■1 群（信号・システム）－ 1 編（情報理論）

8 章 通信路符号化

（執筆者：三宅茂樹）[2009 年 11 月 受領]

■概要■

通信路符号化問題は**図 1** で示すように送り手と受け手の間に通信路が存在する系において，送り手によって送られたメッセージを受け手が正しく受け取るための伝送レート（通信路を 1 回使用するたびにどれほどの文字が送られるかに関する指標）と復号誤り率に関する関係を取り扱う．

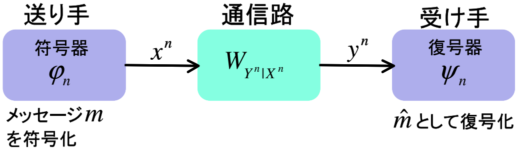

図 1　通信路モデル

8-1 節では通信路符号化定理について述べる．符号化定理は情報スペクトル理論（14 章）を用いて最も一般的な形で与えられるが，本章では最も基本的な定常無記憶通信路の場合を主に紹介する．定常無記憶通信路の場合には，通信路容量が簡単な形式で記述できる（単文字化）という特長があり，このため効率的な計算アルゴリズムが存在する．計算アルゴリズムの詳細については 8-2 節で述べる．

また，送り手と受け手の間の一対一の伝送問題は，**図 2** で示される情報源・通信路結合伝送問題の解決を一つの目標とみなすことができる． 情報源から出現したメッセージを送り手から受け手まで正しく送ることが可能であるための条件は，情報源と通信路との相対的な関係から定まる． この関係を明らかにしたものが情報源・通信路結合伝送定理である．情報源と通信路の統計的性質に何ら制限がないような一般的な場合には，情報スペクトルの理論（14 章）を用いることによって定理が与えられる．一方，情報源が定常無記憶情報源，通信路が定常無記憶通信路の場合は，伝送可能な条件が明確に定まるのみならず，符号器・復号器の構成について情報源に関して最適な符号と通信路に関して最適な符号とを組み合わせることで伝送定理で示される最大の効率でメッセージを伝送できることが明らかになっている． これは，情報源と通信路の分離定理と呼ばれるもので，8-3 節で紹介する．

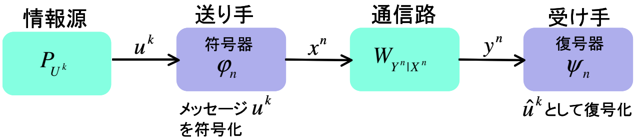

図 2　情報源・通信路結合モデル

【本章の構成】

本章では，最初に各用語の定義を明確にした後に通信路符号化定理を紹介し（8-1 節），ある特別な場合には通信路容量の効率的な計算法が存在することを示す（8-2 節）．また，情報源と通信路とを組み合わせた系における伝送可能性に関する定理を述べ，やはり特別な場合においては情報源と通信路に関して個々に最適化された符号の組合せによって，最も効率的な符号を構成できることを紹介する（8-3 節）．

■1 群 - 1 編 - 8 章

8-1 符号化定理

（執筆者：三宅茂樹）［2009 年 11 月 受領］

8-1-1 通信路容量

まず使用する記号，用語を定める．送り手が送るメッセージは集合 $\mathcal{M}$ の要素とする．$\mathcal{M}$ は有限集合で，要素数は $|\mathcal{M}|$ で表す．通信路への入力は $\mathcal{X}$ に，また出力は $\mathcal{Y}$ に属するアルファベットとする．このとき，通信路は $\mathcal{X}^n$ に属する系列 x^n（系列長を n とする）を条件とし，$\mathcal{Y}^n$ に属する系列 y^n を出力する際の条件付き確率 $W(y^n|x^n)$ によってモデル化される．本章では特に断らない限り，$\mathcal{X}$ も $\mathcal{Y}$ も有限かつ離散集合であるとし，通信路は最も基本的な定常無記憶モデル，すなわち

