率的に管理する必要性が高まっている．実際，頻繁にアクセスされるデータを保有するストレージについては，故障によるデータ消失のリスクが無視できない頻度で生じ得る．データ消失に対する最も単純な対策としては，保存すべきデータ（元データと呼び $\boldsymbol{m} \in \mathbb{F}_q^B$ で表す．ここで，$\mathbb{F}_q^B$ は位数 q の有限体 $\mathbb{F}_q$ 上の B 次元ベクトル空間を表す．）を複数個（n 個）のストレージに複製することだが，これは元データの n 倍のデータサイズを必要とするため効率が悪い．そこで，元データ $\boldsymbol{m}$ に対して冗長性を付加する写像（符号化と呼ぶ） $\boldsymbol{m} \mapsto (\boldsymbol{c}_1, \ldots, \boldsymbol{c}_n) \in (\mathbb{F}_q^\alpha)^n$ を施し，写像されたデータの一部（分散情報と呼ぶ） $\boldsymbol{c}_i, i = 1, \ldots, n$ を各ストレージに保存するシステム（分散ストレージステム）で元データ $\boldsymbol{m}$ を管理することを考える．ここで，$\alpha \in \mathbb{N}$ を分散情報のサイズと呼ぶ．

分散ストレージステムが備えるべき主機能は元データの復元機能である．これまで復元機能を持つ符号化として，Reed-Solomon 符号化を始めとする MDS 符号化に関する研究がなされてきた．この符号化により，分散ストレージシステムは

(1) n 個のストレージの内，任意の k 個のストレージが持つ分散情報から元データを復元可能
（$\overset{\text{def.}}{\Longleftrightarrow}$ 任意の $i_1, \ldots, i_k \in \{1, \ldots, n\}$ に対して，ある写像 $(\boldsymbol{c}_{i_1}, \ldots, \boldsymbol{c}_{i_k}) \mapsto \boldsymbol{m}$ が存在）

という機能を実現できる．すなわち，任意の $n-k$ 個のストレージが故障したとしても，残りの k 個のストレージから元データを復元できる．その後，元データの復元機能に加えて，以下のような付加機能を持つ分散ストレージ符号化に関する研究がなされてきた．

(2) 元データの情報漏えい耐性機能

(3) 故障ストレージの効率的な修復機能

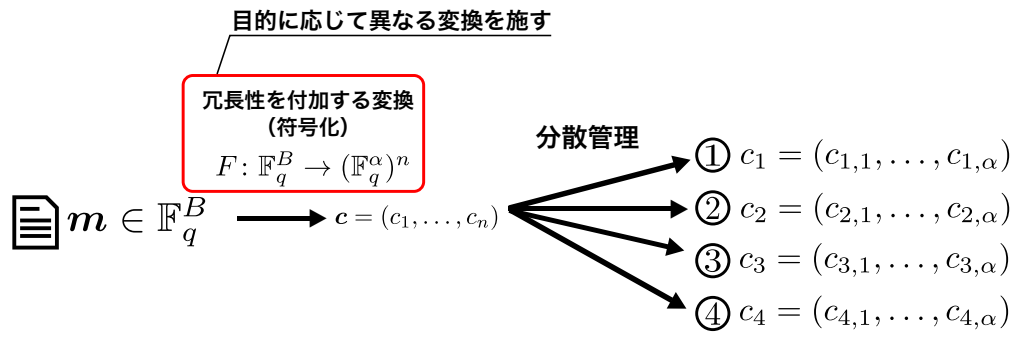

図 1.1　冗長性を加える写像（分散ストレージ符号化）

(2) を実現する符号化としては，(k,n)-秘密分散法に関する研究がなされてきた．代表的な符号化に Shamir による (k,n)-しきい値法がある．これは，元データと一様乱数をもとに生成した多項式上の n 点を分散情報として各ストレージが保存する方式である．この符号化を用いると，主機能 (1) に加え，

- 任意の $k-1$ 個以下のストレージが持つ分散情報からは元データに関する情報を得られない
  （$\overset{\text{def.}}{\iff}$ 任意の $i_1, \ldots, i_k$ に対して，$H(\boldsymbol{m} \mid \boldsymbol{c}_{i_1}, \ldots, \boldsymbol{c}_{i_{k-1}}) = H(\boldsymbol{m})$），

（ここで $H(\cdot \mid \cdot)$ や $H(\cdot)$ は情報理論における情報エントロピー関数を表す）という機能を分散ストレージステムに持たせることができる．Shamir は (k,n)-秘密分散法を

用いた際の各ストレージが保存すべき分散情報のサイズの限界を示し，(k, n)-しきい値法がこの限界を達成する方式であることを示した．

(3) を実現する符号化としては，近年，Dimakis らによって $[n, k, d]$-再生成符号化が提案されている．従来，故障ストレージの修復は，復元した元データに再度符号化を施すことによってなされてきた（これを自明な修復法と呼ぶ）．分散情報のサイズが α であるため，自明な修復法には $k\alpha$ だけの通信量が必要になる．$[n, k, d]$-再生成符号化された分散ストレージステムにおいては，j 番目の故障ストレージの修復の際にはまず，$d\,(\leq n-1)$ 個の修復用ストレージが選ばれる．選ばれた各ストレージは，各々の分散情報 $\boldsymbol{c}_i$ から修復用データ $p_{i\to j} \in \mathbb{F}_q^{\beta}$ を生成（$\boldsymbol{c}_i \mapsto p_{i\to j}$）し，故障ストレージに送信する．故障ストレージは d 個の修復用データを用いて分散情報を再生成することにより修復を行う．修復用データのサイズは $\beta \in \mathbb{N}$ であるので，このときの通信量（修復バンドワイズと呼ぶ）は $d\beta(\leq k\alpha)$ となり，自明な修復法よりも効率的に修復ができる．Dimakis らは，$[n, k, d]$-再生成符号における分散情報のサイズ α と修復バンドワイズ $d\beta$ の間のトレードオフ不等式を示した：

$$\sum_{i=0}^{k-1} \min\{\alpha, (d-i)\beta\} \geq B,$$

ここで，B は元データのサイズを表す．このトレードオフ不等式において，分散情報のサイズ α を最小にしたもとで修復バンドワイズ $d\beta$ を最小にする $[n, k, d]$-再生成符号化を MSR (minimum-storage regenerating) 符号化と呼ぶ．一方，修復バンドワイズを最小にしたもとでストレージを最小にする $[n, k, d]$-再生成符号化を MBR (minimum-bandwidth regenerating) 符号化と呼ぶ．具体的な MSR/MBR 符号化の構成法としては，Rashmi らによる Product Matrix 法や，Shah らによる Repair by Transfer 法等が提案されている．

1.2　研究の目的と位置付け

前節で説明した従来の分散ストレージステムの機能 (1)(2)(3) はいずれも，ストレージ数が一定のしきい値（k や d）以上あるいは以下になったときに発揮されるしきい値型の分散ストレージシステムである．しかしながら，実際の分散ストレージシステムの構築および運用においては，すべてのストレージが全く同じ能力（スト

レージ容量，耐久性，計算能力等）を持っているわけではないため，ストレージ毎の役割を考慮した分散ストレージを設計することが必要になる．すなわち，(1)(2)(3) の条件を一般化した機能をもつ分散ストレージステムの構築が必要である．

(1) および (2) の条件の一般化に関する研究としては，伊東らによって Γ-秘密分散法が提案されている．ここで，Γ は (1) および (2) に関して一般化された条件を表す．具体的には，n 個のストレージのインデックスを表す集合を $\{1,\ldots,n\}$ とするとき，元データを復元可能なストレージのインデックスの集合族 $\mathcal{A}$ と，元データに関する情報を一切得られないストレージのインデックスの集合族 $\mathcal{B}$ の組 $\Gamma = (\mathcal{A},\mathcal{B})$ として定義される．Γ-秘密分散法の構成法としては，各ストレージに対して，しきい値法によって生成される分散情報を複数個割り当てる方式（複数割当法）が提案されている．ここで，与えられた条件 Γ を満たすためには，ストレージ集合 $\boldsymbol{A} \in \mathcal{A}$ に対しては，ある (t,m)-しきい値法で復元するのに十分な個数（t 個以上）の分散情報を割り当て，$\boldsymbol{B} \in \mathcal{B}$ に対しては，(t,m)-しきい値法で元データに関する情報が得られなくなるような個数（$t-1$ 個以下）の分散情報を割り当てればよい．その後，各ストレージが保存する分散情報サイズの平均 ρ を最小化する構成法が岩本らによって提案されている．この構成法は $\mathcal{A},\mathcal{B}$ に対する割当の仕方を制約として，ρ を最小化する整数計画問題を繰り返し解くことで最適なパラメータ (t,m) を探索している．

本研究では，(1) および (3) に関する条件を一般化した Ω-再生成符号およびその構成法を提案する．この一般化の動機づけとしては例えば，修復に関して，

- 耐久性の高いストレージを，故障ノード修復に多く参加させたい場合
- 修復の際には，距離が近いノード同士で修復をさせたい場合

が挙げられる．本研究では (1) および (3) に関する一般化条件 Ω を Γ-秘密分散法と同様に，ストレージのインデックスの集合族の組 $\Omega = \left(\mathcal{A},(\mathcal{B}_j)_{j=1}^{n}\right)$ として定義し，Ω が従来の $[n,k,d]$-再生成符号における条件 (1) および (3) を含むことを示す．ここで，$\mathcal{A}$ は元データを復元可能なストレージのインデックスの集合族を表し，$\mathcal{B}_j$ は故障ストレージ j を修復可能なストレージのインデックスの集合族を表す．

Ω-再生成符号においては，各ストレージ i が保存する分散情報 $\boldsymbol{c}_i \in \mathbb{F}_q^{\alpha_i}$ のサイズ $\alpha_i \in \mathbb{N}$ や，故障ストレージ j へ送信する修復用データ $p_{i\to j} \in \mathbb{F}_q^{\beta_{i\to j}}$ のサイズ

$\beta_{i\to j} \in \mathbb{N}$ が，ストレージごとに異なる．そこで本研究では，Ω-再生成符号の評価基準として，各ストレージが保存する分散情報のサイズの平均 ρ_S および修復バンドワイズの平均 ρ_R を提案し，従来の MBR/MSR 符号に相当する Ω-MSR 再生成符号および Ω-MBR 再生成符号を定義する．

Ω-再生成符号の具体的な構成法としては，従来の再生成符号の分散情報を用いた複数割当法を提案する．このとき，与えられた条件 Ω を満たすための条件として，$\boldsymbol{A} \in \mathcal{A}$ に対しては，ある $[\ell, t, r]$ 再生成符号で元データを復元するのに十分な個数（t 個以上）の分散情報を割り当て，$\boldsymbol{B} \in \mathcal{B}_j$ に対しては，$[\ell, t, r]$-再生成符号において故障ストレージ j を修復するのに十分な個数（r 個以上）の分散情報を割り当てればよいことを示す．

本研究ではさらに，複数割当法による符号クラスの中で「ρ_S を最小にしたもとで ρ_R を最小にする符号（Ω-MSR-map 符号）」および「ρ_R を最小にしたもとで ρ_S を最小にする符号（Ω-MBR-map 符号）」を定義し，その整数計画法を用いた探索による構成アルゴリズムを導出する．この構成アルゴリズムではまず，$\mathcal{A}, (\mathcal{B}_j)_{j=1}^n$ に対する割当の仕方を制約とした，ρ_S あるいは ρ_R のいずれか一方を最小化する整数計画問題を繰り返し解き，最小値を与えるパラメータ $[\ell, t, r]$ を探索する．次に，探索したパラメータの中でもう一方を最小化する $[\ell, t, r]$ を求める．ここで，Ω-MSR/MBR-map 符号を構成する際には，Γ-秘密分散法の場合と異なり，$[\ell, t, r]$-再生成符号におけるパラメータ (α, β) をも最適化する必要がある．本提案においては，それぞれ MSR/MBR 符号のパラメータを用いれば良いことを示す．

Ω-再生成符号は Γ-秘密分散法と異なり (3) の修復条件を一般化しているため，故障ストレージの修復法に関して工夫の余地がある．そこで本研究ではさらに，複数割当法を用いた場合の，通信量の意味でより効率的な修復法を提案し，その効率性について解析を行う．また，その修復法を用いた場合の Ω-MSR/MBR-map 符号の構成法についても考え，Ω-MSR-map 符号については上述と同様の構成法が導出できることを示す．一方，Ω-MBR-map 符号については，割り当てる再生成符号における最適なパラメータ (α, β) が決定できないため，準最適な構成法を提案する．

1.3　本論文の構成

本論文の構成は以下の通りである．第 2 章では，準備として $[n, k, d]$-再生成符号および (k, n)-秘密分散法について概観する．第 3 章では，復元および再生成に関する条件を一般化した Ω-再生成符号とその評価基準を提案する．構成法としては複数割当法を提案し，複数割当法を用いた符号クラスの中での最適な符号として，Ω-MSR/MBR-map 符号の構成アルゴリズムを導出する．第 4 章では 複数割当法を用いた場合の故障ストレージの修復法に関して，通信量の意味でより効率的な修復法を提案し，修復にかかる通信量について解析を行う．そのうえで，効率的な修復法を用いた場合の Ω-MSR/MBR-map 符号の構成アルゴリズムについて考察する．第 5 章では，提案した各アルゴリズムに関して，具体的な数値例を構成し，効率性について考察する．最後に，第 6 章で本論文の結論と今後の展望を述べる．

第 2 章

準備

本章では，分散ストレージの主機能である (1) 復元機能の付加機能である

(2) 元データの情報漏えい耐性機能

(3) 故障ストレージの効率的な修復機能

を実現する符号化に関する従来研究として，

1. $[n, k, d]$-再生成符号
2. (k, n)-秘密分散法およびその一般化である Γ-秘密分散法

に関して述べる．

まずは，情報理論の基礎事項について述べ，その後，各符号の定義および性質と，具体的な構成法について述べる．

2.1 情報理論における基礎事項

本節では，情報理論で用いられる情報エントロピーおよび条件付きエントロピーの定義と性質について述べる．

定義 2.1 (確率空間)**.** Ω を任意の集合とし，Ω の σ-加法族を $\mathcal{A}$ とする．また，$\mathcal{A}$ 上の確率測度を $\mu\colon \mathcal{A} \to [0, 1]$ とする．このとき，これらの 3 つ組 $(\Omega, \mathcal{A}, \mu)$ を**確率空間**と呼ぶ．

以降，確率空間 $(\Omega, \mathcal{A}, \mu)$ は 1 つ固定されているものする．

定義 2.2 (確率変数)**.** $X\colon \Omega \to \mathbb{R}$ が以下の条件を満たすとき，X を Ω 上の**確率変数**と呼ぶ：

任意の $B \in \mathcal{B}$ に対して，

$$X^{-1}(B) \in \mathcal{A}, \tag{2.1}$$

ここで，$\mathcal{B}$ は実数体 $\mathbb{R}$ 上のボレル集合族を表す．特に，X の値域 $X(\Omega)$ が高々可算集合のとき，すなわち，ある可算無限集合 $\mathcal{X}$ が存在して $\mu(X^{-1}(\mathcal{X})) = 1$ のとき，X を**離散確率変数**と呼ぶ．

定義 2.3 (確率分布)**.** 確率変数 X に対して，以下で定義される関数 $P^X\colon \mathcal{B} \to [0,1]$ を X の**確率分布**と呼ぶ：

$$P^X(B) := \mu\left(X^{-1}(B)\right), \qquad B \in \mathcal{B}. \tag{2.2}$$

定義 2.4 (確率質量関数)**.** 離散確率変数 X に対して，以下で定義される関数 $p_X\colon \mathcal{X} \to [0,1]$ を X の**確率質量関数**と呼ぶ：

$$p_X(x) = \mu(X^{-1}(\{x\})), \qquad x \in \mathcal{X}. \tag{2.3}$$

特に，値域 $\mathcal{X}(\Omega) = \mathcal{X}$ が有限である確率変数 X の確率質量関数が以下で与えられるとき，X は**一様分布**に従うと呼ぶ：

$$p_X(x) = \frac{1}{|\mathcal{X}|}, \qquad x \in \mathcal{X}. \tag{2.4}$$

定義 2.5 (同時確率関数，条件付き確率関数)**.** 離散確率変数 X, Y に対し，以下で定義される関数 $p_{X,Y}\colon \mathcal{X} \times \mathcal{Y} \to [0,1]$ を X と Y の**同時確率関数**と呼ぶ：

$$p_{X,Y}(x,y) := \mu^{-1}\left(\{x\}, \{y\}\right), \qquad x \in \mathcal{X}, y \in \mathcal{Y}. \tag{2.5}$$

また，以下で定義される関数 $p_{X|Y}\colon \mathcal{X} \times \mathcal{Y} \to [0,1]$ を Y が与えられたもとでの X に関する**条件付き確率関数**と呼ぶ：

$$p_{X|Y}(x \mid y) := \frac{p_{X,Y}(x,y)}{p_Y(y)}. \tag{2.6}$$

以降，$X, Y, \ldots,$ は離散確率変数とし，$\mathcal{X}$ は有限集合とする．

定義 2.6 (エントロピー)**.** 確率変数 X とその確率質量関数 p_X に対し，以下で定義される量 $H(X)$ を X の**情報エントロピー**と呼ぶ：

$$H(X) := -\sum_{x \in \mathcal{X}} p_X(x) \log p_X(x). \tag{2.7}$$

定義 2.7 (条件付きエントロピー)**.** 確率変数 X, Y に対して，以下で定義される量を $H(X \mid Y)$ Y が与えられたもとでの X に関する**条件付きエントロピー**と呼ぶ：

$$H(X \mid Y) := -\sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}} p_{X,Y}(x,y) \log p_{X|Y}(x \mid y). \tag{2.8}$$

定理 2.8 ([3])**.** 任意の確率変数 X, Y に対して以下が成り立つ：

$$H(X \mid Y) \leq H(X), \tag{2.9}$$

ここで，等号成立条件は X と Y が互いに独立であるときである．

注意 2.9. この定理は，任意の条件付けは，片方の確率変数に関する平均的な情報量を増加させないことを示している．

2.2　秘密分散法

本節では，(2) 元データの情報漏えい耐性機能をもつ符号化として，(k, n)-秘密分散法およびその一般化である Γ-秘密分散法の定義と性質および具体的な符号の構成法について述べる．

以降，元データを $m \in \mathbb{F}_q$ とおき，$\mathbb{F}_q$ 上の一様分布に従うとする．

2.2.1　(k,n)-DSS と (k,n)-SSS の定義

本節では (k,n)-DSS および (k,n)-秘密分散法 (SSS; Secret Sharing Scheme) を定義する.

