解　説　論　文

シャノン理論
－通信路符号化定理の今昔－

Shannon Theory
— Channel Coding Theorem, Now and Then —

植松友彦 Tomohiko UYEMATSU

アブストラクト　シャノン理論とは，情報理論における各種の符号化問題に対して，符号化の限界について研究する分野である．シャノン理論の主要な研究分野は，情報源符号化，通信路符号化，乱数生成，予測，検定などであり，時代とともに広がってきている．小文では，通信路符号化定理を例として取り上げ，シャノン理論の研究対象がどのような問題であるかについて解説するとともに，符号理論との親密な関係を保ちながらシャノン理論がどのように発展してきたかについて概説する．

キーワード　シャノン理論，通信路符号化，信頼性関数，連接符号

1．シャノン理論とは何か

シャノン理論とは，97年に亡くなられたベル研究所のWyner博士の造語であり，何らかの符号化問題の限界とその限界を達成するアルゴリズムあるいは符号化法を追求する理論体系の総称である．情報源の可逆圧縮における平均符号長の限界（情報源のエントロピー）を求めることや，通信路符号化問題における任意に小さい誤り率を達成できる伝送速度の限界（通信路容量）を求めることなどがその代表的な例である．しかしながら，このような符号化のしきい値を求めることだけが，シャノン理論の問題ではない．情報源符号化定理や通信路符号化定理の精密化もまたシャノン理論の問題である．例えば情報源符号化では，1入力記号当りの平均符号長がエントロピーよりもϵ以上長い符号語が得られる確率（オーバフロー確率）を求める問題，符号長が平均符号長を中心にしてどのような分布を有するかを調べる問題などが挙げられる．一方，通信路符号化では，伝送速度が通信路容量よりも小さいとき，最も復号誤り率の小さい符号の復号誤り率が，符号長の増加に対してどのように減少するかを定める問題，そのような最良符号の具体的構成法，伝送速度が通信路容量よりも大きいとき，最良符号の復号誤り率が符号長の増加に従い，どのように変化するかを調べることなどが挙げられる．

このようにシャノン理論は新しい符号化問題を提案し，符号化という工学的操作の限界を求めることにその興味がある．例えるならば，船に乗って未知の大陸を探し，海図のない海で船が座礁しないように浅瀬や岩場の位置を明らかにする開拓者としての学問である[1]．それゆえ，シャノン理論の研究者は，実際の航路にあたる実用的な符号化法については興味がなく，他の研究者の仕事であるという立場に立つ者が多い．

小文では，通信路符号化問題を例にとり，シャノン理論の問題設定並びにその成果について解説を行うことでシャノン理論の紹介を行う．なお，小文で取り扱った信頼性関数については，既に有本と平澤による優れた解説論文[2],[3]がある．情報源符号化，多端子情報理論を含めたシャノン理論のほぼ全貌については，例えば，440篇の論文を引用したVerdúによるコンパクトな解説論文[4]を参考にされたい．

2．シャノンの通信路符号化定理

シャノンは1948年に発表した論文“A mathematical theory of communication”の2章において雑音のある通信路の符号化問題を取り上げ，次の定理を示した．

[定理1]（文献(5), Theorem 11）

通信路容量Cを有する離散通信路と単位時間あたりのエントロピーHを有する情報源を考えよう．もし，$H \leqq C$ならば，ある符号化法が存在して，情報源の出力を通信路を通じて任意に小さい誤り率（または任意に小さいあいまい度）で伝送することができる．他方，もし$H > C$ならば任意の$\epsilon > 0$に対し，通信路出力におけるあいまい度を$H - C + \epsilon$以下にするような符号化は可能だが，あいまい度を$H - C$以下にできるような符号化法は存在しない．

情報源として，単位時間あたりのエントロピーがRビット（これは伝送速度Rに対応）の一様分布に従う情報源を考えれば，この定理は，伝送速度Rが通信路容量よりも真に小さければ，任意に小さい誤りで通信が行えるというおなじみの通信路符号化定理にほかならないことが分る．