$$W(y^n|x^n) = \prod_{i=1}^{n} W(y_i|x_i) \tag{8・1}$$

が成り立つものを取り扱う．

メッセージ $m \in \mathcal{M}$ を決まった長さ n の $\mathcal{X}$ に属する系列で表したものをブロック符号と呼び，n をブロック長と呼ぶ．このとき，復号は長さ n の通信路出力が与えられたときに，どのメッセージが送られたかを推定するものである．正確には，ブロック符号は符号器 $\varphi_n : \mathcal{M} \to \mathcal{X}^n$ 及び復号器 $\psi_n : \mathcal{Y}^n \to \mathcal{M}'$ の組 (φ_n, ψ_n) で与えられる．ここで，復号器の値域を $\mathcal{M}$ ではなく，$\mathcal{M}' \supseteq \mathcal{M}$ とした理由は，復号器の推定は必ずしも特定の $m \in \mathcal{M}$ を出力するとは限らず，例えば，「何のメッセージが送られたかは分からないけれどエラーが発生している」という推定結果を復号器が出力する場合も含めているからで，そのために，$\mathcal{M}$ を含むより大きい集合 $\mathcal{M}'$ を復号器の値域として考えている．

ブロック長 n 及び送信メッセージ集合 $\mathcal{M}$ が与えられたとき，符号 (φ_n, ψ_n) の伝送レート R は，

$$R = \frac{1}{n} \log |\mathcal{M}| \tag{8・2}$$

で与えられる（log の底は特に断らない限り 2 とする）．すなわち，伝送レートが R であるとは，メッセージとして大体 $|\mathcal{M}| = 2^{nR}$ 個の中から何が選ばれたか，という情報を n 回の通信路の使用によって送ることに対応する（したがって，メッセージ集合 $\mathcal{M}$ は n に従って変動し得る）．また，本稿では復号誤り基準として，最大復号誤り

$$e_m(\varphi_n, \psi_n) \stackrel{\text{def}}{=} \max_{m \in \mathcal{M}} W_{Y^n|X^n}\left(\psi_n^{-1}(m)^c \,\middle|\, \varphi_n(m)\right) \tag{8・3}$$

を用いる．ただし，集合の肩にある c は補集合演算を表している．誤り基準としてはほかに平均誤り

$$e_a(\varphi_n, \psi_n) \stackrel{\text{def}}{=} \frac{1}{|\mathcal{M}|} \sum_{m=1}^{|\mathcal{M}|} W_{Y^n|X^n}\left(\psi_n^{-1}(m)^c \,\middle|\, \varphi_n(m)\right) \tag{8・4}$$

を用いたものがあるが，定常無記憶通信路の場合はどちらを用いても同じ結果を与える．

以上で通信路容量（Capacity）を定義する準備ができた．まず，達成可能レート（Acievable Rate）とは，任意の正数 $\varepsilon > 0$ が与えられたとき，伝送レート R の符号 (φ_n, ψ_n) が

$$e_m(\varphi_n, \psi_n) < \varepsilon \tag{8・5}$$

を満足するとき，R を達成可能レートと呼ぶ．この達成可能レートが様々な符号 (φ_n, ψ_n) を考えることによってある上限を持つことになるが，その上限のことを通信路容量と呼ぶ．すなわち，通信路容量を C とすると

$$C \stackrel{\mathrm{def}}{=} \lim_{\varepsilon\to 0} \sup_n \sup_{(\varphi_n,\psi_n)} \{R \,\big|\, e_m(\varphi_n, \psi_n) < \varepsilon\} \tag{8・6}$$

となる．大まかに言えば，通信路容量 C は復号誤り基準を満足する考え得るあらゆる符号 (φ_n, ψ_n) の中でとり得る最大の伝送レートである．このように通信路容量 C は操作的に定義された量であるため，ある与えられた通信路 $W_{Y|X}$ について，定義そのものから C を求めるためには，ありとあらゆる符号をチェックして，復号誤り基準を満たすものの中から伝送レートを計算して，その最大値をとる，という無限回の手順が必要となる．この通信路容量 C の計算を通信路モデル $W_{Y|X}$ に付随する量として計算可能であることを明らかにしたのが通信路符号化定理である．