定義 2.10. 次の 2 つのフェーズから構成される方式を (k,n)-DSS と呼ぶ.

＜符号化フェーズ＞　管理者は，関数 $F\colon \mathbb{F}_q \to \left(\mathbb{F}_q\right)^n$ を用いて元データ $m \in \mathbb{F}_q$ に対する n 個の分散情報 $F(m) = (w_1, \ldots, w_n)$, $w_i \in \mathbb{F}_q, i \in [n]$ を生成する．次に，安全な通信路を用いて各 w_i をノード i に送信する．ノード i は受信した分散情報 w_i をそれぞれ保管する.

＜元データ復元フェーズ＞　データコレクタ DC は n 個のノード集合から任意の k 個のノード $i_1, \ldots, i_k$ を選択し，各ノードが保管している分散情報を受信する．DC は，関数 $G\colon \left(\mathbb{F}_q\right)^k \to \mathbb{F}_q$ を用いて，元データ $\hat{\boldsymbol{m}} = G(w_{i_1}, \ldots, w_{i_k}) \in \mathbb{F}_q$ を推定する.

注意 2.11. (k,n)-DSS は $[n,k,d]$-DSS と比較したときに,

- $B = 1, \alpha = 1$ である
- ＜修復フェーズ＞を持たない

ことに注意せよ.

定義 2.12. (k,n)-DSS において，以下の条件を満たす関数の組 (F,G) を (k,n)-SSS（秘密分散法）と呼ぶ.

任意の $i_1, \ldots, i_k \in [n]$ に対して，以下が成り立つ：

$$H\left(m \mid w_{i_1}, \ldots, w_{i_k}\right) = 0, \tag{2.10}$$

ここで，$H(X \mid Y)$ は Y が与えられたもとでの X の条件付きエントロピーである.

任意の $i_1, \ldots, i_{k-1} \in [n]$ に対して，以下が成り立つ：

$$H\left(m \mid w_{i_1}, \ldots, w_{i_{k-1}}\right) = H(m). \tag{2.11}$$

注意 2.13. ここで,

- 条件 (2.10) は，任意の k 個のストレージの分散情報から，元データ $\boldsymbol{m}$ を復元可能であることを示している
- 条件 (2.11) は，任意の $k-1$ 個以下のストレージの分散情報からは，元データ $\boldsymbol{m}$ に関する情報が一切得られないことを示している

ことに注意せよ.

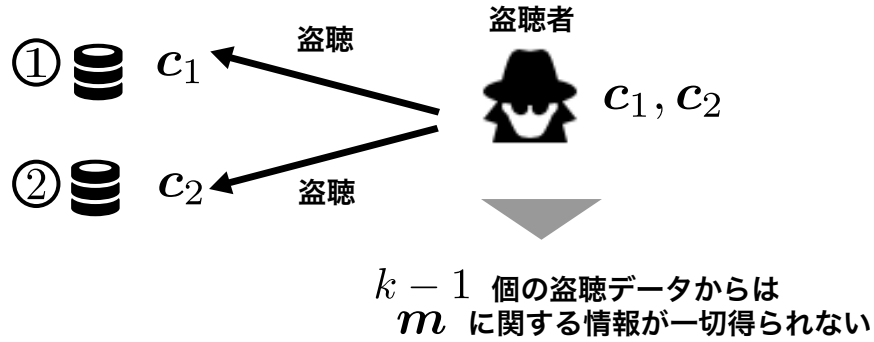

図 2.1　(k,n)-秘密分散法 ($k = 3$)

2.2.1.1　(k,n)-SSS の分散情報サイズの限界式

本節では，Shamir によって示された，(k,n)-SSS の分散情報の限界式について述べる.

定理 2.14. 任意の (k,n)-SSS は以下を満たす：

$$H(w_j) \geq H(m), \qquad j = 1, \ldots, n. \tag{2.12}$$

この定理は，(k,n)-SSS においては分散情報 w_j のサイズが，元データ $\boldsymbol{m}$ のサイズ以上でなければならないことを示している．

2.2.2　Shamir による (k,n)-SSS の構成法（(k,n)-しきい値法）

本節では，(k,n)-SSS の具体的な構成法として，(k,n)-しきい値法を説明する．

＜符号化フェーズ＞

1. $k-1$ 個の乱数 $a_1,\ldots,a_{k-1}$ を一様分布に従って独立に生成する
2. $(k-1)$ 次多項式 $f(x)$ を以下で定義する：

$$f(x) := m + a_1 x + a_2 x^2 + \cdots + a_{k-1}x^{k-1} \tag{2.13}$$

3. ストレージ i に保管する分散情報 w_i は，以下で生成：

$$w_i = f(i) \tag{2.14}$$

$$= s + a_1 i + a_2 i^2 + \cdots + a_{k-1} i^{k-1}, \qquad i = 1,\ldots,n. \tag{2.15}$$

例 2.1. $k=3, n=4, m=5 \in \mathbb{F}_{256}$ の場合の例を示す：

＜符号化フェーズ 1,2,3 ＞

1. $a_1 = 1, a_2 = 2$ が得られたとする．
2. このときの f は，

$$f(x) = 5 + x + 2x^2. \tag{2.16}$$

3. 各ストレージ i への分散情報 w_i は以下で与えられる：

$$v_1 = 5 + 1\times 1 + 2\times 1^2 = 8, \tag{2.17}$$

$$v_2 = 5 + 1\times 2 + 2\times 2^2 = 15, \tag{2.18}$$

$$v_3 = 5 + 1\times 3 + 2\times 3^2 = 26, \tag{2.19}$$

$$v_4 = 5 + 1\times 4 + 2\times 4^2 = 41. \tag{2.20}$$

＜元データ復元フェーズ＞

1. ストレージ $i_1, \ldots, i_k$ の復元する場合，以下の連立方程式を解けば良い：
   （k 個の未知変数 $m, a_1, \ldots, a_{k-1}$）：

$$\begin{cases} v_{i_1} = m + i_1 a_1 + i_1^2 a_2 + \cdots + i_1^{k-1} a_{k-1} \\ v_{i_2} = m + i_2 a_1 + i_2^2 a_2 + \cdots + i_2^{k-1} a_{k-1} \\ \qquad\qquad \vdots \\ v_{i_k} = m + i_k a_1 + i_k^2 a_2 + \cdots + i_k^{k-1} a_{k-1} \end{cases} \tag{2.21}$$

2. 上記方程式を書き換えると，

$$\begin{bmatrix} v_{i_1} \\ v_{i_1} \\ \vdots \\ v_{i_k} \end{bmatrix} = \begin{bmatrix} 1 & i_1 & i_1^2 & \cdots & i_1^{k-1} \\ 1 & i_2 & i_2^2 & \cdots & i_2^{k-1} \\ \vdots & \vdots & \ddots & \vdots & \\ 1 & i_k & i_k^2 & \cdots & i_k^{k-1} \end{bmatrix} \begin{bmatrix} s \\ a_1 \\ \vdots \\ a_{k-1} \end{bmatrix}. \tag{2.22}$$

   となり，係数行列が Vandermonde 行列であるから，正則であり，解が一意に定まる．

例 2.2. $k = 3, n = 4, m = 5 \in \mathbb{F}_{256}$ の場合の例を示す：

ストレージ $1, 2, 3$ の分散情報 $v_1 = 8, v_2 = 15, v_3 = 26$ を用いて，m を復元する：

以下の連立方程式を解く：

$$\begin{cases} 8 &= m + a_1 \times 1 + a_2 \times 1^2, \\ 15 &= m + a_1 \times 2 + a_2 \times 2^2, \cdot \\ 26 &= m + a_1 \times 3 + a_2 \times 3^2 \end{cases} \tag{2.23}$$

これを解くと，$s = m, a_1 = 1, a_2 = 2$ が得られる．

注意 2.15. (k, n)-しきい値法は，不等式 (2.12) の等号を達成するという意味で，最適な構成法であることが知られている [13].

2.2.3　Γ-DSS と Γ-SSS の定義

本節では Γ-DSS および Γ-秘密分散法 (SSS; Secret Sharing Scheme) を定義する．

ストレージノード集合の族 $\mathcal{A}_1 \subseteq 2^{[n]}$ が与えられているとし，これを有資格集合 (qualified set) と呼ぶ．また，ノード集合の族 $\mathcal{A}_0 = 2^{[n]} \setminus \mathcal{A}_1$ とおき，禁止集合 (forbidden set) と呼ぶ．$\mathcal{A}_0, \mathcal{A}_1$ はそれぞれ，m を復元できるノード集合の族および m に関する情報を一切得られないノード集合の族を意味する．さらに，$\mathcal{A}_0$ と $\mathcal{A}_1$ の組を Γ とおき，アクセス構造と呼ぶ．また，ノード集合 $\boldsymbol{A} = \{i_1, \ldots, i_{|\boldsymbol{A}|}\}$ の分散情報を要素としてもつベクトルを $\boldsymbol{w}_{\boldsymbol{A}} := (w_{i_1}, \ldots, w_{i_{|\boldsymbol{A}|}})$ と記す．

定義 2.16. 次の 2 つのフェーズから構成される方式を Γ-DSS と呼ぶ．

＜分散情報生成フェーズ＞　管理者は，符号化関数 $F\colon \mathbb{F}_q \to \prod_{i=1}^{n} \mathbb{F}_q^{\alpha_i}$ を用いて元データ $m \in \mathbb{F}_q$ に対する n 個の分散情報 $F(m) = (w_1, \ldots, w_n)$, $w_i \in \mathbb{F}_q^{\alpha_i}, i \in [n]$ を生成する．次に，安全な通信路を用いて各 w_i をノード i に送信する．ノード i は受信した分散情報 w_i をそれぞれ保管する．

＜元データ復元フェーズ＞　データコレクタ DC は n 個のノード集合から任意のノード集合 $\boldsymbol{A} \in \mathcal{A}_1$ を選択し，各ノードが保管している分散情報を受信する．DC は，復号関数 $G\colon \prod_{j=1}^{|\boldsymbol{A}|} \mathbb{F}_q^{\alpha_{i_j}} \to \mathbb{F}_q$ を用いて，元データ $m = G(w_{\boldsymbol{A}}) \in \mathbb{F}_q$ を復元する．

定義 2.17. Γ-DSS において，以下の条件を満たす関数の組 (F, G) を Γ-SSS と呼ぶ．

任意の $\boldsymbol{A} \in \mathcal{A}_1$ に対して，以下が成り立つ：

$$H(m \mid w_{\boldsymbol{A}}) = 0, \tag{2.24}$$

ここで，$H(X \mid Y)$ は Y が与えられた下での X の条件付きエントロピーである．

任意の $\boldsymbol{A} \in \mathcal{A}_0$ に対して，以下が成り立つ：

$$H(m \mid w_{\boldsymbol{A}}) = H(m). \tag{2.25}$$

アクセス構造 $\Gamma = (\mathcal{A}_0, \mathcal{A}_1)$ は以下の単調性条件 (monotonicity condition) を満たす：

$$\boldsymbol{A} \subseteq \boldsymbol{A}' \text{ and } \boldsymbol{A} \in \mathcal{A}_1 \Longrightarrow \boldsymbol{A}' \in \mathcal{A}_1, \tag{2.26}$$

$$\boldsymbol{A}' \subseteq \boldsymbol{A} \text{ and } \boldsymbol{A} \in \mathcal{A}_0 \Longrightarrow \boldsymbol{A}' \in \mathcal{A}_0. \tag{2.27}$$

したがって，極小有資格集合 $\mathcal{A}_1^-$ および極大禁止集合 $\mathcal{A}_0^+$ が定義される．

例 2.3. 以下のアクセス構造 $\Gamma = (\mathcal{A}_0, \mathcal{A}_1)$ を持つ Γ-SSS は (k, n)-SSS を表す：

$$\mathcal{A}_1 = \left\{ \boldsymbol{A} \in 2^{[n]} : |\boldsymbol{A}| \geq k \right\}, \tag{2.28}$$

$$\mathcal{A}_0 = \left\{ \boldsymbol{A} \in 2^{[n]} : |\boldsymbol{A}| \leq k-1 \right\}. \tag{2.29}$$

定義 2.18. Γ-SSS の効率性は，次の平均符号化レートで定義される [14]：

$$\tilde{\rho} := \frac{1}{n} \sum_{i=1}^{n} \rho_i, \tag{2.30}$$

ここで,

$$\rho_i := \frac{H(w_i)}{H(m)} \geq 1, \qquad i \in [n] \tag{2.31}$$

であり，$H(X)$ は X のエントロピーを表す．

2.2.4　複数割当写像および整数計画法を用いた Γ-SSS の構成法

本節では，文献 [14] で提案されている複数割当写像 (multiple-assignment map) および整数計画法 (integer programming) を用いた Γ-SSS の構成法を概説する．

定義 2.19 (複数割当写像 [14])**.** $\Gamma = (\mathcal{A}_0, \mathcal{A}_1)$ をアクセス構造とし，$\boldsymbol{W}^{(t,m)} := \left\{ w_1^{(t)}, \ldots, w_m^{(t)} \right\}$ を Shamir の (t, ℓ)-しきい値法による分散情報の集合とする．このとき，以下の条件を満たす写像 $\mu_\Gamma \colon [n] \to 2^{\boldsymbol{W}^{(t,m)}}$ を複数割当写像と呼ぶ：

$$|\mu_\Gamma(\boldsymbol{A})| \geq t, \qquad \boldsymbol{A} \in \mathcal{A}_1, \tag{2.32}$$

$$|\mu_\Gamma(\boldsymbol{A})| \leq t-1, \qquad \boldsymbol{A} \in \mathcal{A}_0, \tag{2.33}$$

$$\mu_\Gamma([n]) = \boldsymbol{W}_{(t,m)}. \tag{2.34}$$

ここで，$\mu_\Gamma(\boldsymbol{A}) := \bigcup_{i\in\boldsymbol{A}} \mu_\Gamma(i)$, $\boldsymbol{A} \subseteq [n]$ である．なお，文献 [14] においては，$\boldsymbol{A}$ は分散情報の部分集合として定義されているが，本論文では再生成符号におけるノーテーションとの対応を明確にするため $\boldsymbol{A}$ を分散情報の部分集合と一対一に対応するノード集合の部分集合として定義している．よって，本論文では [14] における複数割当写像の条件をノード集合 $\boldsymbol{A}$ を用いた同値な条件式 (2.32),(2.33),(2.34) で書き換えている．

複数割当写像を用いて以下のように Γ-SSS を構成できる．この構成法を Γ-SSS の複数割当法と呼ぶ．

＜分散情報生成フェーズ＞

まず，元データ $\boldsymbol{m}$ を Shamir の (t,ℓ)-しきい値法で符号化する $(n \leq \ell)$．次に，複数割当写像 μ_Γ を用いて，符号化関数 $F(\boldsymbol{m}) = (\mu_\Gamma(1), \ldots, \mu_\Gamma(n))$ で元データ $\boldsymbol{m}$ を符号化する．

＜元データ復元フェーズ＞

復号関数 G を Shamir の (t,ℓ)-しきい値法における復号関数とすると，データコレクタ DC は以下のようにしてノード集合 $\boldsymbol{A} \in \mathcal{A}_1$ によって元データ $\boldsymbol{m}$ を復元できる：

1. DC は，ノード $i_j \in \boldsymbol{A}$, $j = 1, \ldots, |\boldsymbol{A}|$ に接続
2. DC は，各ノード i_j から総計 t 個の (t,ℓ)-しきい値法の分散情報を受信
3. DC は，t 個の分散情報と (t,ℓ)-しきい値法の復号関数 G から $\boldsymbol{m}$ を復元

よって，式 (2.24) が成り立つ．また，この構成法が式 (2.25) を満たすことは，複数割当写像の式 (2.33) から直ちに分かる．

複数割当写像 μ_Γ による構成法における平均符号化レートは以下で与えられる：

$$\tilde{\rho} = \frac{1}{n}\sum_{i=1}^{n} |\mu_\Gamma(i)| \,. \tag{2.35}$$

岩本らは，式 (2.35) を目的関数に設定し，不等式 (2.32),(2.33) を制約式に設定した整数計画問題（最小化問題）を解くことにより，複数割当写像による符号クラスの中で最適な構成法（平均符号化レートを最小にする構成法）を提案した [14].

注意 2.20. 岩本らの構成法によって構成される符号が，アクセス構造 Γ を実現するすべての符号クラスの中で最適な符号であるとは限らない.

2.3　$[n, k, d]$-再生成符号 [1]

本節では，(3) 元データの情報漏えい耐性機能をもつ分散ストレージシステムおよびその符号化として，$[n, k, d]$-分散ストレージシステム (DSS; Distributed Storage System) および $[n, k, d]$-再生成符号を定義し，その性質と構成法について述べる.

以降，n 個のノードのなす集合を $[n] := \{1, \ldots, n\}$ とおく．また，元データを $\boldsymbol{m} \in \mathbb{F}_q^B$, $B \in \mathbb{N}$ とおき，一様分布に従うとする．ここで，$\mathbb{F}_q$ は位数が q の有限体を表す.

定義 2.21. 次の 3 つのフェーズから構成される方式を $[n, k, d]$-DSS と呼ぶ.

＜分散情報生成フェーズ＞　管理者は，関数 $F\colon \mathbb{F}_q^B \to \left(\mathbb{F}_q^\alpha\right)^n$ を用いて元データ $\boldsymbol{m} \in \mathbb{F}_q^B$ に対する n 個の分散情報 $F(\boldsymbol{m}) = (w_1, \ldots, w_n)$, $w_i \in \mathbb{F}_q^\alpha, i \in [n]$ を生成する．次に，安全な通信路を用いて各 w_i をノード i に送信する．ノード i は受信した分散情報 w_i をそれぞれ保管する．ここで，$\alpha \in \mathbb{N}$ は各ノードの分散情報のサイズを表し，ストレージと呼ぶ.

