早稲田大学大学院 基幹理工学研究科

博士論文審査報告書

論　文　題　目

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

申　請　者

鎌塚	明
Akira	KAMATSUKA

数学応用数理専攻 情報理論研究

2018 年 2 月

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．各ストレージが抱えるリスクとしては，災害等で故障が発生し，データが消失するリスクが挙げられる．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 $\boldsymbol{m} \in \mathbb{F}_q^B$，$\mathbb{F}_q^B$ は位数 q の有限体 $\mathbb{F}_q$ 上の B 次元ベクトル空間）を 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） $\boldsymbol{m} \mapsto (\boldsymbol{c}_1, \ldots, \boldsymbol{c}_n) \in (\mathbb{F}_q^\alpha)^n$ を施し，写像されたデータの一部（分散情報） $\boldsymbol{c}_i, i = 1, \ldots, n$ を各ストレージに保存する分散ストレージシステムで元データ $\boldsymbol{m}$ 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．

分散ストレージシ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（$\overset{\text{def.}}{\iff}$ 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，次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．

(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．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，その限界を達成する方式として (k, n)-しきい値法を提案した．(k, n)-しきい値法は，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用いる方式である．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 $i_1, \ldots, i_{k-1}$ 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システムに持たせることができる．(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自明な修復法によってなされてきた．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システムにおいては，j 番目の故障ストレージの修復の際には，$d\,(\leq n-1)$ 個の修復用ストレージが選ばれ，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．このときの通信量（修復バンドワイズ）は $d\beta (\leq k\alpha)$ となり，通信量の意味で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ている．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 (PM 法) や，Shah らによる Repair by Transfer 法等が提案されている．

上記の分散ストレージシステムの機能 (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．そのため従来の符号化法では「耐久性の高いストレージを，故障ストレージの修復に多く参加させる」のような機能をシステムに持たせることはできない．そこで本論文では，(1) および (3) に関する条件を一般化した Ω-再生成符号を定義し，より柔軟な付加機能をもつような分散ストレージシステムに対する符号化法を与えている．

第 1 章では本研究の背景および目的について述べ，第 2 章では準備として，本論文で扱う $[n,k,d]$-再生成符号，$[k,n]$-秘密分散法および (1),(2) に関する一般化の従来研究である Γ-秘密分散法について概観している．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．

第 3 章では，(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している．$[n] := \{1,\dots,n\}$ をストレージのインデックスの集合，$2^{[n]}$ を $[n]$ のべき集合，$\mathcal{A}$ を元データ $\boldsymbol{m}$ を復元可能なストレージ集合の族，$\mathcal{B}_j$ は故障ストレージ j を修復可能なストレージ集合の族とするとき，本論文では条件 (1) および (3) を一般化した条件 Ω を集合族の組 $\Omega = \left(\mathcal{A}, (\mathcal{B}_j)_{j=1}^n\right)$ $(\mathcal{A} \in 2^{[n]}, \mathcal{B}_j \in 2^{[n]\setminus\{j\}})$ として提案している．その上で，後の効率的な符号化アルゴリズムの導出に有用な，従来の $[n,k,d]$-再生成符号がもつ性質（単調性条件および $\mathcal{B}_j \subseteq \mathcal{A}, j \in [n]$）を Ω に仮定し，Ω-再生成符号が従来の $[n,k,d]$-再生成符号を含む拡張になっていることを示している．

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 $p_{i\to j} \in \mathbb{F}_q^{\beta_{i,j}}$ のサイズ $\beta_{i,j} \in \mathbb{N}$ が，ストレージごとに異なる．そこで本論文では，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 を提案している．

Ω-再生成符号の構成の際には，まずあるパラメータ $[\ell,t,r]$, $\ell \geq n$ に対する $[\ell,t,r]$-再生成符号を用いて元データ $\boldsymbol{m}$ を符号化し分散情報を生成した後で，生成された ℓ 個の分散情報を与えられた条件 Ω を満足するように割り当てる方式を提案している．このとき，復元および修復の際には元の $[\ell,t,r]$-再生成符号の復元および修復関数を用いる．このような符号の構成法を複数割当法と呼ぶ．本論文では，条件 $\Omega = \left(\mathcal{A}, (\mathcal{B}_j)_{j=1}^n\right)$ を満たすための十分条件として，$\boldsymbol{A} \in \mathcal{A}$ 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している．

本論文ではさらに，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，その構成アルゴリズムを導出している．分散情報の割り当てを表現する写像を $\mu_\Omega^{[\ell,t,r],(\alpha,\beta)}$ とし，ストレージ i に割り当てられる分散情報の個数を $x_i = \left|\mu_\Omega^{[\ell,t,r],(\alpha,\beta)}(i)\right|$ とするとき，$[\ell,t,r]$-再生成符号を用いた複数割当法における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，$\rho_S = \frac{1}{n}\sum_{i=1}^{n} x_i \times \alpha, \rho_R = \frac{1}{n}\sum_{i=1}^{n} x_i \times r\beta$ で与えられる．したがって，各符号を構成する際には，(i)(α,β), (ii)$[\ell,t,r]$, (iii) $x_i, i \in [n]$, (iv)$\mu_{\Omega}^{[\ell,t,r],(\alpha,\beta)}$ を最適化する必要がある．本論文では，これらの内，(i) (α,β) については，それぞれ MSR/MBR 点のパラメータを用いれば十分であることを示し，(ii) の ℓ および (iv) $\mu_{\Omega}^{[\ell,t,r],(\alpha,\beta)}$ については最適な t,r および $x_i, i \in [n]$ から自然に定まることを示している．残りについては，割当個数の総数 $\sum_{i=1}^{n} x_i$ を目的関数として，不等式制約 $\sum_{i\in\boldsymbol{A}} x_i \geq t$ および $\sum_{i\in\boldsymbol{B}} x_i \geq r$ （複数割当法が Ω を満たすための十分条件に相当） のもとで整数計画問題（最小化問題） IP(t,r) を各 t,r に関して探索することにより求める．このとき，Ω に仮定した条件を利用して効率的な探索アルゴリズムを導出している．

Ω-再生成符号は Γ-秘密分散法と異なり故障ストレージの修復法に関しては工夫の余地がある．そこで第 4 章において，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っている．具体的には，各種パラメータ $(\alpha,\beta),[\ell,t,r]$ および割当個数 x_i が与えられたときに，自明な修復にかかる通信量と効率的な修復法における通信量に関する比較を行い，両者の大小関係が切り替わるしきい値を導出している．その上で，効率的な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し，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 (α,β) が決定できないため，準最適な構成法を提案している．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している．

最後に，第 6 章で結論と今後の課題を述べている．

以上を総括すると，本論文は，従来考えられていた復元および修復機能を持つしきい値型分散ストレージシステムのモデルを，一般的な状況を考慮したモデルへと拡張し，そのもとでの効率的な符号化アルゴリズムを与えている．これによって，より実際的な運用を考えた場合の分散ストレージシステムの構築が理論的に可能となった．よって，本論文は理論面と実用面の双方から高く評価でき，博士（工学）の学位として価値あるものと認める．

2017 年 11 月

審査員

（主査）	早稲田大学教授	博士（工学）	早稲田大学	松嶋 敏泰
	早稲田大学教授	理学博士	東京大学	橋本 喜一朗
	早稲田大学教授	工学博士	早稲田大学	大石 進一
	早稲田大学教授	博士（工学）	早稲田大学	柏木 雅英
	早稲田大学名誉教授	工学博士	大阪大学	平澤 茂一