8-1-2 通信路符号化定理

符号化定理は，順定理と逆定理の 2 つから成り立つ．どんな符号 (φ_n, ψ_n) を用いても達成不可能である伝送レートの下限を評価したのが逆定理で，一方，ある符号 (φ_n, ψ_n) によって達成可能な伝送レートの上限を評価したのが順定理である．逆定理で明らかにされた下限と順定理で明らかにされた上限が一致すれば，その量は通信路容量に等しい．

通信路が式 (1 · 1) で表される定常無記憶通信路の場合には，次に示すように逆定理の下限と順定理の上限とが一致する．

［**通信路符号化逆定理**］

符号 (φ_n, ψ_n) が $e_m(\varphi_n, \psi_n) < \varepsilon$ を満足するならば，その伝送レート R について

$$R \leq \max_{P_X} I(X;Y)$$

が成り立つ．ただし，$I(X;Y)$ は定常情報源 P_X と定常無記憶通信路 $W_{Y|X}$ との相互情報量である． □

証明は，Fano の不等式を用いてなされる[3)]．

［**通信路符号化順定理**］

$R < \max_{P_X} I(X;Y)$ とする．このとき，任意の正数 $\varepsilon > 0$ に対して，n が十分大きいならば伝送レートが R であるような符号 (φ_n, ψ_n) が存在して，その復号誤りについて

$$e_m(\varphi_n, \psi_n) < \varepsilon$$

が成り立つ． □

証明はランダム符号化を用いるもの[3)]や maximal 符号を用いるもの[4)]がある．

上の 2 つの定理から次の系（容量公式）が導かれる．

[**系：容量公式（定常無記憶通信路）**]

$$C = \max_{P_X} I(X;Y) \tag{8・7}$$

□

一対一の送り手と受け手から成る 2 端子伝送系の場合は，逆定理で示されるレート限界と順定理で示されるレート限界とが一致している場合が多いが，これはむしろ例外的なことである．多端子符号化問題においては（例えば放送通信路や干渉通信路など），逆定理と順定理とのギャップを埋めるのに現在に至るまで多大な努力がなされている（11 章）．

以上の結果は，通信路が定常無記憶通信路の場合であった．通信路が記憶を持つ場合，すなわち現在の通信路の出力が過去の入力に依存する場合の典型的な通信路のモデルに定常通信路がある．定常通信路とは，通信路の出力にある時間シフトを作用して，同時に入力に対しても同じだけ時間シフトを作用しても出力の確率分布は変わらないという性質で定義できる[6)]．定常通信路の容量を C_s とすると，次の容量公式が成り立つことが知られている．

［**容量公式（定常通信路）**］

$$C_s = \sup_{P_X:P_X\text{は定常確率分布}} \lim_{n\to\infty} \frac{1}{n} I(X^n;Y^n) \tag{8・8}$$

□

式 (1 · 7) と式 (1 · 8) を比べると，式 (1 · 7) は式中にブロック長 n に関する極限が入っておらず，$n = 1$ の場合の相互情報量で表されているのがわかる．この表示のことを単文字化（Single Letter Characterization）と呼ぶ．無記憶通信路の場合に容量公式が単文字化されていることのメリットの一つに，次節で述べる効率的な容量の計算アルゴリズム（Arimoto-Blahut アルゴリズム）が存在しているということがある．一方で，式 (1 · 8) の具体的な計算は一般に不可能であるか難しい場合が多い．

再び無記憶通信路の場合に戻る．関数 $c : \mathcal{X} \to \mathbf{R}$ を用いた拘束条件

$$c_n(x^n) \stackrel{\text{def}}{=} \sum_{i=1}^{n} c(x_i) \le \Gamma \tag{8・9}$$

を入力符号語に課した場合の通信路容量を $C(\Gamma)$ として，拘束条件がない場合と同様に定義する．この場合の容量公式は次で与えられる．

［**容量公式（拘束条件付き定常無記憶通信路）**］

$$C(\Gamma) = \max_{P_X:\sum_x P_X(x)c(x)\le\Gamma} I(X;Y) \tag{8・10}$$

□

符号語に制限がある場合の問題設定は，特に $\mathcal{X}$ 及び $\mathcal{Y}$ が連続的なアルファベットの場合に有効である．例えば，$c(x) = x^2$ で与えられる場合は，符号語にパワー制限を課すことになる．連続アルファベットの場合の容量を $C_c(\Gamma)$ とすると，公式は次のように表せる．