＜元データ復元フェーズ＞　データコレクタ DC は n 個のノード集合から任意の k 個のノード $i_1, \ldots, i_k$ を選択し，各ノードが保管している分散情報を受信する．DC は，関数 $G\colon \left(\mathbb{F}_q^\alpha\right)^k \to \mathbb{F}_q^B$ を用いて，元データ $\hat{\boldsymbol{m}} = G(w_{i_1}, \ldots, w_{i_k}) \in \mathbb{F}_q^B$ を推定する.

＜再生成フェーズ＞　故障ノード i の分散情報を再生成する際にはまず，新規ノード i を用意する．その新規ノードは $n-1$ 個のノード集合 $[n] \setminus \{i\}$ から任意の d 個のノード $i_1, \ldots, i_d$ を選択する．次に，選択されたノード i_j, $j = 1, \ldots, d$

は，保管している分散情報と関数 $f_i\colon \mathbb{F}_q^{\alpha} \to \mathbb{F}_q^{\beta}$ を用いて，再生成情報 $v_{i,i_j} = f_i(w_{i_j})$, $j = 1, \ldots, d$ をそれぞれ生成する．ここで，$\beta(\leq \alpha) \in \mathbb{N}$ は再生成情報のサイズを表す．これら d 個の再生成情報は，新規ノード i に送信され，新規ノードは関数 $g_i\colon \left(\mathbb{F}_q^{\beta}\right)^d \to \mathbb{F}_q^{\alpha}$ を用いて，分散情報 $\hat{w}_i = g_i(v_{i,i_1}, \ldots, v_{i,i_d}) \in \mathbb{F}_q^{\alpha}$ を生成する．このときの通信量 $d\beta$ を修復バンドワイズと呼ぶ．このとき，$\hat{w}_i \neq w_i$ であってもよいが，再生成後の $\hat{w}_i$ を用いたノード i を含む k 個のノードによる元データ復元およびノード i を含む d 個のノードによるノード $j \in [n] \setminus \{i\}$ の分散情報の再生成は可能でなければならない．

定義 2.22. $[n, k, d]$-DSS における関数の組 $(F, G, (f_i, g_i)_{i=1}^n)$ を $[n, k, d]$-再生成符号と呼ぶ．

注意 2.23. 以降，k は復元に必要な最小のノード数，$d(\leq n-1)$ は分散情報の再生成に必要な最小のノード数とする．このとき，$d < k$ とすると，d 個のノードから他のノードの分散情報を再生成するプロセスを繰り返すことで，k 個分の分散情報を得ることができる．よって d 個のノードから元の元データを復元できるが，これは k が復元に必要な最小のノード数であることに反する．したがって，$k \leq d$ である．

2.3.1　ストレージと修復バンドワイズのトレードオフ

Dimakis らは $[n, k, d]$-再生成符号において，ストレージ α と修復バンドワイズ $d\beta$ の間のトレードオフ関係が成り立つことを，グラフ理論における最大フロー・最小カット定理に相当する Network Information Flow 理論 [4] を用いることによって示した [1].

定理 2.24. $[n, k, d]$-再生成符号におけるパラメータ $(\alpha, d\beta), B$ は以下を満たす：

$$\sum_{i=0}^{k-1} \min\{\alpha, (d-i)\beta\} \geq B. \tag{2.36}$$

なお，情報エントロピーの関係式からも同様のトレードオフ不等式が示せる [5].

したがって，再生成符号においてはストレージ α と修復バンドワイズ $d\beta$ はともに小さいほうが望ましいが，これらを同時に最小化するのは不可能である．

2.3.2　MSR 符号

定義 2.25 (MSR 点／ MSR 符号)**.** $[n, k, d]$-再生成符号に対して，ストレージ α を最小にした下で修復バンドワイズ $d\beta$ を最小にする点を MSR 点と呼び，対応する符号を MSR 符号と呼ぶ．このときの $(\alpha, \beta) = (\alpha_{\mathrm{MSR}}, \beta_{\mathrm{MSR}})$ の値は以下で与えられる：

$$(\alpha_{\mathrm{MSR}}, \beta_{\mathrm{MSR}}) = \left(\frac{B}{k}, \frac{B}{k(d-k+1)} \right). \tag{2.37}$$

2.3.3　MBR 符号

定義 2.26 (MBR 点／ MBR 符号)**.** $[n, k, d]$-再生成符号に対して，修復バンドワイズ $d\beta$ を最小にした下でストレージ α を最小にする点を MBR 点と呼び，対応する符号を MBR 符号と呼ぶ．このときの $(\alpha, \beta) = (\alpha_{\mathrm{MBR}}, \beta_{\mathrm{MBR}})$ の値は以下で与えられる：

$$(\alpha_{\mathrm{MBR}}, \beta_{\mathrm{MBR}}) = \left(\frac{2dB}{k(2d-k+1)}, \frac{2B}{k(2d-k+1)} \right). \tag{2.38}$$

2.3.4　MSR 符号および MBR 符号の構成法

MSR 符号および MBR 符号の具体的な構成法については，Rashami らによる Product Matrix 法 (PM 法)[6] を始めとして多くの研究がある [7–12]．また，MBR 符号の構成法については，Shah らによる Repair-by-Transfer 法がある [5]．特に後者は，修復の際に演算操作が不要であり，シンボルのやりとりだけを用いて符号語シンボルを修復することができるため，Uncoded-Repair とも呼ばれる．

2.3.5　PM 法

本節では PM 法を用いた MBR 符号の構成法について説明する．特に，$\beta = 1, \alpha = d, B = k(2d-k+1)/2$ の場合を説明する．

＜符号化フェーズ＞

1. まず，元データ $\boldsymbol{m} = (m_1, \ldots, m_B)$ を用いて，以下の形をした行列 $M \in \mathbb{F}_q^{d\times d}$ を構成する：

$$M = \begin{bmatrix} M_1 & M_2 \\ M_2^\top & O \end{bmatrix} \in \mathbb{F}_q^{d\times d}, \tag{2.39}$$

ここで，$M_1 \in \mathbb{F}_q^{k\times k}, M_2 \in \mathbb{F}_q^{k\times(d-k)}, O : (d-k)$ 次零行列 とおいて，以下の成分に B 個の元データシンボルを配置する：

- M_1 の上三角成分の $k(k+1)/2$ 個の部分
- M_2 の $k(d-k)$ 個の成分

2. 残りは M が対称行列になるように定める.

3. 次に，$\Psi = [\Phi \quad \Delta]\,(\Phi \in \mathbb{F}_q^{n\times k}, \Delta \in \mathbb{F}_q^{n\times(d-k)})$ とおいて，Φ, Δ を次を満たすように定める：

(a) Φ の任意の k 行は線型独立

(b) Ψ の任意の d 行は線型独立

これら条件を満たす行列としては例えば，$\gamma_1, \ldots, \gamma_n \in \mathbb{F}_q \setminus \{0\}$ を相異なる元としたときの

$$\Psi = \begin{bmatrix} 1 & \gamma_1 & \gamma_1^2 & \cdots & \gamma_1^{d-1} \\ 1 & \gamma_2 & \gamma_2^2 & \cdots & \gamma_2^{d-1} \\ \vdots & \vdots & \ldots & \vdots & \\ 1 & \gamma_n & \gamma_n^2 & \cdots & \gamma_n^{d-1} \end{bmatrix} \tag{2.40}$$

（Vandermonde 行列）や Cauchy 行列がある.

4. 以下で符号化する：

$$C = \begin{bmatrix} \boldsymbol{c}_1^\top \\ \vdots \\ \boldsymbol{c}_n^\top \end{bmatrix} = \begin{bmatrix} \psi_1^\top \\ \vdots \\ \psi_n^\top \end{bmatrix} M = \Psi M \tag{2.41}$$

例 2.4. $(n, k, d) = (6, 3, 4), B = 9$ の例を示す：

＜符号化フェーズ 1, 2 ＞

$$M = \begin{bmatrix} m_1 & m_2 & m_3 & m_7 \\ m_2 & m_4 & m_5 & m_8 \\ m_3 & m_5 & m_6 & m_9 \\ m_7 & m_8 & m_9 & 0 \end{bmatrix}. \tag{2.42}$$

＜符号化フェーズ 3, 4 ＞

$\Psi = \begin{bmatrix} 1 & \gamma_1 & \gamma_1^2 & \gamma_1^3 \\ 1 & \gamma_2 & \gamma_2^2 & \gamma_2^3 \\ \vdots & \vdots & \vdots & \vdots \\ 1 & \gamma_9 & \gamma_9^2 & \gamma_9^3 \end{bmatrix}$（Vandermonde 行列）で符号化する（ここで，$\gamma_1, \ldots, \gamma_n$ は $\mathbb{F}_q \setminus \{0\}$ の相異なる元）：

$$\begin{bmatrix} \boldsymbol{c}_1 \\ \vdots \\ \boldsymbol{c}_9 \end{bmatrix} = \begin{bmatrix} c_{11} & c_{12} & c_{13} & c_{14} \\ \vdots & \vdots & \vdots & \vdots \\ c_{91} & c_{92} & c_{93} & c_{94} \end{bmatrix} = \begin{bmatrix} 1 & \gamma_1 & \gamma_1^2 & \gamma_1^3 \\ 1 & \gamma_2 & \gamma_2^2 & \gamma_2^3 \\ \vdots & \vdots & \vdots & \vdots \\ 1 & \gamma_9 & \gamma_9^2 & \gamma_9^3 \end{bmatrix} \begin{bmatrix} m_1 & m_2 & m_3 & m_7 \\ m_2 & m_4 & m_5 & m_8 \\ m_3 & m_5 & m_6 & m_9 \\ m_7 & m_8 & m_9 & 0 \end{bmatrix} \tag{2.43}$$

＜元データ復元フェーズ＞

1. ノード $i_1, \ldots, i_k$ で復元する場合，DC は以下の M に関する連立方程式を解けばよい：($\boldsymbol{c}_{i_j}, \psi_{i_j}, j = 1, \ldots, k$ は既知，M が未知)

$$\begin{bmatrix} \boldsymbol{c}_{i_1}^\top \\ \vdots \\ \boldsymbol{c}_{i_k}^\top \end{bmatrix} = \begin{bmatrix} \psi_{i_1}^\top \\ \vdots \\ \psi_{i_k}^\top \end{bmatrix} M = \Psi_{\mathsf{DC}} M = [\Phi_{\mathsf{DC}} \quad \Delta_{\mathsf{DC}}] M \tag{2.44}$$

$$= [\Phi_{\mathsf{DC}} M_1 + \Delta_{\mathsf{DC}} M_2^\top \quad \Phi_{\mathsf{DC}} M_2], \tag{2.45}$$

ここで，Φ_{DC} は Ψ の $i_1, \ldots, i_k$ 列からなる k 次行列.

Δ_{DC} は Ψ_{DC} から Φ_{DC} を除いた $k \times (d-k)$ 行列．Ψ の条件 1. からこの方程式は解ける.

例 2.5. $(n, k, d) = (6, 3, 4), B = 9$ の例を示す：

＜元データ復元フェーズ 1 ＞

ストレージ $1,\ldots,k$ で復元する場合を考える．このとき，以下の連立方程式を解けばよい（$\boldsymbol{c}_1,\boldsymbol{c}_2,\boldsymbol{c}_3,\gamma_1,\gamma_2,\gamma_3$ は既知，$m_1,\ldots,m_9$ が未知）：

$$\begin{bmatrix}\boldsymbol{c}_1\\ \boldsymbol{c}_2\\ \boldsymbol{c}_3\end{bmatrix}=\begin{bmatrix}c_{11} & c_{12} & c_{13} & c_{14}\\ c_{21} & c_{22} & c_{23} & c_{24}\\ c_{31} & c_{32} & c_{33} & c_{34}\end{bmatrix}=\begin{bmatrix}1 & \gamma_1 & \gamma_1^2 & \gamma_1^3\\ 1 & \gamma_2 & \gamma_2^2 & \gamma_2^3\\ 1 & \gamma_3 & \gamma_3^2 & \gamma_3^3\end{bmatrix}\begin{bmatrix}m_1 & m_2 & m_3 & m_7\\ m_2 & m_4 & m_5 & m_8\\ m_3 & m_5 & m_6 & m_9\\ m_7 & m_8 & m_9 & 0\end{bmatrix} \tag{2.46}$$

- まず，次の方程式の右辺の係数行列が正則なので，m_7,m_8,m_9 が解ける：

$$\begin{bmatrix}c_{14}\\ c_{24}\\ c_{34}\end{bmatrix}=\begin{bmatrix}1 & \gamma_1 & \gamma_1^2\\ 1 & \gamma_2 & \gamma_2^2\\ 1 & \gamma_3 & \gamma_3^2\end{bmatrix}\begin{bmatrix}m_7\\ m_8\\ m_9\end{bmatrix} \tag{2.47}$$

- したがって，残りの成分は以下の方程式を解くことで求める：

$$\begin{bmatrix}c_{11} & c_{12} & c_{13}\\ c_{21} & c_{22} & c_{23}\\ c_{31} & c_{32} & c_{33}\end{bmatrix}=\begin{bmatrix}1 & \gamma_1 & \gamma_1^2\\ 1 & \gamma_2 & \gamma_2^2\\ 1 & \gamma_3 & \gamma_3^2\end{bmatrix}\begin{bmatrix}m_1 & m_2 & m_3\\ m_2 & m_4 & m_5\\ m_3 & m_5 & m_6\end{bmatrix}+\begin{bmatrix}\gamma_1^3\\ \gamma_2^3\\ \gamma_3^3\end{bmatrix}\begin{bmatrix}m_7 & m_8 & m_9\end{bmatrix} \tag{2.48}$$

一般に，ストレージ $i_1,\ldots,i_k$ で復元する場合も同様にして元データの復元が可能である．

＜修復フェーズ＞

1. 以下が成り立つことに注意する：

$$mu_f=\psi_f. \tag{2.49}$$

このとき，M は対称行列なので，$M\mu_f=(\psi_f^\top M)^\top=\boldsymbol{c}_f$.
故障ノード f を $i_1,\ldots,i_d$ で修復する場合，以下の M に関する連立方程式を解けば良い：($p_{i_j,f},mu_f=\psi_f,\psi_{i_j}$ は既知，M が未知)

$$\begin{bmatrix} p_{i_1,f} \\ \vdots \\ p_{i_d,f} \end{bmatrix} = \begin{bmatrix} \psi_{i_1}^\top \\ \vdots \\ \psi_{i_d}^\top. \end{bmatrix} \boldsymbol{c}_f \tag{2.50}$$

Ψ の条件 2. からこの方程式は解ける.

例 2.6. $(n, k, d) = (6, 3, 4), B = 9$ の例を示す：

＜修復フェーズ 1 ＞

ストレージ $1, \ldots, d$ で故障ノード j を修復する場合（特に $d = 4$），以下の $\boldsymbol{c}_j = (c_{j1}, \ldots, c_{j_4})$ に関する連立方程式を解けば良い（$p_{1,j}, \ldots, p_{4,j}, \gamma_1, \ldots, \gamma_4$ は既知，$c_{j1}, \ldots, c_{j_4}$ が未知）：

$$\begin{bmatrix} p_{1,j} \\ p_{2,j} \\ p_{3,j} \\ p_{4,j} \end{bmatrix} = \begin{bmatrix} 1 & \gamma_1 & \gamma_1^2 & \gamma_1^3 \\ 1 & \gamma_2 & \gamma_2^2 & \gamma_2^3 \\ 1 & \gamma_3 & \gamma_3^2 & \gamma_3^3 \\ 1 & \gamma_4 & \gamma_4^2 & \gamma_4^3 \end{bmatrix} \begin{bmatrix} c_{j1} \\ c_{j2} \\ c_{j3} \\ c_{j4} \end{bmatrix}. \tag{2.51}$$

- $\begin{bmatrix} 1 & \gamma_1 & \gamma_1^2 & \gamma_1^3 \\ 1 & \gamma_2 & \gamma_2^2 & \gamma_2^3 \\ 1 & \gamma_3 & \gamma_3^2 & \gamma_3^3 \\ 1 & \gamma_4 & \gamma_4^2 & \gamma_4^3 \end{bmatrix}$ は正則なので，この方程式は一意に解くことができる.

一般に，ストレージ $i_1, \ldots, i_d$ で修復する場合も，同様にして故障ストレージの修復が可能である.

注意 2.27. 一般に，条件を満たす Vandermonde 行列や Cauchy 行列を用いて構成される $[n, k, d]$-再生成符号は，$[n, k, d]$-MBR 符号になる．すなわち，トレードオフ (2.36) において，$d\beta$ を最小にしたもとで，α を最小にするパラメータを持つ符号になる.