シャノン以前の時代には，伝送速度と通信の信頼性との間にはトレードオフがあると信じられており，誤り率の小さい

植松友彦　正員　東京工業大学大学院 理工学研究科 集積システム専攻
E-mail　uyematsu@ieee.org
Tomohiko UYEMATSU, Member (Dept. of Communications and Integrated Systems, Tokyo Institute of Technology, Meguro-ku, 152-8550 Japan).
Fundamentals Review Vol. 1 No. 1 pp. 8-18 2007年7月

高信頼な通信を行うには伝送速度を犠牲にするしかないと思われていた．シャノンの成果は，真にトレードオフ関係があるのは，符号化・復号化による遅延時間と信頼性の間であり，伝送速度を通信路容量よりも小さく保てば，符号長を長くすることで任意に小さい誤り率を達成できることを示したところにその眼目がある．

このように，符号化問題における限界（この場合は通信路容量）を明らかにするのが，シャノン理論の最初の一歩である．

3. Elias の繰り返し符号

シャノンの論文[5]には，任意に小さい誤り率を達成する符号の存在を示しているものの，そのような符号の作り方については，全く言及していない．そこで，次の目標は，符号長を長くしたとき任意に小さい誤り率を達成する符号を実際に作ることである．「その程度のことは誤り訂正符号を使えば簡単にできるよ」というのは今だから言える話であり，シャノンの論文の時代では，リードソロモン符号（Reed-Solomon Code）（1960 年）はおろか BCH 符号（1959 年）さえ見つかっていなかった．このように符号理論の援護が望めない時代に，この問題を最初に解いたのが，Elias である[6]．

Elias は 1954 年に，繰り返し符号（Repetition code）という符号化法を提案し，伝送速度を非零に保ったまま，符号長を長くしたとき誤り率を零に近づけることのできる符号の構成法を初めて示した[6]．以下では Elias のアイデアについて述べる．

いま，図 1 で示した誤り率 P_0 の二元対称通信路を考えよう．この通信路では，送信した記号（0 または 1）が確率 P_0 で他方の記号に誤って受信される．まず，最初の符号化として，符号長 N_1 の単一誤り訂正，二重誤り検出符号（実際には拡大ハミング符号を考えればよい）を用いる．この符号を二元対称通信路を通じて送信したとき，復号器では，1 個の誤りを検出したときは訂正し，偶数個の誤りを検出したときは誤り訂正を行わないことにすれば，復号後の 1 符号語中の誤りの個

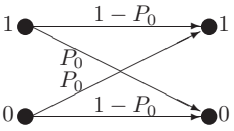

図 1　二元対称通信路

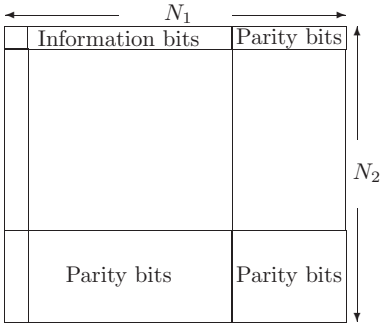

図 2　第 1 段と第 2 段の符号化

数 M_1 は，$N_1P_0 \leqq 3$ ならば，簡単な計算により

$$\begin{aligned} M_1 &\leqq \sum_{\substack{i:\text{even}\\ i\geqq 2}}^{N_1} i\binom{N_1}{i}P_0^i(1-P_0)^{N_1-i} \\ &\quad + \sum_{\substack{i:\text{odd}\\ i\geqq 3}}^{N_1}(i+1)\binom{N_1}{i}P_0^i(1-P_0)^{N_1-i} \\ &\leqq N_1(N_1-1)P_0^2 \end{aligned}$$