［**容量公式（拘束条件付き定常無記憶通信路：連続アルファベット）**］

$$C_c(\Gamma) = \max_{P_X:\int_x c(x)dP_X(x)\le\Gamma} I(X;Y) \tag{8・11}$$

□

制限がある場合の容量公式 (1 · 10) 及び式 (1 · 11) と有歪み情報源符号化におけるレート・歪み関数（7 章 7-1 節）との類似性に注目したい．この類似性は，一方が効率的に計算可能であれば片方も類似の方法で計算できるであろうことを示唆している．実際，8-2 節で示す容量計算のための Arimoto-Blahut アルゴリズムは，より一般的な最適化の手法である「交代最小化（Alternating Minimization）」[4]) の枠組みから統一的にアプローチできることが示されている．

以上，式 (8 · 11) を除いて離散アルファベットの場合の通信路容量公式を概観した．アルファベットが連続の場合，更には通信路が記憶を持つ最も一般の場合の結果については，情報スペクトルの議論を用いて明らかにされている（14 章もしくは韓[8]を参照）．また，定常性などの条件を課した場合の結果については，Gray[6]に詳しい．

8-1-3 信頼性関数

通信路 W が定常無記憶の場合には，$R < C$（もしくは $R > C$）のときに復号誤り率（もしくは 1 − (復号誤り率)）がどの程度の速さで 0 に近づくかについて詳細な結果が得られている．

0（もしくは 1）に近づく速さは $-1/n \log e_m$（もしくは $-1/n \log(1 - e_m)$）によって与えられる指数の大きさで評価される．この指数を信頼性関数（Reliability Function）と呼ぶ．信頼性関数の評価が精密になされれば，与えられた誤り基準 ε に対して，どの程度のブロック長 n をとれば誤り基準を満足するかに関する精密な見積もりを得ることができよう．

$R > C$ の場合，復号誤りは 1 に近づくのでその際の速度は $-1/n \log(1 - e_m)$ で与えられる．このとき次の定理が得られている．

［**定理（$R > C$ の場合の信頼性関数）**］

$$\lim_{n\to\infty} \frac{-1}{n} \log(1 - e_m) = \min_P \min_V \{D(V\|W|P) + |R - I(P, V)|^+\}$$

ただし，P は $\mathcal{X}$ 上の確率分布，V は $\mathcal{X}$ に関する $\mathcal{Y}$ 上の条件付き確率分布である．また，

$$|x|^+ = \begin{cases} x, & \text{if } x \geq 0 \\ 0, & \text{otherwise} \end{cases}$$

更に，$I(P, V)$ は相互情報量 $I(X; Y)$ を確率分布の関数とみなして表現し直したものである．

□

一方，$R < C$ の場合は，復号誤りは 0 に近づくのでその際の速度は $-1/n \log(e_m)$ で与えられるが，$R > C$ の場合と異なり指数の上界と下界にはまだギャップがあり，現在でも活発な研究がなされている．現在までに得られている上限と下限の評価のなかで代表的なものを挙げておく．

［**定理（$R < C$ の場合の信頼性関数の下限；Random Coding Bound）**］

$$\lim_{n\to\infty} \frac{-1}{n} \log(e_m) \geq \max_P \min_V \{D(V\|W|P) + |I(P, V) - R|^+\}$$

上の不等式の左辺の関数を Random Coding Bound と呼び $E_r(R)$ と表す． □

［**定理（$R < C$ の場合の信頼性関数の上限；Sphere Packing Bound）**］

$$\lim_{n\to\infty} \frac{-1}{n} \log(e_m) \le \max_P \min_{V:I(P,V)\le R} D(V||W|P)$$

上の不等式の左辺の関数を Sphere Packing Bound と呼び $E_{sp}(R)$ と表す. □

Random Coding Bound を修正する量として Expurgated Bound が，Sphere Packing Bound を修正する量として Straight Line Bound などがあり[2)]，上限と下限のギャップを克服する試みは現在まで続いている.