注意 2.28. 具体的な Vandermonde 行列 (2.40) の構成法としては，α を有限体 $\mathbb{F}_q$ の原始元とするとき，$\gamma_1 = \alpha, \gamma_2 = \alpha^2, \ldots, \gamma_n = \alpha^n$ とすればよい．このようにして構成される Vandermonde 行列が，2 条件を満たすためには，与えられた再生成符号のパラメータ d に対して，有限体の位数 q を $\alpha^{n(d-1)} \in \mathbb{F}_q$ を満たすように大きくとる必要がある．

2.3.6　Repair-by-Transfer 法

MBR 符号の構成法の 1 つである Repair-by-Transfer 法について説明する．Repair by Transfer は符号語シンボルのやりとりのみで復元・修復する方式である．各ストレージは修復の際に演算操作が不要であり，シンボルのやりとりだけを用いて修復することができるため，Uncoded-Repair とも呼ばれ，特に各ストレージの計算能力が低い場合に有用である．

パラメータは，$\beta = 1, \alpha = d, M = k(2d - k + 1)/2, d = n - 1$ とする．

＜符号化フェーズ＞

1. まず，元データ $\boldsymbol{m} = (m_1, \ldots, m_B)$ を $(n(n-1)/2, B)$-MDS 符号化する
   $\boldsymbol{m} \mapsto (c'_1, \ldots, c'_{n(n-1)/2}) \in \mathbb{F}_q^n$
2. 次に，n 個のストレージノードを頂点集合 V とするような完全 2 部グラフ $G = (V, E)$（E は辺集合）を描き，$n(n-1)/2$ 個の辺に，重複なく $c'_k\ k = 1, \ldots, n(n-1)/2$ 個の符号語シンボルを対応させる．辺 $(i, j) \in E$ に対応する符号語シンボルを $c'_{(i,j)}$ と表記する．
3. 各ストレージノード i の符号語シンボル $\boldsymbol{c}_i$ を以下で定める：

$$\boldsymbol{c}_i = (c'_{(i,j)} \colon \exists j : (i, j) \in E) \in \mathbb{F}_q^d \tag{2.52}$$

＜復元フェーズ＞ストレージ $i = 1, \ldots, k$ で元データを復元することを考える．

1. k 個のストレージノード $i = 1, \ldots, k$ は DC に $\boldsymbol{c}_i$ を送信
2. DC は総計 $d \times k = n - k$ 個の符号語シンボルを受信
3. 元々，$\boldsymbol{m}$ を (n, k)-MDS 符号で符号化していたので，DC は $\boldsymbol{m}$ を復元可能

＜修復フェーズ＞故障ストレージ j をストレージ $1, 2, \ldots, j-1, j+1, \ldots, n-1$ で修復することを考える.

1. 各ストレージノード i は，$p_{i \to j} = c_{(i,j)}$ をストレージ j に送信
2. ストレージ j は,

$$\hat{c}_j = (c_{(i,j)} \colon j = 1, \ldots, j-1, j+1, \ldots, n-1) \tag{2.53}$$

で修復を行う.

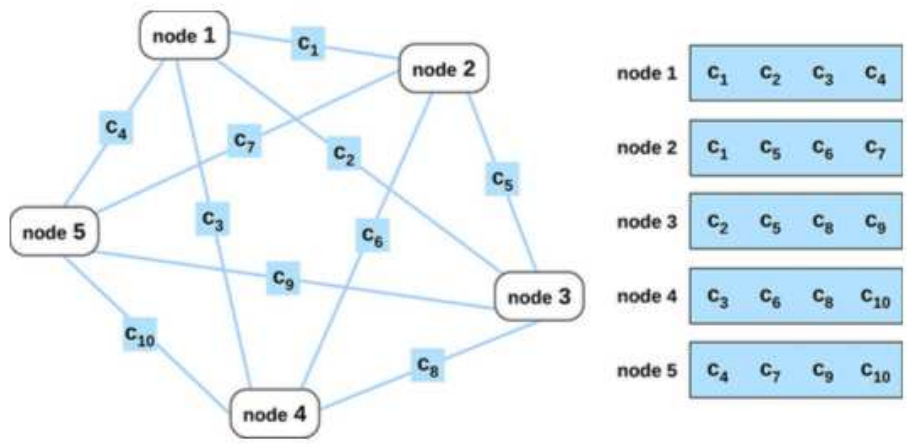

図 2.2　Repair-by-Transfer の概要図 [5]

第 3 章

一般化した再生成符号のモデルとその構成法

本章では，復元および修復に関する条件を一般化した条件 Ω を定め，条件 Ω を満たす再生成符号として，Ω-再生成符号の定義および評価基準を定めた上で，その具体的な構成法として**複数割当法**(ふくすうわりあてほう)を提案する．

まず，一般化条件 Ω をストレージのインデックスの集合族の組 $\Omega = \left(\mathcal{A}, (\mathcal{B}_j)_{j=1}^{n}\right)$ として定義し，Ω が従来の $[n, k, d]$-再生成符号における復元および修復条件を含むことを示す．ここで，

- $\mathcal{A}$ は元データを復元可能なストレージのインデックスの集合族
- $\mathcal{B}_j$ は故障ストレージ $j \in [n]$ を修復可能なストレージのインデックスの集合族

を表す．

Ω-再生成符号においては，各ストレージ i が保存する分散情報 $\boldsymbol{c}_i \in \mathbb{F}_q^{\alpha_i}$ のサイズ $\alpha_i \in \mathbb{N}$ や，故障ストレージ j へ送信する修復用データ $p_{i\to j} \in \mathbb{F}_q^{\beta_{i\to j}}$ のサイズ $\beta_{i\to j} \in \mathbb{N}$ が，ストレージごとに異なる．そこで本章では，Ω-再生成符号の評価基準として，各ストレージが保存する分散情報のサイズの平均 ρ_S および修復バンドワイズの平均 ρ_R を提案する．

Ω-再生成符号の具体的な構成法としては，従来の再生成符号の分散情報を用いた複数割当法を提案する．ここで，複数割当法とは以下のような＜符号化フェーズ＞，＜復元フェーズ＞，＜修復フェーズ＞をもつ構成法をいう：

＜符号化フェーズ＞（図 3.1, 3.2）

1. パラメータ $[\ell, t, r]$ $(\ell \geq n)$ を適当に設定し，データ $\boldsymbol{m}$ を $[\ell, t, r]$-再生成符号 F' で符号化
2. 変換された系列の成分 $\{\boldsymbol{c}'_1, \ldots, \boldsymbol{c}'_\ell\}$ の部分集合を各ノード $i = 1, \ldots, n$ に割り当てたものを符号語とする

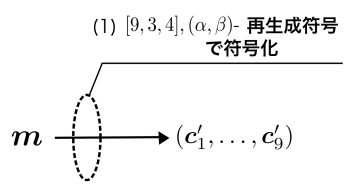

図 3.1　$n = 4, \ell = 9, t = 3, r = 4$ の例

このように構成された符号に対して，復元および修復は以下のように行われる：

＜復元フェーズ＞符号語シンボルを t 個を集め，元の $[\ell, t, r]$ 再生成符号の復号関数を用いて復元（図 3.6）

＜修復フェーズ＞修復用データを r 個集め，元の $[\ell, t, r]$ 再生成符号の修復用関数を用いて復元（図 4.1,4.2）

Ω が与えられたときに，このような復元および修復が可能であるためには，$\boldsymbol{A} \in \mathcal{A}$ に対しては，ある $[\ell, t, r]$ 再生成符号で元データを復元するのに十分な個数（i.e. t 個以上）の分散情報を割り当て，$\boldsymbol{B} \in \mathcal{B}_j$ に対しては，$[\ell, t, r]$-再生成符号において故障

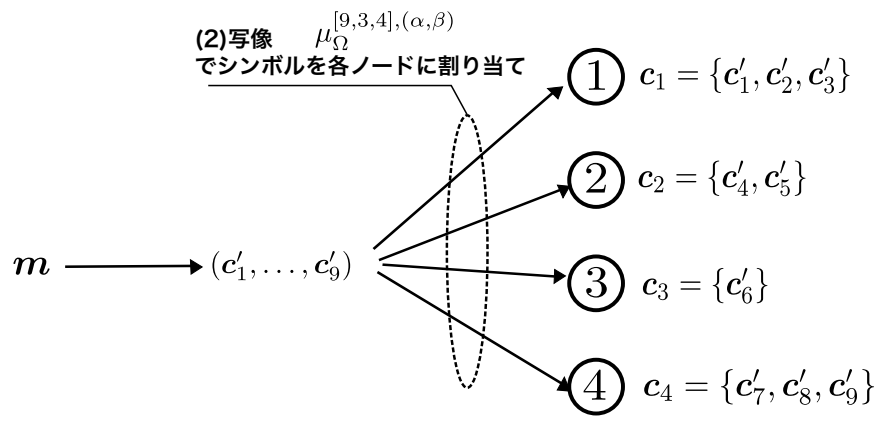

図 3.2　$n=4,\ell=9,t=3,r=4$ の例

ストレージ j を修復するのに十分な個数（i.e. r 個以上）の分散情報を割り当てればよい．ここで，復元および修復が可能であるための割当を表現する写像を複数割当写像 $\mu_\Omega^{[\ell,t,r],(\alpha,\beta)}$ と呼ぶことにすると，この写像は以下の条件を満たす必要がある．

定義 3.1 (複数割当写像)**.** $\Omega=\{\mathcal{A},\mathcal{B}\}$ を復元および再生成に関する条件とし，パラメータ $[\ell,t,r]$ を $n\le l$ かつ $t\le r\le l-1$ を満たす任意の値とする．また，分散情報のサイズ（ストレージ）が α かつ再生成情報のサイズが β の $[\ell,t,r]$-再生成符号の分散情報のなす集合を $\boldsymbol{W}^{[\ell,t,r],(\alpha,\beta)}=\left\{w_1^{[\ell,t,r],(\alpha,\beta)},\ldots,w_l^{[\ell,t,r],(\alpha,\beta)}\right\}$ とおく．このとき，以下の条件を満たす写像 $\mu_\Omega^{[\ell,t,r],(\alpha,\beta)}\colon[n]\to 2^{\boldsymbol{W}^{[\ell,t,r],(\alpha,\beta)}}$ を Ω を実現する複数割当写像と呼ぶ．

$$\left|\mu_\Omega^{[\ell,t,r],(\alpha,\beta)}(\boldsymbol{A})\right|\ge t,\qquad \boldsymbol{A}\in\mathcal{A}, \tag{3.1}$$

$$\left|\mu_\Omega^{[\ell,t,r],(\alpha,\beta)}(\boldsymbol{B})\right|\ge r,\quad \boldsymbol{B}\in\mathcal{B}_i,\ \text{for any } i\in[n]. \tag{3.2}$$

後の命題 3.11 で正確に述べるように，これらの条件 (3.1),(3.2) は，複数割当法で元データの復元や故障ノードの修復ができるための十分条件になっている．

次の命題 3.2 より，与えられた Ω を実現する複数割当写像の存在が保証される．

命題 3.2. $\Omega=\{\mathcal{A},\mathcal{B}\}$ を復元および再生成に関する条件とし，$\tilde{t}=\min_{\boldsymbol{A}\in\mathcal{A}}|\boldsymbol{A}|$, $\tilde{r}=\min_{\boldsymbol{B}\in\mathcal{B}_i,\,i\in[n]}|\boldsymbol{B}|$ とする．写像 $\mu_\Omega^{[n,\tilde{t},\tilde{r}],(\alpha,\beta)}$ を

$$\mu_{\Omega}^{[n,\tilde{t},\tilde{r}],(\alpha,\beta)}(i) = \{w_i^{[n,\tilde{t},\tilde{r}],(\alpha,\beta)}\}, \quad \text{for any } i \in [n] \tag{3.3}$$

によって定めると，この写像は複数割当写像である．

証明 写像 $\mu_{\Omega}^{[n,\tilde{t},\tilde{r}],(\alpha,\beta)}$ が複数割当写像の条件を満たすことは次のように確かめられる．任意の $\boldsymbol{A} \in \mathcal{A}$ に対して，$|\boldsymbol{A}| \geq \tilde{t}$ であるので，不等式 (3.1) を満たす．同様に，各 $i \in [n]$ と任意の $\boldsymbol{B} \in \mathcal{B}_i$ に対して，$|\boldsymbol{B}| \geq \tilde{r}$ が成り立つので不等式 (3.2) を満たす．
■

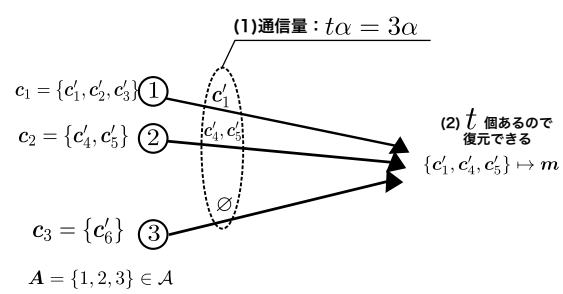

図 3.3　複数割当法における元データ復元 ($n = 4, \ell = 9, t = 3$)

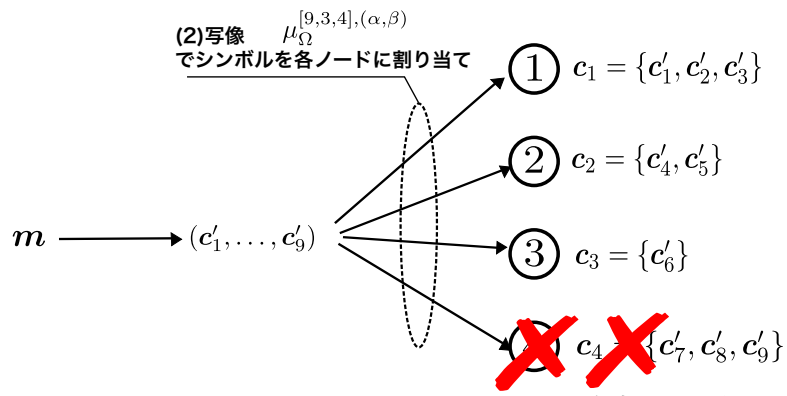

図 3.4　ストレージノード 4 が故障した場合

本章ではさらに，複数割当法による符号クラスの中で

- ρ_S を最小にしたもとで ρ_R を最小にする符号（Ω-MSR-map 符号）

および

- ρ_R を最小にしたもとで ρ_S を最小にする符号（Ω-MBR-map 符号）

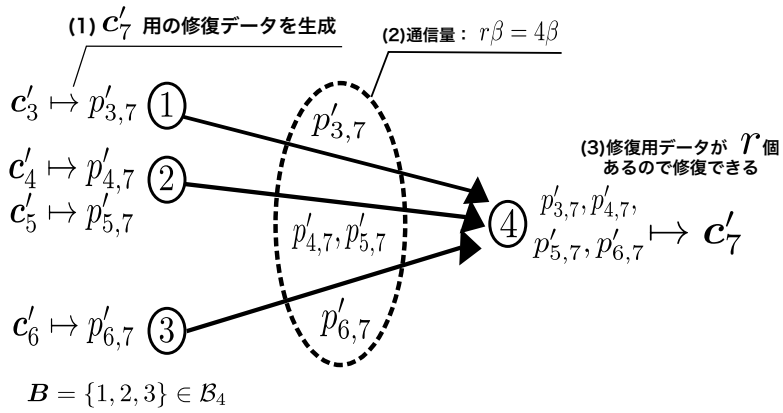

図 3.5　ノード 4 の修復 ($n = 4, \ell = 9, r = 4$)

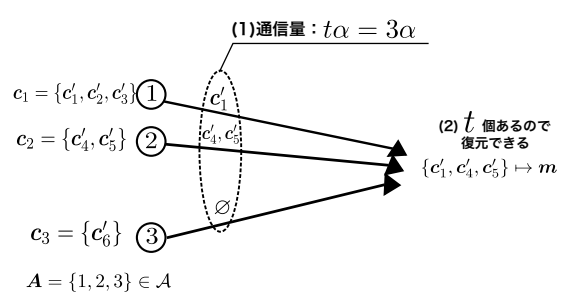

図 3.6　複数割当法における元データ復元 ($n = 4, \ell = 9, t = 3$)

を定義し，整数計画法を用いた探索による構成アルゴリズムを導出する．ここで，最適化すべきパラメータは

- (α, β)
- $[\ell, t, r]$
- $\mu_{\Omega}^{[\ell,t,r]}, (\alpha, \beta)$

である．続く 3.2.2 節において，これらの内，(α, β) および ℓ f および $\mu_{\Omega}^{[\ell,t,r]}, (\alpha, \beta)$ については，探索せずに最適な値が決定できることを示す．残る t, r については，整数計画問題を効率的に繰り返し解くことで探索するアルゴリズムを提案する．

3.1　復元および再生成の条件を一般化した再生成符号のモデル

本節では，復元および再生成の条件を一般化した再生成符号のモデルを提案する．

3.1.1　Ω-DSS と Ω-再生成符号の定義 [2]

ノード集合 $[n] = \{1, \ldots, n\}$ の族 $\mathcal{A} \subseteq 2^{[n]}$ を，データコレクタ DC が元データ $\boldsymbol{m}$ を復元可能なノード集合の族とする．また $\mathcal{B}_i \subseteq 2^{[n]\setminus\{i\}}, i \in [n]$ を，故障ノード i の分散情報を再生成可能なノード集合の族とする．$\mathcal{A}, \mathcal{B}_1, \ldots, \mathcal{B}_n$ は任意に与えられているとする．以降，$\mathcal{A}$ を復元に関する条件と呼び，$\mathcal{B} = (\mathcal{B}_1, \ldots, \mathcal{B}_n)$ を再生成に関する条件と呼ぶ．さらに，これらのなす集合を $\Omega = \{\mathcal{A}, \mathcal{B}\}$ と記す．

このとき，以下のように Ω-DSS および Ω-再生成符号を定義する．

定義 3.3. 次の 3 つのフェーズから構成される方式を Ω-DSS と呼ぶ．

＜分散情報生成フェーズ＞　管理者は，符号化関数 $F\colon \mathbb{F}_q^M \to \prod_{i=1}^n \mathbb{F}_q^{\alpha_i}$ を用いて元データ $\boldsymbol{m} \in \mathbb{F}_q^M$ に対する n 個の分散情報 $F(\boldsymbol{m}) = (w_1, \ldots, w_n)$, $w_i \in \mathbb{F}_q^{\alpha_i}, i \in [n]$ を生成する．次に，安全な通信路を用いて各 w_i をノード i に送信する．ノード i は受信した分散情報 w_i をそれぞれ保管する．ここで，$\alpha_i \in \mathbb{N}$ は各ノード i の分散情報のサイズとし，i のストレージと呼ぶ．

＜元データ復元フェーズ＞　データコレクタ DC はノード集合 $\boldsymbol{A} \in \mathcal{A}$ を選択し，各ノードが保管している分散情報を受信する．DC は，復号関数 $G\colon \prod_{j=1}^{|\boldsymbol{A}|} \mathbb{F}_q^{\alpha_{i_j}} \to \mathbb{F}_q^M$ を用いて，元データ $\boldsymbol{m} = G(w_{\boldsymbol{A}}) \in \mathbb{F}_q^M$ を復元する．