となる．従って，復号後の符号語中のあるビットに誤りが生じている確率 P_1 は

$$P_1 = M_1/N_1 \leqq (N_1-1)\,P_0^2 < N_1P_0^2$$

となり，$N_1P_0 < 1$ ならば，$P_1 < P_0$ であり，符号化によって誤り率が減少することになる．

次に，これらの符号語を各行に並べ，列方向に符号長 N_2 の拡大ハミング符号によって符号化することを考える（図 2）．この符号も最初の符号と同様に復号するとすれば，復号後のあるビットに誤りが生じている確率 P_2 は

$$P_2 < N_2P_1^2 < N_2N_1^2P_0^4$$

となる．以下，この操作を k 段繰り返すことで，各ビットの誤り率は

$$P_k < N_k^{2^0}N_{k-1}^{2^1}\cdots N_1^{2^{k-1}}\cdot P_0^{2^k}$$

となる．ここで，各段の拡大ハミング符号の符号長を 2 倍ずつ長くすることとし，符号長を $N_1 = 2^\ell$，$N_j = 2^{j-1}N_1$（ℓ は正整数，$j = 1, 2, \ldots, k$）によって定めると

$$P_k < \frac{1}{N_1}(2N_1P_0)^{2^k}\cdot 2^{-(k+1)}$$

が得られ，$N_1P_0 \leqq 1/2$ ならば，

$$P_k \to 0 \quad (k\to\infty)$$

となる．

一方，k 段の符号化を行った際の符号の伝送速度 R_k は，不等式 $(1-a)(1-b) > 1-(a+b)$ を用いると

$$R_k = \prod_{j=1}^{k}\left(1-\frac{j+\ell}{2^{j+\ell-1}}\right) > 1-\frac{\ell+2}{2^{\ell-1}}$$

で下から抑えられ，$\ell > 3$ すなわち $N_1 > 8$ ならば，伝送速度 R_k は段数 k を大きくしても零にはならない．以上のことから，通信路の誤り率 P_0 が小さいとき，符号長を長くすることで任意に小さい誤り率を達成する非零の伝送速度を有する符号が

構成できたことになる．

多重誤りが訂正できるBCH符号やリードソロモン符号が発見される以前に，任意に小さい誤り率を達成する符号を作ったという点で，Eliasの成果は特筆に値する．また，何段にもわたり符号化および復号化を繰り返すというEliasの手法は，この後，各種の符号構成において用いられる基本的なテクニックとなる．

4．信頼性関数の導出

50年代の半ばころから，MITにおけるシャノン門下生は，通信路符号化定理の精密化について検討を始めた．すなわち，通信路容量よりも真に小さい伝送速度において，最良の符号の復号誤り率は，符号長nに対して，どのような減少関数になるのかという問題を考えた．

この問題について，まず，Eliasは二元対称通信路に対する復号誤り率が符号長の指数関数的に減少することを示した[7]．このような誤り率を定める指数関数の指数部の係数のことを「信頼性関数(reliability function)」あるいは「誤り指数(error exponent)」と呼ぶ．任意の離散無記憶通信路における信頼性関数の上界と下界はFanoによって与えられた[8]．

この後，Gallagerによって，ランダム符号化法を用いたときの平均誤り率に対する信頼性関数の下界を初等的に求める方法が提案された[9]．このGallagerによる成果を次の定理に示す．

[定理2]（文献(9)，Theorem 2）

入力アルファベット$\mathcal{X}$，出力アルファベット$\mathcal{Y}$を有する離散無記憶通信路が条件付確率$W(b|a)$（$a\in\mathcal{X}$，$b\in\mathcal{Y}$）によって与えられるとする．このとき，任意の符号長N，任意の伝送速度Rに対し，復号誤り率p_eが

$$p_e \leqq \exp\{-NE_r(R)\}$$

を満足する符号が存在する．ただし，

$$E_r(R) \triangleq \max_{\substack{\rho:0\leqq\rho\leqq 1\\ Q}} [-\rho R + E_0(\rho,Q)]$$

$$E_0(\rho,Q) \triangleq -\ln \sum_{b\in\mathcal{Y}} \left(\sum_{a\in\mathcal{X}} Q(a)W(b|a)^{1/(1+\rho)} \right)^{1+\rho}$$