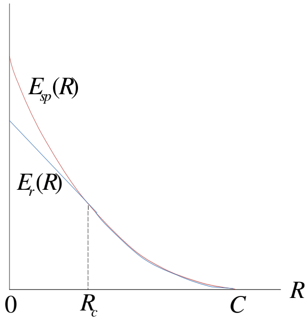

図 8･3 $R < C$ **の場合の信頼性関数の上限と下限**

図 8･3 は $R < C$ の場合の信頼性関数の上限及び下限のグラフを伝送レート R の関数として表したものである．上限と下限はグラフの傾きが 1 となる点 R_c 以下の範囲でギャップが現れている．この点 R_c は臨界レート（Critical Rate）と呼ばれる.

本節では通信路符号化定理を概観した．順定理は「良い符号」の存在定理であって，具体的な構成については明示的に述べているものではないと一般にはみなされている．ところで，Gallager はその教科書[7)]で “the difficult problem is not to find good codes of long block length but to find practical encoding and decoding techniques for such codes.”と述べている．90 年代以降のターボ符号や LDPC 符号の発展（2 編参照）により “good”であり，なおかつ “practical” な符号の実現も全くの夢物語ではなくなってきていること，更に，これら符号の構成は順定理の証明に用いられるランダム符号化と深く関係していることに注意しておく.

■1 群 - 1 編 - 8 章

8-2 通信路容量の計算法

（執筆者：三宅茂樹）[2009 年 11 月 受領]

8-2-1 通信路容量に関する簡単な例

定常無記憶通信路 W の容量公式は，式 $(1 \cdot 7)$ もしくは式 $(1 \cdot 10)$ で与えられた．以下，簡単な通信路モデルに対して具体的な容量を計算してみる．

（1）W が 2 値対称通信路（Binary Symmetric Channel）の場合

$W(y|x)$ は，

$$W(y|x) = \begin{cases} 1-\delta, & \text{if } x = y \\ \delta, & \text{otherwise} \end{cases}$$

で与えられる．このとき，容量は $\max_{P_X} I(X;Y) = 1 - h(\delta)$ となる（ただし，$h(\delta) = -\delta \log \delta - (1-\delta)\log(1-\delta)$ は 2 値エントロピー関数）．

（2）W が消失通信路（Erasure Channel）の場合

$W(y|x)$ は，

$$W(y|x) = \begin{cases} 1-\delta, & \text{if } x = y \\ \delta, & \text{if } y = \text{“erasure”} \end{cases}$$

で与えられる．このとき，容量は $\max_{P_X} I(X;Y) = 1 - \delta$ となる．

（3）W がガウス通信路の場合（$\mathcal{X} = \mathcal{Y} = \mathbf{R}$）

$W(y|x)$ は，

$$W(y|x) = \frac{1}{2\pi\sigma^2} e^{-\frac{(y-x)^2}{2\sigma^2}}$$

で与えられる．ここで，σ^2 は通信路の付加雑音である．更に，符号語 x^n に対する制約条件を $\sum_{i=1}^n x_i^2 \le \Gamma$ とする．このとき，容量は $\max_{P_X : \int x^2 dP_X(x) \le \Gamma} I(X;Y) = 1/2 \log(1 + \Gamma/\sigma^2)$ となる．

しかし，このようにあらかじめ与えられた通信路モデル W に対して容量が明示的な形で求まるのはむしろ例外で，一般には，式 $(1 \cdot 7)$ もしくは式 $(1 \cdot 10)$ の右辺の近似値を数値計算によって得るしかない．したがって，効率的な計算法があれば大変役に立つであろうことは容易に予想できる．

式 $(1 \cdot 7)$ もしくは式 $(1 \cdot 10)$ の右辺に出てくる最適化は，制約付きの最適化問題である．そこで，Kuhn-Tucker の公式を用いれば，既存の様々な非線形最適化法と組み合わせることで所望の値を求めることができる．