＜再生成フェーズ＞　故障ノード i の分散情報の再生成をする際にはまず，新規ノード i を用意する．その新規ノードはノード集合 $\boldsymbol{B} \in \mathcal{B}_i$ を選択する．次に，選択されたノード集合の各ノード i_j, $j = 1, \ldots, |\boldsymbol{B}|$ は，保管している分散情報と関数 $f_i\colon \mathbb{F}_q^{\alpha_{i_j}} \times \mathcal{B}_i \to \mathbb{F}_q^{\beta_{i,i_j}}$ を用いて，再生成情報 $v_{i,i_j}^{\boldsymbol{B}} = f_i(w_{i_j}, \boldsymbol{B}) \in \mathbb{F}_q^{\beta_{i,i_j}}$, $j = 1, \ldots, |\boldsymbol{B}|$ をそれぞれ生成する．ここで，$\beta_{i,i_j} \in \mathbb{N}$ は再生成情報のサイズを表す．これら $|\boldsymbol{B}|$ 個の再生成情報は，新規ノード i に送信され，新規ノードは関数 $g_i\colon \prod_{j=1}^{|\boldsymbol{B}|} \mathbb{F}_q^{\beta_{i,i_j}} \times \mathcal{B}_i \to \mathbb{F}_q^{\alpha_i}$ を用いて，分散情報 $\hat{w}_i = g_i(v_{i,i_1}^{\boldsymbol{B}}, \ldots, v_{i,i_{|\boldsymbol{B}|}}^{\boldsymbol{B}}, \boldsymbol{B}) \in \mathbb{F}_q^{\alpha_i}$ を生成する．このとき，$\hat{w}_i \neq w_i$ であってもよいが，再生成後の $\hat{w}_i$ を用いたノード $i \in \boldsymbol{A} \in \mathcal{A}$ による元データ復元およびノード $i \in \boldsymbol{B} \in \mathcal{B}_j$ によるノード $j \in [n] \setminus \{i\}$ の分散情報の再生成は可能でなければならない．

定義 3.4. Ω-DSS における関数の組 $(F, G, (f_i, g_i)_{i=1}^n)$ を Ω-再生成符号と呼ぶ．

例 3.1. $[n, k, d]$-再生成符号においては，$\alpha_i = \alpha$, $\beta_{i,i_j} = \beta$ であり，復元および再生成に関する条件 $\Omega = \{\mathcal{A}, \mathcal{B}\}$ は以下のように表される：

$$\mathcal{A} = \left\{ \boldsymbol{A} \in 2^{[n]} : |\boldsymbol{A}| \geq k \right\}, \tag{3.4}$$

$$\mathcal{B}_i = \left\{ \boldsymbol{B} \in 2^{[n]\setminus\{i\}} : |\boldsymbol{B}| \geq d \right\}, \quad \text{for any } i \in [n]. \tag{3.5}$$

このとき，$[n, k, d]$-再生成符号における復元および再生成に関する条件を表す集合族 (3.4),(3.5) に関して，$k \leq d$ より，

$$\mathcal{B}_i \subseteq \mathcal{A}, \qquad \text{for any } i \in [n] \tag{3.6}$$

が成り立っている（$\boldsymbol{C} \in \mathcal{B}_i$ とすると，$|\boldsymbol{C}| \geq d \geq k$ だから，$\boldsymbol{C} \in \mathcal{A}$ が成り立つ）.

この性質は，故障ノードの符号語を再生成可能なノード集合は，元の元データの復元能力を有することを意味している.

さらに，明らかに以下が成り立つ：

$$\boldsymbol{A} \subseteq \boldsymbol{A}' \text{ and } \boldsymbol{A} \in \mathcal{A} \Longrightarrow \boldsymbol{A}' \in \mathcal{A}, \tag{3.7}$$

$$\boldsymbol{B} \subseteq \boldsymbol{B}' \text{ and } \boldsymbol{B} \in \mathcal{B}_i \Longrightarrow \boldsymbol{B}' \in \mathcal{B}_i, \quad \text{for any } i \in [n]. \tag{3.8}$$

この条件は Γ-SSS における条件式 (2.26) に対応する．すなわち，$\boldsymbol{m}$ を復元可能なノード集合を包含するノード集合もまた $\boldsymbol{m}$ を復元でき，ノード i の分散情報を再生成可能なノード集合を包含するノード集合もまたノード i の分散情報を再生成可能であるという条件である．したがって，2.2 節と同様，極小有資格集合 $\mathcal{A}^-, \mathcal{B}_i^-$ が定義される.

これらの条件は，後に，3.2.2.2 節において，最適化パラメータの効率的な探索を行う際に有用であるため，一般的な条件 Ω に対しても，これらの性質が成り立つことを仮定する.

仮定 3.5. 復元および再生成に関する条件 $\Omega = \{\mathcal{A}, \mathcal{B}\}$ は以下を満たすとする：

$$\mathcal{B}_i \subseteq \mathcal{A}, \qquad \text{for any } i \in [n]. \tag{3.9}$$

仮定 3.6 (単調性条件)**.** $\Omega = \{\mathcal{A}, \mathcal{B}\}$ は以下を満たすとする：

$$\boldsymbol{A} \subseteq \boldsymbol{A}' \text{ and } \boldsymbol{A} \in \mathcal{A} \Longrightarrow \boldsymbol{A}' \in \mathcal{A}, \tag{3.10}$$

$$\boldsymbol{B} \subseteq \boldsymbol{B}' \text{ and } \boldsymbol{B} \in \mathcal{B}_i \Longrightarrow \boldsymbol{B}' \in \mathcal{B}_i, \quad \text{for any } i \in [n]. \tag{3.11}$$

これらの条件は $[n, k, d]$-再生成符号も満たすので，次が言える．

命題 3.7. 条件式 (3.9),(3.10), (3.11) のもとで，Ω-再生成符号のクラスは従来の $[n, k, d]$-再生成符号のクラスを含む．

3.1.2　Ω-再生成符号の評価基準と Ω-MSR/MBR 符号

一般化した条件 $\Omega = \{\mathcal{A}, \mathcal{B}\}$ の下での再生成符号における効率性に関する評価基準を，以下のように定義する．

定義 3.8. ストレージ平均 ρ_S および修復バンドワイズ平均 ρ_R を以下で定義する：

$$\rho_S := \frac{1}{n} \sum_{i=1}^{n} \alpha_i, \tag{3.12}$$

$$\rho_R := \frac{1}{n} \sum_{i=1}^{n} \min_{\boldsymbol{B} \in \mathcal{B}_i^-} \sum_{i_j \in \boldsymbol{B}} \beta_{i,i_j}. \tag{3.13}$$

注意 3.9. 修復バンドワイズに関する評価基準としては，式 (3.13) 以外にも，各 i に対して $\mathcal{B}_i$ 全体で平均をとる次の量

$$\rho_R := \frac{1}{n} \sum_{i=1}^{n} \frac{1}{|\mathcal{B}_i|} \sum_{\boldsymbol{B} \in \mathcal{B}_i} \sum_{i_j \in \boldsymbol{B}} \beta_{i,i_j} \tag{3.14}$$

を採用することも考えられるが，本論文で提案する複数割当法による構成法においては，両者の値は一致する（詳細は注意 4.3 で後述する）．

以上の評価基準を用いて，復元および再生成に関する条件を一般化したモデルにおける MSR 符号を定義する．

定義 3.10 (Ω-MSR/MBR 符号)**.** $\Omega = \{\mathcal{A}, \mathcal{B}\}$ を復元および再生成に関する条件とする．このとき，ストレージ平均 ρ_S を最小にした下で，修復バンドワイズ平均 ρ_R を

最小にする再生成符号を Ω-MSR 符号と定義する．

同様に，修復バンドワイズ平均 ρ_R を最小にした下で，ストレージ平均 ρ_S を最小にする再生成符号を Ω-MBR 符号と定義する．

3.2　復元および再生成の条件を一般化した再生成符号の構成法

与えられた条件 $\Omega = \left(\mathcal{A}, (\mathcal{B}_i)_{i=1}^n\right)$ に，仮定 3.5 と仮定 3.6 以外の仮定をおかない場合，トレードオフの解析等は困難である．したがって，Ω-MSR/MBR 符号を任意の Ω に対して効率的に構成するアルゴリズムを導出することもまた困難である．一般化に関する従来研究が行なわれている Γ-秘密分散法も同様の困難さを抱えている．

そこで本節では，Γ-SSS の構成法と同様に，与えられた一般化条件 Ω を実現する再生成符号として，

- まず，従来の再生成符号の分散情報を用いた複数割当法を提案し，
- そのうえで，複数割当法による再生成符号のクラスの中で最適な構成法（複数割当法）の提案

を行う．

最適性に関しては，具体的には，その構成による符号クラスの中で

- ストレージ平均を小さくした下で修復バンドワイズ平均を小さくする符号

および

- 修復バンドワイズ平均を小さくした下でストレージ平均を小さくする符号

の構成法を提案する．

3.2.1　複数割当法を用いた Ω-再生成符号の構成法

3.2.1.1　Ω-再生成符号の構成法（複数割当法）

本節では Ω-再生成符号である複数割当法のプロトコルを以下に示し，復元および修復に関する通信量について述べる．

＜分散情報生成フェーズ＞

まず, 元データ $\boldsymbol{m}$ を $[\ell, t, r]$-再生成符号で符号化する ($n \leq l$, $t \leq r \leq l-1$)．次に, 複数割当写像 $\mu_{\Omega}^{[\ell,t,r],(\alpha,\beta)}$ を用いて, 符号化関数 $F(\boldsymbol{m}) = \left(\mu_{\Omega}^{[\ell,t,r],(\alpha,\beta)}(1), \ldots, \mu_{\Omega}^{[\ell,t,r],(\alpha,\beta)}(n)\right)$ で元データ $\boldsymbol{m}$ を符号化する．

＜元データ復元フェーズ＞

復号関数 G を $[\ell, t, r]$-再生成符号における復号関数とすると，データコレクタ DC は以下のようにしてノード集合 $\boldsymbol{A} \in \mathcal{A}$ によって元データ $\boldsymbol{m}$ を復元できる：

1. DC は，ノード $i_j \in \boldsymbol{A}$, $j = 1, \ldots, |\boldsymbol{A}|$ に接続
2. DC は，各ノード i_j から総計 t 個の $[\ell, t, r]$-再生成符号の分散情報を受信
3. DC は，t 個の分散情報と $[\ell, t, r]$-再生成符号の復号関数 G から $\boldsymbol{m}$ を復元

＜再生成フェーズ＞（自明な方式）

故障ノード i の修復が行えることを示す．ノード i に保管されていた $[\ell, t, r]$-再生成符号の分散情報の個数を $x_i = \left|\mu_{\Omega}^{[\ell,t,r],(\alpha,\beta)}(i)\right|$ とする．このとき，ノード集合 $\boldsymbol{B} \in \mathcal{B}_i$ によって x_i 個の分散情報を再生成する自明な方式として，以下の方法が考えられる：

1. 新規ノード i を用意し，新規ノード i が $i_j \in \boldsymbol{B}$ に接続
2. i は，各ノード i_j から総計 t 個の $[\ell, t, r]$-再生成符号の分散情報を受信
3. i は，t 個の分散情報と $[\ell, t, r]$-再生成符号の復号関数から $\boldsymbol{m}$ を復元し，$\boldsymbol{m}$ と $[\ell, t, r]$-再生成符号の符号化関数を用いて x_i 個の分散情報を再生成

<再生成フェーズ＞（効率的な方式）この方式による通信量は $t\alpha$ であるが，$[\ell, t, r]$-再生成符号の性質を使うことで，以下のようにより効率的な修復が可能である．

ノード i に保管されていた $[\ell,t,r]$-再生成符号の分散情報の個数を $x_i = \left|\mu_{\Omega}^{[\ell,t,r],(\alpha,\beta)}(i)\right|$ とする．このとき，以下の手順で故障ノード i の修復を行う．

1. 新規ノード i を用意し，新規ノード i が $i_j \in \boldsymbol{B}$, $j = 1,\ldots,|\boldsymbol{B}|$ に接続
2. i は，各ノード i_j から 1 個目の分散情報を再生成するための，総計 r 個の再生成情報を受信
3. i は，r 個の再生成情報と $[\ell,t,r]$-再生成符号における修復用の関数を用いて，1 個目の分散情報を再生成
4. 以上の操作を x_i 個の分散情報が再生成されるまで繰り返す

この方式による通信量は $r\beta \times x_i$ である．

命題 3.11. 以上の構成法によって，元データの復元および故障ノードの再生成が可能である．

証明 ＜元データ復元フェーズ＞：複数割当写像における条件 (3.1) より，ステップ 2. において，DC は確実に t 個の分散情報を得ることができる．したがって，元データ $\boldsymbol{m}$ は $[\ell,t,r]$-再生成符号で符号化されているため，これら t 個の分散情報から，$\boldsymbol{m}$ を復元することができる．

＜再生成フェーズ＞（自明な方式）は明らか．（効率的な方式）については，複数割当写像の条件 (3.2) から，ステップ 2. において，各ノード $i_j, j \in B$ から確実に r 個の分散情報を，故障ノードに送信することができる．したがって，$[\ell,t,r]$-再生成符号の性質から，1 個目の分散情報を再生成できる．のこりの分散情報についても同様． ■

注意 3.12. 複数割当法における元データ復元フェーズおよび再生成フェーズでは，$[\ell,t,r]$-再生成符号の符号化関数，復号関数および再生成用の関数を用いているが，これらが必ずしも最適である（ρ_S や ρ_R を最小にする）とは限らない．しかしながら，解析や実装が容易であるという利点を持つ．

注意 3.13. 各ノードが保管する分散情報の個数 $x_i = \left|\mu_{\Omega}^{[\ell,t,r],(\alpha,\beta)}(i)\right|$ に関して，本論文では与えられた条件 $\Omega = \{\mathcal{A},\mathcal{B}\}$ によっては，$x_i = 0$ であることを許している．また，$x_i > r$ のときは，r 個の分散情報を再生成後は，既に再生成した r 個の分散情

報を用いることにより，追加の通信をすることなく残りの分散情報を再生成できる．したがって，各ノード i に対して r 個より多くの分散情報を割り当てる必要はないので，以降では $x_i \leq r$ の場合のみを考える．

3.2.2　Ω-MSR-map 符号/Ω-MBR-map 符号とその構成法

本節では，分散情報生成フェーズにおいて適当な $[\ell, t, r]$-再生成符号および複数割当写像 $\mu_{\Omega}^{[\ell,t,r],(\alpha,\beta)}$ を求めることにより，前節で示した構成法（複数割当法）による符号クラスの中で

- ストレージ平均を最小にし，その下で修復バンドワイズ平均を最小にする Ω-再生成符号（Ω-MSR-map 符号）

および

- 修復バンドワイズ平均を最小にし，その下でストレージ平均を最小にする Ω-再生成符号（Ω-MBR-map 符号）

の構成法を提案する．ここで，元データ復元フェーズおよび再生成フェーズにおいては，前節と同様に $[\ell, t, r]$-再生成符号の復号関数や再生成用の関数を用いるものとする．

3.2.2.1　Ω-MSR/MBR-map 符号の定義と性質

本節では，Ω-MSR-map/MBR-map 符号の定義と性質を述べる．

定義 3.14 (Ω-MSR/MBR-map 符号)**.** $\Omega = \{\mathcal{A}, \mathcal{B}\}$ を復元および再生成に関する条件とし，$\mu_{\Omega}^{[\ell,t,r],(\alpha,\beta)}$ を Ω-再生成符号を構成する複数割当写像とする．このとき，複数割当法による Ω-再生成符号のクラスの中で最小のストレージ平均をもち，その条件の下で最小のバンドワイズ平均をもつ符号を Ω-MSR-map 符号と定義する．Ω-MSR-map 符号のストレージ平均およびバンドワイズ平均をそれぞれ $\rho_{S_{\text{MSR-map}}}, \rho_{R_{\text{MSR-map}}}$ と記す．

注意 3.15. 注意 2.20 と同様に，Ω-MSR-map 符号は必ずしも Ω-MSR 符号にはならない．

次に，Ω-MSR-map 符号を構成するためには，複数割当写像で割り当てる分散情報としては，MSR 符号の分散情報を用いればよいことを示す．

命題 3.16. $\Omega = \{\mathcal{A}, \mathcal{B}\}$ を復元および再生成に関する条件とし，$\mu_\Omega^{[\ell,t,r],(\alpha,\beta)}$ を Ω に対する複数割当写像とする．このとき，任意の l, t, r, α, β に対して $\mu_\Omega^{[\ell,t,r],(\alpha,\beta)}$ による再生成符号が Ω-MSR-map 符号になるための十分条件は，$[\ell, t, r]$-再生成符号が MSR 符号であること，すなわち，

$$\alpha = \alpha_{\mathrm{MSR}} = \frac{B}{t}, \tag{3.15}$$

$$\beta = \beta_{\mathrm{MSR}} = \frac{B}{t(r-t+1)} \tag{3.16}$$

が成り立つことである．同様に，$\mu_\Omega^{[\ell,t,r],(\alpha,\beta)}$ による再生成符号が Ω-MBR-map 符号になるための十分条件は，$[\ell, t, r]$-再生成符号が MBR 符号であること，すなわち，

$$\alpha = \alpha_{\mathrm{MBR}} = \frac{2rB}{t(2r-t+1)}, \tag{3.17}$$

$$\beta = \beta_{\mathrm{MBR}} = \frac{2B}{t(2r-t+1)} \tag{3.18}$$

が成り立つことである．

証明 $[\ell, t, r]$-MSR 符号および $[\ell, t, r]$-MBR 符号の定義と，Ω-再生成符号の構成法から明らか． ■

3.2.2.2　Ω-MSR-map 符号の構成アルゴリズム

以降，$\mu_\Omega^{[\ell,t,r],(\alpha_{\mathrm{MSR}},\beta_{\mathrm{MSR}})}$ を $\mu_\Omega^{[\ell,t,r]}$ と略記する．複数割当写像 $\mu_\Omega^{[\ell,t,r]}$ により構成された符号のストレージ平均 ρ_S および修復バンドワイズ平均 ρ_R は，$x_i = \left|\mu_\Omega^{[\ell,t,r]}(i)\right|$ とするとき，それぞれ以下で与えられる：

$$\rho_S = \frac{1}{n}\sum_{i=1}^{n}\left|\mu_\Omega^{[\ell,t,r]}(i)\right| \times \frac{M}{t} \tag{3.19}$$

$$= \frac{1}{n}\cdot\frac{M}{t}\sum_{i=1}^{n} x_i, \tag{3.20}$$

$$\rho_R = \frac{1}{n}\sum_{i=1}^{n}\left|\mu_\Omega^{[\ell,t,r]}(i)\right| \times r \times \frac{M}{t(r-t+1)} \tag{3.21}$$

$$= \frac{1}{n}\cdot\frac{rM}{t(r-t+1)}\sum_{i=1}^{n} x_i, \tag{3.22}$$

ここで，$x_i := \left|\mu_\Omega^{[\ell,t,r]}(i)\right|$ とおいた．

本節では，Ω-MSR-map 符号の構成法として，次の整数計画問題 $\mathrm{IP}_{\Omega,S}(t)$ を繰り返し解くアルゴリズムを導出する．

$$\begin{aligned}\mathrm{IP}_{\Omega,S}(t):&\\ \text{minimize}\quad & \sum_{i=1}^{n} x_i,\\ \text{subject to}\quad & \sum_{i\in\boldsymbol{A}} x_i \geq t, \quad \boldsymbol{A}\in\mathcal{A}^{-}.\end{aligned} \tag{3.23}$$