一方で，相互情報量 $I(P,W)$ は P に関して上に凸の関数であり，更に，制約条件は $\sum_i P_i = 1$，$P_i \ge 0$，$\sum_i P_i c_i \le \Gamma$ と，すべて線形制約である．したがって，これらの性質を有効に用いれば，より効率的な計算法が存在することが期待できる．1970 年代に Arimoto や Blahut によって発見されたアルゴリズムは（以下 Arimoto-Blahut のアルゴリズムと呼ぶ），相互情報量

や線形制約の性質を最大限に活用することによって目的値への効率的な収束を保証するものである．次の項において，このアルゴリズムを式 (1 · 10) に適用した際の計算手順を述べる．

8-2-2 Arimoto-Blahut のアルゴリズム

証明は省略するが，任意に与えられた正数 $\gamma > 0$ に対して

$$F(\gamma) = \max_{P}\{I(P, W) - \gamma c(P)\} \tag{8・12}$$

が各 $\gamma > 0$ に関して与えられれば，関数 $C(\Gamma)$ の上に凸である性質を利用することによって

$$C(\Gamma) = \min_{\gamma \geq 0}\{F(\gamma) + \gamma\Gamma\} \tag{8・13}$$

となることが示される．ただし，式 (2 · 1) において $c(P) = \sum_x P(x)c(x)$ とした．証明は，Csiszár の教科書[2)]などを参照されたい（図 8・4 参照）．

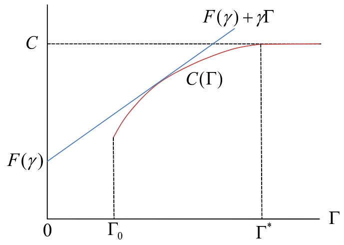

図 8・4　$C(\Gamma)$ の概形 (Csiszár[2)]**より簡略化して引用**)

図 8・4 において，Γ_0 は，$\Gamma_0 = \min_x c(x)$ で定義される点である．また，Γ^* は，$C(\Gamma)$ の折線の傾きがちょうど 0 となる点である．

以上の議論に従って，以下で $F(\gamma)$ の計算手順を示す．

$F(\gamma)$ を変形すると，

$$F(\gamma) = -\min_{P}\min_{\phi}\left\{\sum_{x,y} P(x)W(y|x)\log\frac{P(x)}{\phi(x|y)} + \gamma c(P)\right\} \tag{8・14}$$

と 2 重の最小化の形となる．

ここで，P の候補としての P_n が与えられたとする．このとき，式 (2 · 3) の右辺を ϕ に関して最小化すると，容易に

$$\phi_n(x|y) = \frac{P_n(x)W(y|x)}{P_nW(y)} \tag{8・15}$$

のときに最小値 $I(P_n, W) - \gamma c(P_n)$ が与えられることが示される．ただし，$P_nW(y) = \sum_x P_n(x)W(y|x)$ とした．

一方，ϕ の候補としての ϕ_n が与えられたとする．このとき，式 (2 · 3) の右辺を Lagrange の未定常数法を用いて P に関して最小化を実行し，その際に最小値を与える P を P_{n+1} とす

ると，

$$P_{n+1}(x) = \frac{e^{-\gamma c(x)} \prod_y \phi_n(x|y)^{W(y|x)}}{A_n} \tag{8・16}$$

ここで，A_n は規格化定数で

$$A_n = \sum_x \frac{e^{-\gamma c(x)} \prod_y \phi_n(x|y)^{W(y|x)}}{A_n} \tag{8・17}$$

で与えられる．

以上の手順を繰り返すと，結局

$$P_1 \to \phi_1 \to P_2 \to \phi_2 \to \cdots \to P_n \to \phi_n \to \cdots$$

の順番で最適化が実行され（交代最小化（Alternating Minimization）），その結果

$$I(P_1, W) - \gamma c(P_1) \to I(P_2, W) - \gamma c(P_2) \to \cdots \to I(P_n, W) - \gamma c(P_n) \\ \to \cdots \to -F(\gamma)\ (n \to \infty)$$

と $F(\gamma)$ の値へ収束することが示されている[4)]．なお，制約条件がない場合の容量 C は，上記手順において $\gamma = 0$ とすることによって得られる．

ここで述べた最適化アルゴリズムを Arimoto-Blahut アルゴリズムと呼ぶ．制約付き通信路容量 $C(\Gamma) = \max_{P:C(P)\le\Gamma} I(P, W)$ とレート・歪み関数 $R(D) = \min_{W:\sum_{x,y} P(x)W(y|x)d(x,y)\le D} I(P, W)$ の最適化の形の類似性より，レート・歪み関数の計算にも Arimoto-Blahut アルゴリズムが適用できることが予想されるが，実際，$C(\Gamma)$ の計算手順を多少変更するだけで $R(D)$ の計算が実行できることは，例えば教科書 2)[3)]にて確認できる．

一般に，ある集合 $\mathcal{P}$，$\mathcal{Q}$ が与えられた際に $\min_{P\in\mathcal{P}} \min_{Q\in\mathcal{Q}} \delta(P, Q)$（ただし，$\delta : \mathcal{P} \times \mathcal{Q} \to (-\infty, \infty]$ はあらかじめ与えられた関数とする）は，上で述べたアルゴリズムのように片方の変数を固定し，残りの変数について最適化する，ということを交互に実行する交代最小化（Alternating Minimization）によって達成されるかどうかは，自明ではない．Csiszár と Tusnády は，交代最小化によって最小値が与えられるための一つの十分条件を与えた．彼らの結果は，十分条件とはいえ幅広い適用範囲を持ち，拘束条件付き通信路容量やレート・歪み関数の計算のみならず，統計分野で使われる EM アルゴリズムの収束性についても一般的な枠組みのもとで明らかにしている．

■1 群 - 1 編 - 8 章

8-3 情報源・通信路結合符号化

（執筆者：三宅茂樹）［2009 年 11 月 受領］

8-3-1 情報源・通信路結合伝送問題

章概要の図 2 で示されるように，送り手のメッセージがある情報源の統計的法則に従って出力される際に情報源と通信路との関係がどうなっていれば受け手側の復号誤りを限りなく 0 に近づけることができるか，という問題を情報源・通信路結合伝送問題と呼ぶ．この問題は，以下のように定式化される．

情報源は有限アルファベット $\mathcal{U}^k$ 上の分布 P_{U^k} で表されるものとする．ここで，k は情報源から出現するメッセージの長さである．通信路の定義は，前節までのものと同じである．このとき，符号器 $\varphi_n : \mathcal{U}^k \to \mathcal{X}^n$ および復号器 $\psi_n : \mathcal{Y}^n \to \mathcal{U}^k$ が与えられたならば，復号誤り確率 $e(\varphi_n, \psi_n)$ は

$$e(\varphi_n, \psi_n) \stackrel{\text{def}}{=} \sum_{u^k} P_{U^k}(u^k) W_{Y^n|X^n}\left(\psi_n^{-1}(u^k)^c \,\middle|\, \varphi_n(u^k)\right) \tag{8・18}$$

によって定義される．

このとき，$\lim_{n\to\infty} e(\varphi_n, \psi_n) = 0$ を満足するような符号 (φ_n, ψ_n) に対して最も効率的な伝送レート k/n を求めること，すなわちあらかじめ与えられた任意の正数 $\varepsilon > 0$ に対して

$$\sup_{(\varphi_n,\psi_n):e(\varphi_n,\psi_n)<\varepsilon} \frac{k}{n} \tag{8・19}$$

を求めることが情報源・通信路伝送問題ということができる．

n は通信路の使用回数，k は情報源から出現したメッセージの長さであったから，k/n を大きくするということは通信路を 1 回使用当たりの情報源アルファベットの伝送速度をなるべく大きくすることを目指す．

この理論的に最も効率的な伝送レート $\sup k/n$ のことを LMTR（Limit of Maximum Transmission Rate）ともいう[2)]．

8-3-2 情報源・通信路結合符号化

前の小節で述べた情報源・通信路伝送問題も情報スペクトルの理論（14 章もしくは韓[8)]）を用いることによって，定常性やエルゴード性を仮定しない最も一般の P_{U^k} 及び $W_{Y^n|X^n}$ に対する取り扱いが可能となるが，ここでは例によって最も基本的な場合，すなわち情報源及び通信路が共に定常無記憶の場合に得られている結果を紹介する．