ここで，$\alpha_{\mathrm{MSR}} = M/t \geq 1$ であることに注意する．整数計画問題 $\mathrm{IP}_{\Omega,S}(t)$ の最適解のなす集合を $\boldsymbol{X}(t)$，最適解を $\boldsymbol{x}(t) = (x_1,\ldots,x_n) \in \boldsymbol{X}(t)$ とおき，最適値を $l(t) = \sum_{i=1}^{n} x_i$ とおく．また，このときのストレージ平均を $\rho_S(t)$ とおく．すなわち，

$$\rho_S(t) = \frac{B}{nt} \times l(t) \tag{3.24}$$

である．さらに，$M/t \geq 1$ を満たす t の中で $\rho_S(t)$ の最小値を与える t の集合を T とおく．すなわち，

$$T = \left\{ t \;\middle|\; \rho_S(t) = \min_{u:\, M/u\geq 1} \rho_S(u) \right\} \tag{3.25}$$

である．また，t を固定したときの修復バンドワイズ平均の式 (4.16) を $\rho_R(r)$ とおく．

整数計画問題 $\mathrm{IP}_{\Omega,S}(t)$ の解に対して，$\boldsymbol{B} \in \mathcal{B}_i$ に関する制約条件 $\sum_{j\in\boldsymbol{B}} x_j \geq r$ については，仮定 (3.9) により $r = t$ のときは自明に成り立つ．つまり，$\mathrm{IP}_{\Omega,S}(t)$ に制約条

件 $\sum_{j\in\boldsymbol{B}} x_j \geq t$ を加えた問題の解集合は元の問題 $\mathrm{IP}_{\Omega,S}(t)$ の解集合に一致する．さらに，$r > t$ のときは，制約条件 $\sum_{j\in\boldsymbol{B}} x_j \geq r$ を $\mathrm{IP}_{\Omega,S}(t)$ に加えた問題の解集合は，元の問題 $\mathrm{IP}_{\Omega,S}(t)$ の解集合に含まれる．したがって，Ω-MSR-map 符号を構成するには，まず整数計画問題 $\mathrm{IP}_{\Omega,S}(t)$ を $M/t \geq 1$ を満たすすべての t について解いて T を求め，その後で各 $t \in T$ に対して $\rho_R(r)$ を最小にする解を探索すればよい．

そこで，$t \in T$ の中で $\rho_R(r) = \rho_R(r(t))$ を最小にするものを t^* とおく．すなわち，

$$t^* = \operatorname*{argmin}_{t\in T} \rho_R(r(t)), \tag{3.26}$$

とする．

さらに，$l^* = l(t^*), r^* = r(t^*), \boldsymbol{x}^* = \operatorname{argmin}_{\boldsymbol{x}(t^*)\in\boldsymbol{X}(t^*)} r(t^*)$ とおくと，Ω-MSR-map 符号の構成法は Algorithm 1 で与えられる．

Algorithm 1 Construciton of Ω-MSR-map codes

Require: $\boldsymbol{m}, n, B, \Omega = \{\mathcal{A}, \mathcal{B}\}$

Ensure: $\left(\mu_\Omega^{[l^*,t^*,r^*]}(1), \ldots, \mu_\Omega^{[l^*,t^*,r^*]}(n)\right)$

1: $t \leftarrow 1$
2: **while** $B/t \geq 1$ **do**
3:　　solve $\mathrm{IP}_{\Omega,S}(t)$
4:　　$t \leftarrow t + 1$
5: **end while**
6: calculate $\min_{u:\ B/u\geq 1} \rho_S(u)$
7: calculate T by (3.25)
8: calculate t^*, l^*, r^* and $\boldsymbol{x}^*$ by (3.26)
9: calculate the multiple assignment map $\mu_\Omega^{[l^*,t^*,r^*]}$
10: encode $\boldsymbol{m}$ to $\left(\mu_\Omega^{[l^*,t^*,r^*]}(1), \ldots, \mu_\Omega^{[l^*,t^*,r^*]}(n)\right)$

以上の議論により，次が成り立つ．

定理 3.17. $\Omega = \{\mathcal{A}, \mathcal{B}\}$ を復元および再生成に関する条件とするとき，Algorithm 1 は，Ω-MSR-map 符号を構成するアルゴリズムである．

3.2.2.3　Ω-MBR-map 符号の構成アルゴリズム

以降，$\mu_\Omega^{[\ell,t,r]} = \mu_\Omega^{[\ell,t,r],(\alpha_{\mathrm{MBR}},\beta_{\mathrm{MBR}})}$ と略記する．このとき，ストレージの平均 ρ_S および修復バンドワイズの平均 ρ_R はそれぞれ以下で与えられる：

$$\rho_S = \rho_R \tag{3.27}$$

$$= \frac{1}{n}\sum_{i=1}^{n}\left|\mu_\Omega^{[\ell,t,r]}(i)\right| \times r \times \frac{2B}{t(2r-t+1)} \tag{3.28}$$

$$= \frac{1}{n}\cdot\frac{2rB}{t(2r-t+1)}\sum_{i=1}^{n} x_i \tag{3.29}$$

以下，Ω-MBR-map 符号の構成法として，次の整数計画法 $\mathrm{IP}_\Omega(t,r)$ を繰り返し解くアルゴリズムを導出する．

$$\begin{aligned}
&\mathrm{IP}_\Omega(t,r):\\
&\qquad\text{minimize} \quad \sum_{i=1}^{n} x_i,\\
&\qquad\text{subject to} \quad \sum_{i\in\boldsymbol{A}} x_i \geq t, \qquad \boldsymbol{A}\in\mathcal{A}^-,\\
&\qquad\qquad\qquad\quad \sum_{i\in\boldsymbol{B}} x_i \geq r, \quad \boldsymbol{B}\in\mathcal{B}_i^-, i\in[n].
\end{aligned} \tag{3.30}$$

ここで，$2M/t(2r-t+1) \geq 1$ であることに注意する．整数計画問題 $\mathrm{IP}_\Omega(t,r)$ の最適解および最適解のなす集合をそれぞれ $\boldsymbol{x}(t,r), \boldsymbol{X}(t,r)$ とおき，最適値を $l(t,r) = \sum_{i=1}^{n} x_i$ とおく．

注意 3.18. MBR-map 符号を構成するには，$2B/t(2r-t+1) \geq 1$ を満たすすべての (t,r) について整数計画問題 $\mathrm{IP}_\Omega(t,r)$ を解く必要があるが，r については探索範囲を狭められることを示す．

$$\rho_R(t,r) = \frac{2l(t,r)rB}{nt(2r-t+1)}, \tag{3.31}$$

$$f(r) = \frac{2r^2B}{nt(2r-t+1)} \tag{3.32}$$

とおくと，$f(r)$ は $0 < r < 2(t-1)$ で単調減少関数であり，一方，$r \geq 2(t-1)$ では単調増加関数である．さらに，整数計画問題 $\mathrm{IP}_\Omega(t,r)$ の最適解 $\boldsymbol{x}(t,r)$ は $\sum_{i=1}^{n} x_i \geq r$ を満たすので,

$$\rho_R(t,r) \geq f(r) \tag{3.33}$$

が成り立つ．ここで各 t に対して，r に関する方程式

$$f(r) = \rho_R(t,t) \tag{3.34}$$

の解を $T(t)$ とおくと，r については $t \leq r \leq T(t)$ の範囲を探索すればよいことがわかる．

したがって,

$$(t^*, r^*) = \underset{\substack{(t,r):2B/t(2r-t+1)\geq 1,\\ t\leq r\leq \lceil T(t)\rceil}}{\operatorname{argmin}} \rho_R(t,r) \tag{3.35}$$

とおき，$l^* = l(t^*, r^*), \boldsymbol{x}^* = \boldsymbol{x}(t^*, r^*)$ とおくと，MBR-map 符号の構成法は Algorithm 2 で与えられる．

Algorithm 2 Construciton of Ω-MBR-map codes

Require: $\boldsymbol{m}, n, B, \Omega = \{\mathcal{A}, \mathcal{B}\}$

Ensure: $\left(\mu_\Omega^{[l^*,t^*,r^*]}(1), \ldots, \mu_\Omega^{[l^*,t^*,r^*]}(n)\right)$

$t \leftarrow 1, r \leftarrow 1$
while $2B/t(2r - t + 1) \geq 1$ **do**
  $r \leftarrow t$
  calculate $T(t)$ by solving (3.34)
  while $r \leq \lceil T(t) \rceil$ **do**
    solve $\mathrm{IP}_\Omega(t, r)$
    calculate $\rho_R(t, r)$
    $r \leftarrow r + 1$
  end while
  $t \leftarrow t + 1$
end while
calculate t^*, l^*, r^* and $\boldsymbol{x}^*$ by (3.35)
calculate the multiple assignment map $\mu_\Omega^{[l^*,t^*,r^*]}$
encode $\boldsymbol{m}$ to $\left(\mu_\Omega^{[l^*,t^*,r^*]}(1), \ldots, \mu_\Omega^{[l^*,t^*,r^*]}(n)\right)$

定理 3.19. $\Omega = \{\mathcal{A}, \mathcal{B}\}$ を復元および再生成に関する条件とするとき，Algorithm 2 は，Ω-MBR-map 符号を構成するアルゴリズムである．

注意 3.20. $[\ell, t, r]$-MBR-再生成符号として，Shah らの Repair-by-Transfer 法 [5] を用いれば，本提案における Ω-MBR-map 符号もまた Uncoded-Repair の性質をもつ．

第 4 章

再生成フェーズの改良

Ω-再生成符号は Γ-秘密分散法と異なり故障ノードの修復条件を一般化しているため，故障ストレージの修復法に関して工夫の余地がある．そこで本章では，複数割当法を用いた場合の，通信量の意味でより効率的な修復法を提案し，その効率性について解析を行う．また，その修復法を用いた場合の Ω-MSR/MBR-map 符号の構成法についても考え，Ω-MSR-map 符号については上述と同様の構成法が導出できることを示す．一方，Ω-MBR-map 符号については，割り当てる再生成符号における最適なパラメータ (α, β) が決定できないため，準最適な構成法を提案する．

4.1 より効率的な再生成フェーズの提案

前章で提案した方式による 1 つのノードの修復に必要な通信量は $r\beta \times x_i$ であるが，ノード i に割当られている分散情報の個数 x_i によっては，より少ない通信量で故障ノード i の分散情報の再生成が可能である．

＜再生成フェーズ＞（より効率的な方式）

1. 新規ノード i を用意し，新規ノード i が $i_j \in \boldsymbol{B}$, $j = 1, \ldots, |\boldsymbol{B}|$ に接続
2. i は，各ノード i_j から 1 個目の分散情報を再生成するための，総計 r 個の再生成情報を受信
3. i は，r 個の再生成情報と $[\ell, t, r]$-再生成符号における再生成用の関数を用いて，1 個目の分散情報を再生成

4. 次に，i は各ノード i_j から 2 個目の分散情報を再生成するための総計 $r-1$ 個の再生成情報を受信
5. i は (3) で再生成した 1 個目の分散情報から 2 個目の分散情報を再生成するための再生成情報を生成
6. i は (4) で受信した $r-1$ 個の再生成情報と (5) で生成した再生成情報から $[\ell, t, r]$-再生成符号における再生成用の関数を用いて，2 個目の分散情報を再生成
7. 以上の操作を x_i 個の分散情報が再生成されるまで繰り返す

この方式による通信量は $r\beta + (r-1)\beta + \cdots + (r-x_i+1)\beta = x_i(2r+1-x_i)\beta/2$ である．したがって，故障ノード i に保管されていた分散情報の個数 x_i に応じて，$t\alpha < x_i(2r+1-x_i)\beta/2$ のときには自明な方式を用い，$t\alpha \geq x_i(2r+1-x_i)\beta/2$ のときには効率的な方式を用いればよい．

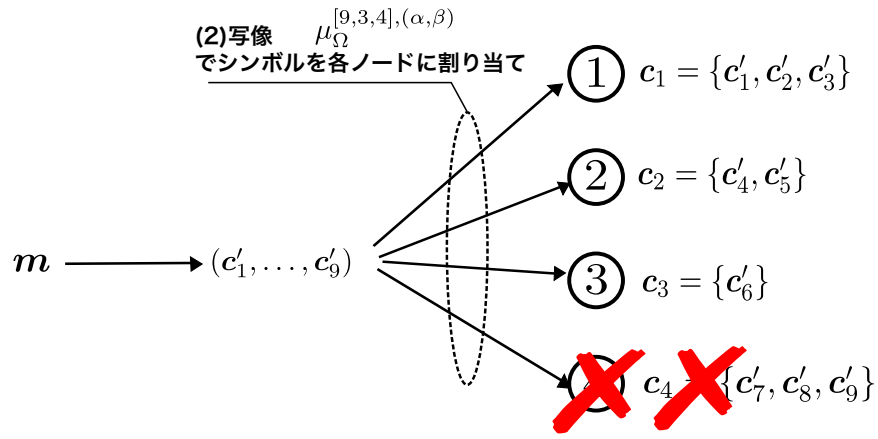

図 4.1　ストレージノード 4 が故障した場合

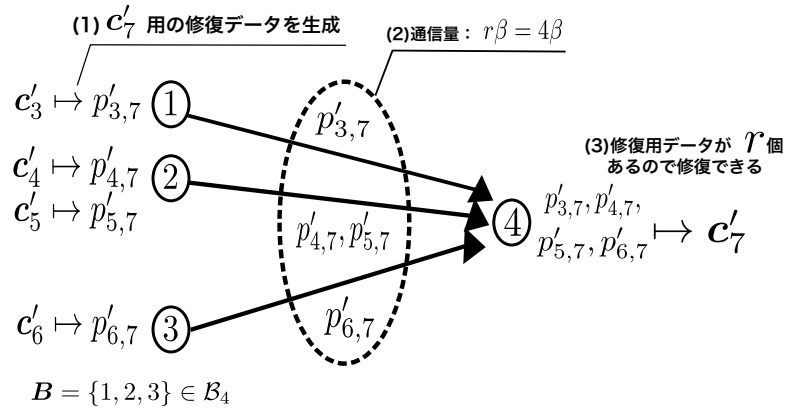

図 4.2　ノード 4 の修復（従来法） $(n=4,\ell=9,r=4)$

命題 4.1. 以上の再生成フェーズをもつ構成法によって，メッセージの復元および故障ノードの再生成が可能である．

証明 命題 3.11 と同様にして，複数割当写像の条件 (3.1),(3.2) から示せる． ■

命題 4.2. 複数割当写像 $\mu_\Omega^{[\ell,t,r],(\alpha,\beta)}$ により構成された符号のストレージ平均 ρ_S および修復バンドワイズ平均 ρ_R は，$x_i=\left|\mu_\Omega^{[\ell,t,r],(\alpha,\beta)}(i)\right|$ とするとき以下で与えられる：

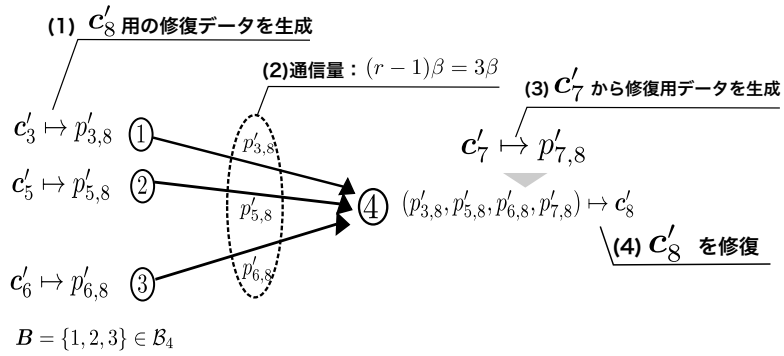

図 4.3　複数割当法による効率的な故障ノードの修復 ($n = 4, \ell = 9, r = 4, f = 4$)

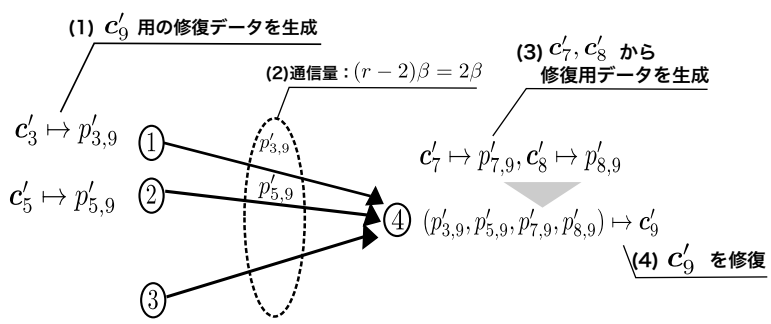

図 4.4　複数割当法による効率的な故障ノードの修復 ($n = 4, \ell = 9, r = 4, f = 4$)

$$\rho_S = \frac{1}{n}\sum_{i=1}^{n} x_i\alpha, \tag{4.1}$$

$$\rho_R = \frac{1}{n}\sum_{i=1}^{n} \min\left\{t\alpha, \frac{x_i\left(2r+1-x_i\right)\beta}{2}\right\}. \tag{4.2}$$

証明 ＜復元フェーズ＞における各ストレージ i からの通信量が $x_i \times \alpha$ であることと，＜修復フェーズ＞における各ストレージ i からの通信量が，$\min\left\{t\alpha, \frac{x_i(2r+1-x_i)\beta}{2}\right\}$ であることから明らか．■

注意 4.3. 再生成フェーズ（効率的な方式）のステップ (2)-(7) より，各故障ノード i の分散情報を再生成する際に必要な通信量は，ノード集合 $\boldsymbol{B}(\in \mathcal{B}_i)$ によらず，$\min\left\{t\alpha, \frac{x_i(2r+1-x_i)\beta}{2}\right\}$ である．よって，$\min_{\boldsymbol{B}\in\mathcal{B}_i^-}\sum_{i_j\in\boldsymbol{B}}\beta_{i,i_j} = \min\left\{t\alpha, \frac{x_i(2r+1-x_i)\beta}{2}\right\}$ であり，一方，$\sum_{\boldsymbol{B}\in\mathcal{B}_i}\sum_{i_j\in\boldsymbol{B}}\beta_{i,i_j} = |\mathcal{B}_i| \times \min\left\{t\alpha, \frac{x_i(2r+1-x_i)\beta}{2}\right\}$ である．したがって，本

提案方式においては，修復バンドワイズに関する評価基準の式 (3.13) と (3.14) の値は一致し，式 (4.2) で与えられる．

4.2　$t\alpha$ と $x_i(2r+1-x_i)\beta/2$ の大小関係

本節では，前節で示した自明な再生成方式を用いたときの通信量 $t\alpha$ と，効率的な方式を用いたときの通信量 $x_i(2r+1-x_i)\beta/2$ の大小関係が，ノード i に保管されている $[\ell,t,r]$-再生成符号の分散情報の個数 $x_i = \left|\mu_{\Omega}^{[\ell,t,r],(\alpha,\beta)}(i)\right|$ や各種パラメータ t,r,α,β によって，どのように変化するかを解析する．

命題 4.4.　1. $8t\alpha \geq (2r+1)^2\beta$ のとき，任意の $x_i\,(0 \leq x_i \leq r)$ に対して以下が成り立つ：

$$t\alpha \geq \frac{x_i(2r+1-x_i)\beta}{2}. \tag{4.3}$$

2. $8t\alpha < (2r+1)^2\beta$ のとき，以下が成り立つ：

$$\begin{cases} t\alpha \geq \dfrac{x_i(2r+1-x_i)\beta}{2}, & 0 \leq x_i \leq \theta, \\ t\alpha < \dfrac{x_i(2r+1-x_i)\beta}{2}, & \theta < x_i \leq r, \end{cases} \tag{4.4}$$

ここで，$\theta(\geq 0)$ は次の x_i に関する 2 次方程式の小さい方の解である：

$$\beta x_i^2 - (2r+1)\beta x_i + 2t\alpha = 0. \tag{4.5}$$

証明 $f(x_i) = t\alpha - x_i(2r+1-x_i)\beta/2$ とおき，x_i に関する 2 次方程式 $f(x_i) = 0$ の判別式や $f(x_i)$ の正負を調べればよい．また，2 次方程式 (4.5) の左辺を変形すると $g(x_i) = \beta\{x-(2r+1)/2\}^2 - (2r+1)^2\beta/4 + 2t\alpha$ となるので，$y = g(x_i)$ が表す放物線の頂点の x 座標 $= r+1/2 > 1$ および $g(0) = 2t\alpha \geq 0$ より，$\theta \geq 0$ である．　■

特に，MSR 点におけるパラメータについては，後者が成り立つ．

命題 4.5. $\alpha = \alpha_{\mathrm{MSR}}, \beta = \beta_{\mathrm{MSR}}$ のとき，以下が成り立つ：

$$8t\alpha_{\mathrm{MSR}} < (2r+1)^2\beta_{\mathrm{MSR}}. \tag{4.6}$$

証明 式 (2.37) より，

$$\begin{aligned} &8t\alpha_{\mathrm{MSR}} - (2r+1)^2\beta_{\mathrm{MSR}} \\ &= \frac{8t(r-t+1) - (2r+1)^2}{t(r-t+1)} \times B. \end{aligned} \tag{4.7}$$

ここで，$1 \leq t \leq r$ より，$t(r-t+1) > 0$ および

$$\begin{aligned} &8t(r-t+1) - (2r+1)^2 \\ &= -8\left(t - \frac{r+1}{2}\right)^2 + 2(r+1)^2 - (2r+1)^2 &(4.8)\\ &\leq -2r^2 + 1 < 0 &(4.9) \end{aligned}$$

が成り立つ．よって，不等式 (4.6) が成り立つ． ■

注意 4.6. MBR 点においては，$8t\alpha_{\mathrm{MBR}} - (2r+1)^2\beta_{\mathrm{MBR}}$ の正負は (t,r) に依存して決まる．実際，$t = r = 1$ のときは，$8t\alpha_{\mathrm{MBR}} - (2r+1)^2\beta_{\mathrm{MBR}} < 0$ であり，一方，$r = t = 2$ のときは $8t\alpha_{\mathrm{MBR}} - (2r+1)^2\beta_{\mathrm{MBR}} > 0$ である．

4.2.1　改良した構成法における Ω-MSR-map 符号/Ω-MBR-map の構成法

本節では，改良された再生成フェーズをもつ構成法における Ω-MSR-map 符号/Ω-MBR-map 符号の構成法について述べる．

4.2.1.1　改良した構成法における Ω-MSR/MBR-map 符号の定義と性質

本節では，改良された再生成フェーズをもつ構成法における Ω-MSR-map/MBR-map 符号の定義と性質を述べる．

定義 4.7 (Ω-MSR-map 符号)**.** $\Omega = \{\mathcal{A}, \mathcal{B}\}$ を復元および再生成に関する条件とし，$\mu_{\Omega}^{[\ell,t,r],(\alpha,\beta)}$ をより効率的な再生性フェーズをもつ構成法による Ω-再生成符号の複数割当写像とする．このとき，複数割当法による Ω-再生成符号のクラスの中で最小のストレージ平均をもち，その条件の下で最小のバンドワイズ平均をもつ符号を Ω-MSR-map 符号と定義する．Ω-MSR-map 符号のストレージ平均およびバンドワイズ平均をそれぞれ $\rho_{S_{\text{MSR-map}}}, \rho_{R_{\text{MSR-map}}}$ と記す．

次に，Ω-MSR 符号を構成するためには，複数割当写像で割り当てる分散情報としては，MSR 符号の分散情報を用いればよいことを示す．

命題 4.8. $\Omega = \{\mathcal{A}, \mathcal{B}\}$ を復元および再生成に関する条件とし，$\mu_\Omega^{[\ell,t,r],(\alpha,\beta)}$ を Ω に対する複数割当写像とする．このとき，任意の l, t, r, α, β に対して $\mu_\Omega^{[\ell,t,r],(\alpha,\beta)}$ による再生成符号が Ω-MSR-map 符号になるための十分条件は，$[\ell, t, r]$-再生成符号が MSR 符号であること，すなわち，

$$\alpha = \alpha_{\mathrm{MSR}} = \frac{B}{t}, \tag{4.10}$$

$$\beta = \beta_{\mathrm{MSR}} = \frac{B}{t(r-t+1)} \tag{4.11}$$

が成り立つことである．

証明 まず，ストレージ平均 ρ_S を最小化することを考える．式 (4.1) および MSR 符号の定義より，任意の α に対して

$$\rho_S = \frac{1}{n}\sum_{i=1}^{n} x_i\alpha \geq \frac{1}{n}\sum_{i=1}^{n} x_i\alpha_{\mathrm{MSR}} \tag{4.12}$$

が成り立つ．ここで，$x_i = \left|\mu_\Omega^{[\ell,t,r],(\alpha,\beta)}(i)\right|$ であり，これはノード i に保管されている $[\ell, t, r]$-再生成符号の分散情報の個数を表す．したがって，ρ_S を最小化するには $\alpha = \alpha_{\mathrm{MSR}}$ となる $[\ell, t, r]$-再生成符号を用いればよい．

次に，ρ_S を最小にした下で，ρ_R を最小化することを考える．$\alpha = \alpha_{\mathrm{MSR}}$ のとき，MSR 符号の定義より，

$$\rho_R = \frac{1}{n}\sum_{i=1}^{n} \min\left\{t\alpha_{\mathrm{MSR}}, \frac{x_i\,(2r+1-x_i)\,\beta}{2}\right\} \tag{4.13}$$

$$\geq \frac{1}{n}\sum_{i=1}^{n} \min\left\{t\alpha_{\mathrm{MSR}}, \frac{x_i\,(2r+1-x_i)\,\beta_{\mathrm{MSR}}}{2}\right\} \tag{4.14}$$

が成り立つ．

したがって，ρ_S を最小化した下で ρ_R を最小化するには $\alpha = \alpha_{\mathrm{MSR}}$ かつ $\beta = \beta_{\mathrm{MSR}}$ となる $[\ell, t, r]$-再生成符号，すなわち MSR 符号を用いればよい．　■

注意 4.9. ρ_R の式 (4.2) の式および注意 4.6 から，MBR-map 符号については同様の性質を持たないことがわかる．すなわち，$[\ell, t, r]$-MBR を用いることは，より効率的な再生成フェーズをもつ構成法における複数割当写像による再生成符号を構成するための十分条件とは限らない．

以降，$\mu_\Omega^{[\ell,t,r],(\alpha_{\mathrm{MSR}},\beta_{\mathrm{MSR}})}$ を $\mu_\Omega^{[\ell,t,r]}$ と略記する．複数割当写像 $\mu_\Omega^{[\ell,t,r]}$ により構成された符号のストレージ平均 ρ_S および修復バンドワイズ平均 ρ_R は，$x_i = \left|\mu_\Omega^{[\ell,t,r]}(i)\right|$ とするとき，それぞれ以下で与えられる：

$$\rho_S = \frac{B}{nt}\sum_{i=1}^{n} x_i, \tag{4.15}$$

$$\rho_R = \frac{B}{n}\sum_{i=1}^{n}\left\{I[\theta < x_i \le r] + \frac{x_i(2r+1-x_i)}{2t(r-t+1)} I[0 \le x_i \le \theta]\right\}, \tag{4.16}$$

ここで，θ は 2 次方程式 (4.5) において $\alpha = \alpha_{\mathrm{MSR}}, \beta = \beta_{\mathrm{MSR}}$ としたときの小さい方の解である．ここで，$I[\cdot]$ は定義関数，すなわち，$[\cdot]$ 内の命題が真のときに 1 を返し，そうでないときに 0 を返す関数である．このとき，式 (4.15) より，t を固定したときの ρ_S は，$\sum_{i=1}^{n} x_i$ に依存する．

4.2.1.2　改良した構成法における Ω-MSR-map 符号の構成アルゴリズム

本節では，より効率的な再生成フェーズをもつ最適な Ω-MSR-map 符号の構成法について述べる．

命題 4.8 より，改良前の再生成フェーズをもつ構成法における Ω-MSR-map の構成法（Algorithm 1）と全く同様のアルゴリズムを用いることで，Ω-MSR-map を構成することができる．

4.2.1.3　準最適な Ω-MBR-map 符号の構成アルゴリズム

本節では，より効率的な再生成フェーズをもつ準最適な Ω-MBR-map 符号の構成法について述べる．

注意 4.9 より, Ω-MBR-map 符号の構成においては, トレードオフ曲線上のどのパラメータ (α, β) を用いればよいか定まらない．ただし，命題 4.4 より，$8t\alpha \geq (2r+1)^2\beta$ を満たす (α, β) では ρ_R の式 (4.2) が β の一次式となることがわかる．したがって，条件 $8t\alpha \geq (2r+1)^2\beta$ を満たす (α, β) の中では，トレードオフ曲線と直線 $8t\alpha - (2r+1)^2\beta = 0$ との交点

$$(\tilde{\alpha}, \tilde{\beta}) = \left(\frac{(2r+1)^2 B}{4t^2(2r-t+1)}, \beta_{\mathrm{MBR}} \right) \tag{4.17}$$

を用いるのが最適である．このパラメータを用いるときのストレージ平均および修復バンドワイズ平均はそれぞれ

$$\rho_S(t, r) = \frac{1}{n} \sum_{i=1}^{n} x_i \tilde{\alpha}, \tag{4.18}$$

$$\rho_R(t, r) = \frac{M}{2n} \sum_{i=1}^{n} \frac{x_i(2r+1-x_i)}{t(2r-t+1)} \tag{4.19}$$

となる．このとき，解くべき最適化問題は次の二次整数計画問題となる．

$$\mathrm{IP}_{\Omega,R}(t, r): \tag{4.20}$$

$$\begin{aligned} \text{minimize} \quad & \sum_{i=1}^{n} \frac{x_i(2r+1-x_i)}{t(2r-t+1)}, \\ \text{subject to} \quad & \sum_{i \in \boldsymbol{A}} x_i \geq t, \quad \boldsymbol{A} \in \mathcal{A}^{-}, \\ & \sum_{i \in \boldsymbol{B}} x_i \geq r, \quad \boldsymbol{B} \in \mathcal{B}_i, i \in [n]. \end{aligned} \tag{4.21}$$

このとき準最適な構成法として，次のようなアルゴリズム (Algorithm 3) が導出できる．$\alpha_{\mathrm{MBR}} = B/t(2r-t+1) \geq 1$ であるので，まずこの条件を満たすすべての (t, r) について $\mathrm{IP}_{\Omega,R}(t, r)$ を解き，$\rho_R(t, r)$ を最小にした下で $\rho_S(t, r)$ を最小にする割当 $\tilde{\boldsymbol{x}}$ およびパラメータ $(\tilde{m}, \tilde{t}, \tilde{r})$ を求める．次に，$\alpha_{\mathrm{MBR}} \leq \tilde{\alpha}$ であるので，求めた割当個数に対して，実際に割り当てるシンボルには $[\tilde{m}, \tilde{t}, \tilde{r}]$-MBR 符号を用いてメッセージ $\boldsymbol{m}$ を符号化する．

Algorithm 3 Construction of suboptimal Ω-MBR-map codes

Require: $\boldsymbol{m}, n, B, \Omega = \{\mathcal{A}, \mathcal{B}\}$

Ensure: $\left(\mu_\Omega^{[\tilde{m},\tilde{t},\tilde{r}]}(1), \ldots, \mu_\Omega^{[\tilde{m},\tilde{t},\tilde{r}]}(n)\right)$

$t \leftarrow 1, r \leftarrow 1$
while $B/t(2r - t + 1) \geq 1$ **do**
  $r \leftarrow t$
  while $B/t(2r - t + 1) \geq 1$ **do**
    solve $\mathrm{IP}_{\Omega,R}(t, r)$
    $r \leftarrow r + 1$
  end while
  $t \leftarrow t + 1$
end while
calculate $\min_{u,v\,:\,B/u(2v-u+1)\geq 1} \rho_R(u, v)$
calculate $\tilde{m}, \tilde{t}, \tilde{r}$ and $\tilde{\boldsymbol{x}}$
calculate the multiple assignment map $\mu_\Omega^{[\tilde{m},\tilde{t},\tilde{r}]}$
encode $\boldsymbol{m}$ to $\left(\mu_\Omega^{[\tilde{m},\tilde{t},\tilde{r}]}(1), \ldots, \mu_\Omega^{[\tilde{m},\tilde{t},\tilde{r}]}(n)\right)$ from MBR codes

第 5 章

数値例

5.1 構成例

本節では，Algorithm 1, 2, 3 による Ω-MSR-map 符号の構成例を示す．

例 5.1. $n = 6, M = 100$ とし，以下の $\Omega = \{\mathcal{A}, \mathcal{B}\}$ を考える．

$$\mathcal{A}^- = \{\{1,2\},\{1,3\},\{1,4\},\{1,5\},$$
$$\{1,6\},\{2,3\},\{2,4\},\{2,5\},\{2,6\},\{3,4,5,6\}\}, \tag{5.1}$$
$$\mathcal{B} = \{\mathcal{B}_1^-, \mathcal{B}_2^-, \mathcal{B}_3^-, \mathcal{B}_4^-, \mathcal{B}_5^-, \mathcal{B}_6^-\} \tag{5.2}$$

ここで,

$$\mathcal{B}_1^- = \{\{2,3,4,5,6\}\}, \tag{5.3}$$
$$\mathcal{B}_2^- = \{\{1,3,4,5,6\}\}, \tag{5.4}$$
$$\mathcal{B}_3^- = \{\{1,2,4\},\{1,2,5\},\{1,2,6\}\}, \tag{5.5}$$
$$\mathcal{B}_4^- = \{\{1,2,3\},\{1,2,5\},\{1,2,6\}\}, \tag{5.6}$$
$$\mathcal{B}_5^- = \{\{1,2,3\},\{1,2,4\},\{1,2,6\}\}, \tag{5.7}$$
$$\mathcal{B}_6^- = \{\{1,2,3\},\{1,2,4\},\{1,2,5\}\}. \tag{5.8}$$