［情報源・通信路結合符号化定理］

情報源及び通信路が共に定常無記憶の場合，

$$\sup_{(\varphi_n,\psi_n):e(\varphi_n,\psi_n)<\varepsilon} \frac{k}{n} = \frac{C}{H(U)}$$

が成り立つ．ただし，$H(U)$ は情報源のエントロピー，C は通信路の容量である． □

いまの場合，さらに興味深いことが言える．情報源 P_U に対して圧縮限界 $H(U)$ 近くまで

圧縮を行う符号長 k のブロック符号を $(\hat{\varphi}_k, \hat{\psi}_k)$ とする．この符号の存在は情報源符号化定理（5 章）によって保証される．また，通信路 $W_{Y|X}$ に対して容量 C 近くのレートで伝送可能な符号長 n のブロック符号を $(\tilde{\varphi}_k, \tilde{\psi}_k)$ とする．この符号の存在は通信路符号化定理（4-1 節）によって保証される．このとき，符号器 $\varphi_n : \mathcal{U}^k \to \mathcal{X}^n$ および復号器 $\psi_n : \mathcal{Y}^n \to \mathcal{U}^k$ を

$$\varphi_n = \tilde{\varphi}_n \circ \hat{\varphi}_k \tag{8・20}$$

$$\psi_n = \hat{\psi}_k \circ \tilde{\psi}_n \tag{8・21}$$

とすれば，この符号 (φ_n, ψ_n) は LMTR を達成することを示すことができる．ただし，$\circ$ は関数の合成演算を表す．このことは，情報源・通信路結合系の LMTR を達成する符号を構成するには，情報源に関して最適な符号と通信路に関して最適な符号とを個別に構成して，最後に 2 つの符号を組み合わせることで可能となることを述べている．

以上のことをまとめたのが，次の定理である．

［**情報源・通信路分離定理**］

情報源及び通信路が共に定常無記憶の場合，情報源の圧縮限界 $H(U)$ を漸近的に達成する情報源符号 $(\hat{\varphi}_k, \hat{\psi}_k)$ と通信路の伝送容量 C を漸近的に達成する通信路符号 $(\tilde{\varphi}_k, \tilde{\psi}_k)$ とを式 (3·3) 及び式 (3 · 4) のように組み合わせることで，符号 (φ_n, ψ_n) を構成すれば，符号 (φ_n, ψ_n) は LMTR を達成する． □

容易に予想されるように，2 端子系において情報源や通信路がエルゴード性もしくは AEP（3 章）を持つ場合は分離定理が成り立つ．その一方で，多端子系の場合には，例え無記憶系でさえも分離定理は一般には成り立たない[5)]．

また，結合符号化定理及び分離定理は，情報源の復号に際して歪みを許す場合や，通信路入力に制限を課す場合にも，それぞれ対応する量を $R(D)$ や $C(\Gamma)$ などで置き換えることによって同様に成立する．

■参考文献

1) 韓　太舜：“情報理論における情報スペクトル的方法,” 培風館, 1998.
2) I. Csiszár and J. Körner：“Information Theory: Coding Theorems for Discrete Memoryless Systems,” Academic Press, 1982.
3) T.M. Cover and J.A. Thomas：“Elements of Information Theory 2nd Edition,” Wiley-Blackwell, 2006.
4) I. Csiszár and Tusnády：“Information geometry and alternating minimization procedures,” Statistics and Decisions, Supplement Issue I, pp.205-237, 1984.
5) T.M. Cover, A. El Gamal, and M. Salehi：“Multiple access channels with arbitrarily correlated sources,” IEEE Trans. Inform. Theory, vol.IT-26, no.6, pp.648-657, 1980.
6) R. M. Gray：“Entropy and Information Theory,” Springer-Verlag, New York, 1990.
7) R.G. Gallager：“Information Theory and Reliable Communication,” John Wiley & Sons, 1968.
8) 植松友彦：“現代シャノン理論,” 培風館, 1998.