このとき，Algorithm 1 を用いると以下のパラメータ $l^*, t^*, r^*, \boldsymbol{x}^*$ を持つ複数割当写像 $\mu_\Omega^{[l^*,t^*,r^*]}$ が構成できる：

$$l^* = 10, \qquad t^* = 4, \qquad r^* = 7, \tag{5.9}$$

$$x_1^* = x_2^* = 3, \tag{5.10}$$

$$x_3^* = x_4^* = x_5^* = x_6^* = 1. \tag{5.11}$$

このとき，Ω-MSR-map 符号の分散情報は $[10, 4, 7]$-MSR 符号を用いて構成され，その割当は以下のようになる：

$$\mu_\Omega(1) = \{w_1, w_2, w_3\}, \qquad \mu_\Omega(2) = \{w_4, w_5, w_6\}, \tag{5.12}$$

$$\mu_\Omega(3) = \{w_7\}, \qquad \mu_\Omega(4) = \{w_8\}, \tag{5.13}$$

$$\mu_\Omega(5) = \{w_9\}, \qquad \mu_\Omega(6) = \{w_{10}\}. \tag{5.14}$$

ここで，w_i は $[10, 4, 7]$-MSR 符号の分散情報を表す．このときの θ, ストレージ平均および修復バンドワイズ平均はそれぞれ，$\theta \approx 2.58, \rho_{S_{\text{MSR-map}}} \approx 41.67, \rho_{R_{\text{MSR-map}}} = 62.50$ であり，これは命題 3.2 の方法で $[6, 2, 3]$-MSR 符号を用いて構成したときの $\rho_S = 50.00, \rho_R = 75.00$ と比べて確かに効率が良いことがわかる．ここで，θ は 2 次方程式 (4.5) において，$M = 100, r = r^*, t = t^*, \alpha = \alpha_{\text{MSR}} = M/t^* = 25, \beta = \beta_{\text{MSR}} = M/t^*(r^* - t^* + 1) = 25/4$ として係数を設定したときの小さい方の解である．

例 5.1 と同様の設定の下で，Algorithm 2 を用いると以下のパラメータ $l^*, t^*, r^*, \boldsymbol{x}^*$ を持つ複数割当写像 $\mu_\Omega^{[l,t,r]}$ が構成できる：

$$l^* = 3, \qquad t^* = 1, \qquad r^* = 1 \text{ or } 2, \tag{5.15}$$

$$x_1^* = x_2^* = x_3^* = 1, \tag{5.16}$$

$$x_4^* = x_5^* = x_6^* = 0. \tag{5.17}$$

このとき，Ω-MBR-map 符号の符号語は $[3, 1, 1]$-MBR 符号もしくは $[3, 1, 2]$-MBR 符号を用いて構成され，そのときの割当は以下のようになる：

$$\mu_\Omega(1) = \{w_1\}, \mu_\Omega(2) = \{w_2\}, \mu_\Omega(3) = \{w_3\}, \tag{5.18}$$

$$\mu_\Omega(4) = \mu_\Omega(5) = \mu_\Omega(6) = \varnothing, \tag{5.19}$$

ここで，w_i は $[3, 1, 1]$-MBR 符号もしくは $[3, 1, 2]$-MBR 符号の分散情報を表す．このときのストレージ平均および修復バンドワイズ平均はそれぞれ $\rho_{S_{\text{MBR-map}}} = \rho_{R_{\text{MBR-map}}} =$

50 であり，これは命題 3.2 の方法で構成したときの $\rho_S = \rho_R = 60$ と比べて確かに効率が良いことがわかる．

例 5.2. 最後に，例 5.1 と同様の設定の下で，Algorithm 1,2,3 および $[\ell, t, r]$-MSR/MBR 符号を用いた自明な構成法によって，Ω-再生成符号を構成したときの，ストレージ平均 ρ_S および修復バンドワイズ平均 ρ_R の値を以下の表 5.1 に示す：

符号	ストレージ平均 ρ_S	バンドワイズ平均 ρ_R
自明な構成法 w/ MSR 符号	50.00	75.00
従来の提案法 w/ MSR 符号	41.67	72.92
効率的な修復法 w/ MSR 符号	41.67	62.50
自明な構成法 w/ MBR 符号	60.00	60.00
従来の提案法 w/ MBR 符号	50.00	50.00
効率的な修復法 w/ $(\tilde{\alpha}, \tilde{\beta})$	50.00	25.00

表 5.1　数値例の比較

ただし，効率的な修復法 w/ $(\tilde{\alpha}, \tilde{\beta})$ の ρ_R の値については，$(\alpha, \beta) = (\tilde{\alpha}, \tilde{\beta} = \beta_{\mathrm{MBR}})$ の下で Algorithm 3 によって割当個数 $x_i, i \in [n]$ を求めたあと，$\alpha = \alpha_{\mathrm{MBR}}$ とした場合の値を載せている．

5.2　比較と考察

表 5.1 の結果より，いずれの場合も効率的な修復フェーズをもつ構成法において，Algorithm 1,3 によって，ストレージ平均および修復バンドワイズ平均が改善していることが確認できる．

例 5.1 の $\Omega = (\mathcal{A}, (\mathcal{B}_i)_{i=}^{n})$ に対する Ω-MSR-map 符号をみると，$[\ell^* = 6, t^* = 2, r^* = 3]$-再生成符号の分散情報の割当の仕方が

$$\mu_\Omega(1) = \{w_1, w_2, w_3\}, \qquad \mu_\Omega(2) = \{w_4, w_5, w_6\} \tag{5.20}$$

となっており，他のストレージノードに比べて多く割り当てられていることがわかる．これは，これは，$\mathcal{A}$ をみると，ストレージノード 1 および 2 が多くの部分集合の元になっており，復元において重要な役割を持っているような構造になっていることによるものだと考えられる．

一方，例 5.1 の $\Omega = (\mathcal{A}, (\mathcal{B}_i)_{i=}^{n})$ に対する Ω-MBR-map 符号をみると，$[\ell^* = 3, t^* = 1, r^* = 1\text{or}2]$-再生成符号の分散情報の割当の仕方が

$$\mu_\Omega(1) = \{w_1\}, \mu_\Omega(2) = \{w_2\}, \mu_\Omega(3) = \{w_3\} \tag{5.21}$$

で，他のノードについては $\varnothing$ となっている．これは，修復に関する条件 $\mathcal{B}$ をみると，各ストレージノードの故障に対しては，ノード 1, 2, 3 が自身以外の修復条件の部分集合の元になっており，他のストレージノードと比べて重要度が高くなっていることが原因と考えられる．

第 6 章

結論と今後の展望

6.1 まとめ

本研究では，分散ストレージシステム (DSS) に対する符号化法として，実際の運用におけるさまざまな条件を反映させるための符号化法の提案を行った．具体的な符号化法として，複数割当法と整数計画問題を用いた構成アルゴリズムを導出した．また，具体的な数値例を用いて，自明な構成法と提案アルゴリズムの比較を行った．

2 章では，本研究で扱う分散ストレージ符号化の従来研究として，再生成符号および秘密分散法の概要について説明した．

3 章では，従来の $[n, k, d]$-DSS モデルにおける復元および再生成に関する条件を集合族としての条件 $\Omega = \{\mathcal{A}, \mathcal{B}\}$ に拡張した Ω-DSS モデルおよび Ω-再生成符号を提案し，複数割当法を用いた構成法を提案した．さらに，この複数割当法を用いた符号のクラスの中で，ストレージ平均を最小にした下で，修復バンドワイズ平均を最小にする符号（Ω-MSR-map 符号）および修復フェーズ平均を最小にした下で，ストレージ平均を最小にする符号（Ω-MBR-map 符号）の構成法として，整数計画問題を繰り返し解くアルゴリズムを導出した．

4 章では，より効率的な修復フェーズをもつ Ω-MSR-map 符号の構成アルゴリズムおよび，Ω-MBR-map 符号の準最適な構成アルゴリズムについての導出を行った．

5 章では，数値例を用いて，提案アルゴリズムの効率性について比較を行った．

6.2　今後の展望

今後の課題としては，以下の課題が挙げられる：

- 改良した修復フェーズをもつ Ω-再生成符号における Ω-MBR-map 符号を構成すること
- $[l, t, r]$-再生成符号の復号関数や再生成用の関数をそのまま利用しない，より効率的な再生成方式を提案すること

また注意 3.12，3.15 でも述べたように，与えられた条件 Ω を実現する Ω-MSR/MBR-map 符号は，Ω によっては，ρ_S や ρ_R の意味で最適であるとは一般には言えない．実際，条件 Ω が一般的であるため，トレードオフの解析等も困難である．これは，より研究が進んでいる Γ-SSS についても同様である．

しかしながら，Ω に現実的に意味のある構造を仮定した上で，トレードオフの解析や限界を達成する符号を構成するアプローチが考えられる．実際，秘密分散法の分野においては，Γ に階層型構造を仮定した上でストレージの下限およびそれを達成する具体的な符号化方式を導出する研究がある [15].

また，一般化した条件 Ω が与えられたもとで，一般化された情報漏えい機能をも各分散情報に対して，秘密分散法で考慮されているような，セキュリティ条件を付加した場合の再生成符号化方式の提案についても今後の課題とする．

謝辞

本論文をまとめるにあたり主査として御指導頂いた,

早稲田大学基幹理工学部応用数理学科

松嶋 敏泰教授

に心より感謝いたします．松嶋教授には研究室に配属されて以来，終始熱心なご指導を頂き，研究活動に留まらない数多くの有益な御指導，御助言を賜りました．

また，副査として，大変お忙しい中，貴重なお時間を頂きご指導頂きました

早稲田大学基幹理工学部応用数理学科

橋本 喜一朗教授

早稲田大学基幹理工学部応用数理学科

大石 進一教授

早稲田大学基幹理工学部応用数理学科

柏木 雅英教授

早稲田大学理工学術院総合研究所

平澤 茂一名誉教授

に心より感謝いたします．

また，松嶋研究室の諸先輩方には，多くの御指導，御助言を頂き感謝いたします．特に，横浜商科大学 吉田隆弘准教授，早稲田大学 須子統太准教授，早稲田大学 グローバルエデュケーションセンター 堀井俊佑准教授には研究のみならず，さまざまな場面でお世話になり，親身な御助言を頂きました．

また，横浜商科大学 浮田善文教授，北見工業大学 前田康成准教授，専修大学 野村亮准教授，日本電気株式会社 峯松一彦博士，株式会社 NTT データ 末永高志博士，小樽商科大学 小泉大城准教授，株式会社東芝 安田豪毅博士，株式会社 NTT ドコモ 桑田修平博士，湘南工科大学 齋藤友彦講師，青山学院大学 宮希望助教には研究室のゼミを通じて多くの議論やご助言をいただきましたこと，感謝申し上げます．また，本研究のきっかけになった共同研究者である トランスコスモス株式会社 東優太氏に感謝いたします．

松嶋研究室に所属する学生一同には，常日頃より大変お世話になりました．審査に関わる諸々の作業について多くのご支援を頂き，感謝いたします．この場を借りて心よりお礼申し上げます．

また，研究室での生活をともに過ごした松嶋研究室の先輩・後輩諸氏，特に，飯窪祐二氏，石井智氏，中井祥人氏，山本粋士氏，岩崎悠介氏，宮下有咲氏に感謝申し上げます．

本論文は以上をはじめとする多くの方々のご指導，ご支援の賜物です．お世話になりました皆様に深く感謝いたします．最後に，著者の研究生活をあらゆる面から支え，温かく見守ってくれた家族に心から感謝いたします．

参考文献

[1] A. Dimakis, P. Godfrey, Y. Wu, M. Wainwright, and K. Ramchandran, "Network coding for distributed storage systems," *Information Theory, IEEE Transactions on*, vol. 56, pp. 4539–4551, Sept 2010.

[2] A. Kamatsuka, Y. Azuma, T. Yoshida, and T. Matsushima, "Regenerating codes with generalized conditions of reconstruction and regeneration," in *2016 International Symposium on Information Theory and Its Applications (ISITA)*, pp. 41–45, Oct 2016.

[3] T. M. Cover and J. A. Thomas, *Elements of Information Theory (Wiley Series in Telecommunications and Signal Processing)*. Wiley-Interscience, 2006.

[4] R. Ahlswede, N. Cai, S.-Y. Li, and R. Yeung, "Network information flow," *Information Theory, IEEE Transactions on*, vol. 46, pp. 1204–1216, Jul 2000.

[5] N. B. Shah, K. V. Rashmi, P. V. Kumar, and K. Ramchandran, "Distributed storage codes with repair-by-transfer and non-achievability of interior points on the storage-bandwidth tradeoff," *CoRR*, vol. abs/1011.2361, 2010.

[6] 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, pp. 5227–5239, Aug 2011.

[7] T. Ernvall, "Exact-regenerating codes between MBR and MSR points," *CoRR*, vol. abs/1304.5357, 2013.

[8] C. Suh and K. Ramchandran, "On the existence of optimal exact-repair MDS codes for distributed storage," *CoRR*, vol. abs/1004.4663, 2010.

[9] R. Tandon, S. Amuru, T. C. Clancy, and R. M. Buehrer, "Towards optimal secure distributed storage systems with exact repair," *CoRR*, vol. abs/1310.0054, 2013.

[10] T. Ernvall, T. Westerbäck, R. Freij-Hollanti, and C. Hollanti, "A connection between

locally repairable codes and exact regenerating codes," in *2016 IEEE International Symposium on Information Theory (ISIT)*, pp. 650–654, July 2016.

[11] N. B. Shah, K. V. Rashmi, and P. V. Kumar, "Information-theoretically secure regenerating codes for distributed storage," in *Global Telecommunications Conference (GLOBECOM 2011), 2011 IEEE*, pp. 1–5, Dec 2011.

[12] S. Goparaju, A. Fazeli, and A. Vardy, "Minimum storage regenerating codes for all parameters," *IEEE Transactions on Information Theory*, vol. PP, no. 99, pp. 1–1, 2017.

[13] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[14] M. Iwamoto, H. Yamamoto, and H. Ogawa, "Optimal multiple assignments based on integer programming in secret sharing schemes with general access structures(protocols, cryptography and information security)," *IEICE transactions on fundamentals of electronics, communications and computer sciences*, vol. 90, pp. 101–112, jan 2007.

[15] O. Farras and C. Padro, "Ideal hierarchical secret sharing schemes," *IEEE Transactions on Information Theory*, vol. 58, pp. 3273–3286, May 2012.

研究業績

種類別	題名，発表・発行掲載誌名，発表・発行年月，連名者（申請者含む）
1. 論文◯	復元および再生成の条件を一般化した再生成符号とその構成法, 電子情報学会論文誌 A，2017, 鎌塚 明，東 優太，吉田 隆弘，松嶋 敏泰
2. 国際会議（査読有）◯	Regenerating codes with generalized conditions of reconstruction and regeneration, 2016 International Symposium on Information Theory and Its Applications (ISITA), pp. 41–45, Oct 2016, A. Kamatsuka, Y. Azuma, T. Yoshida, and T. Matsushima
3. 国際会議（査読有）	A maximum likelihood decoding algorithm of gabidulin codes in deterministic network coding, in 2016 International Symposium on Information Theory and Its Applications (ISITA), pp. 666–670, Oct 2016, K. Kazama, A. Kamatsuka, and T. Matsushima
4. 国際会議（査読有）◯	Parallel Concatenation of Polar Codes and Iterative Decoding,”Proceedings of the 2014 International Symposium on Information Theory and its Applications, p.347, Oct 2014, Akira KAMATSUKA, Shunsuke HORII, Toshiyasu MATSUSHIMA

種類別	題名，発表・発行掲載誌名，発表・発行年月，連名者（申請者含む）
5. 講演	一般化された再生成符号に対する効率的な複数割当法による構成法，第 39 回情報理論とその応用シンポジウム（SITA2016），富山県，2016 年 12 月，鎌塚 明，吉田 隆弘，松嶋敏泰
6. 講演	潜在変数を仮定した非線形回帰モデルおけるベイズ基準のもと最適な予測，第 39 回情報理論とその応用シンポジウム（SITA2016），富山県，2016 年 12 月，鎌塚 明，吉田 隆弘，松嶋敏泰
7. 講演	シンボルペア通信路における符号のリスト復号に関する一考察，第 39 回情報理論とその応用シンポジウム（SITA2016），富山県，2016 年 12 月，風間皐希，鎌塚 明，松嶋敏泰
8. 講演	Array-Error モデルにおける軟判定復号に関する一考察, 電子情報通信学会技術研究報告,vol.115, no.394, IT2015-49, pp.7–12, 電子情報通信学会情報理論研究会（IT）, 2016 年 1 月 18 日—19 日, 大阪府， 風間皐希, 鎌塚明, 松嶋敏泰
9. 講演	条件を一般化した再生成符号とその複数割当法による構成法，第 5 回誤り訂正符号のワークショップ (ECCW2016)，佐賀県，2016 年 9 月 鎌塚 明，吉田隆弘，松嶋敏泰

種類別	題名，発表・発行掲載誌名，発表・発行年月，連名者（申請者含む）
10. 講演	Polar 符号の探索アルゴリズムを用いた復号法に関する一考察，第 38 回情報理論とその応用シンポジウム（SITA2015），岡山県，2015 年 11 月鎌塚 明，松嶋敏泰
11. 講演	復元および再生成の条件を一般化した再生成符号に関する一考察，第 38 回情報理論とその応用シンポジウム（SITA2015），岡山県，2015 年 11 月東 優太，鎌塚 明，吉田 隆弘，松嶋敏泰
12. 講演	Polar 符号の探索アルゴリズムを用いた復号について，電子情報通信学会情報理論研究会（IT），石川県，2015 年 9 月，鎌塚 明，松嶋敏泰
13. 講演	消失中継通信路上での Decode - and - Forward 型通信におけるパンクチャされた空間結合 LDPC 符号のユニバーサル性，第 37 回情報理論とその応用シンポジウム（SITA2014），岡山県，2014 年 12 月中原悠太，齋藤翔太，鎌塚 明，松嶋敏泰

種類別	題名，発表・発行掲載誌名，発表・発行年月，連名者（申請者含む）
14. 講演	非線形コンバイナ型乱数生成器に対する Sum Product Algorithm を用いる攻撃に関する一考察, 電子情報通信学会技術研究報告,vol.114, no.306, IBISML2014-83, pp.357–364, 電子情報通信学会情報論的学習理論と機械学習研究会（IBISML）, 2014 年 11 月 17 日–19 日, 愛知県, 久保航汰, 齋藤翔太, 鎌塚明, 松嶋敏泰
15. 講演	有限バッファ Hybrid SR-ARQ における最適制御方式に関する一考察, 電子情報通信学会情報理論研究会（IT），兵庫県，2014 年 7 月，影山優太，鎌塚 明，前田康成，松嶋敏泰
16. 講演	Polar 符号を用いた並列連接符号化に関する一考察，第 36 回情報理論とその応用シンポジウム（SITA2013），岡山県，2013 年 11 月，鎌塚明，堀井俊佑，松嶋敏泰