であり，maxは$0\leqq\rho\leqq 1$を満足するρと$\mathcal{X}$上の確率分布Qについて取られる．

この定理における$E_r(R)$は「Gallagerの信頼性関数」あるいは「ランダム符号化による信頼性関数」と呼ばれる．この名前の由来は，確率分布Qを有する無記憶情報源からの長さ$N\exp\{NR\}$の出力系列を長さNのブロック$\exp\{NR\}$個に区切り，各々のブロックを符号語として得た「ランダム符号」の復号誤り率の平均値が上記の限界式を満足することに起因する．

信頼性関数$E_r(R)$について，Gallagerは次の性質を示した．

[定理3]（文献(9)，Theorem 3）

任意の離散的無記憶通信路において，$E_r(R)$は$0\leqq R<C$の範囲で下に凸であり，かつ正の値を取る連続関数である．従って，復号誤り率の限界式

$$p_e \leqq \exp\{-NE_r(R)\},$$

は$0\leqq R<C$において符号長Nに対して指数関数的に限少する．

更に，Gallagerは伝送速度が小さいところでは，復号誤り率の上界が改善できることを示した．

[定理4]（文献(9)，Theorem 6）

定理2と同一条件で，任意の符号長N，任意の伝送速度Rに対し，復号誤り率p_eが

$$p_e \leqq \exp\{-NE_{ex}(R)\},$$

を満足する符号が存在する．ただし，

$$E_{ex}(R) \triangleq \max_{\substack{\rho:\rho\geqq 1\\ Q}} [-\rho R + E_x(\rho,Q)]$$

$$E_x(\rho,Q) \triangleq -\rho\ln \sum_{a,a'\in\mathcal{X}} Q(a)Q(a') \times \left(\sum_{b\in\mathcal{Y}} \sqrt{W(b|a)W(b|a')} \right)^{1/\rho}$$

であり，maxは$\rho\geqq 1$を満足するρと$\mathcal{X}$上の確率分布Qについて取られる．

$E_0(1,Q)=E_x(1,Q)$が成り立つので，十分小さな$R>0$に対して，一般に$E_r(R)<E_{ex}(R)$が成り立つ．信頼性関数$E_{ex}(R)$のことを「修正信頼性関数」あるいは「削除誤り指数(expurgated error exponent)」という．図3に，誤り率$P_0=0.01$の二元対称通信路に対するGallagerの信頼性関数$E_r(R)$及び修正信頼性関数$E_{ex}(R)$を示す．

Gallagerの成果は，後にForneyによって拡張され，復号時に誤り検出を許した場合，リスト復号法を用いた場合，フィードバックを許した場合などの信頼性関数が導出されている[10]．

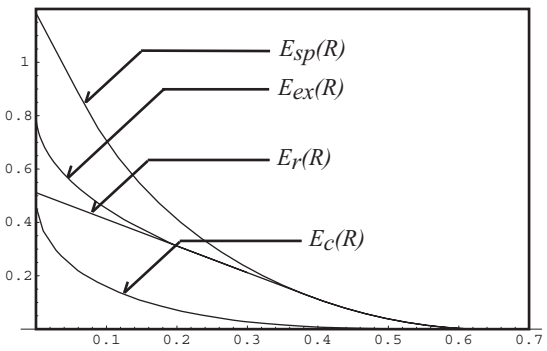

図3　二元対称通信路(P_0=0.01)における信頼性関数

一方，どのように巧妙な符号化・復号化を行っても達成できない復号誤り率の下界についても考察が行われており，次の成果がShannonの最後の論文で示されている．

[定理5]（文献(11)，Theorem 2）

離散無記憶通信路Wに対し，符号長N，伝送速度Rを有する任意の符号の復号誤り率p_eは

$$p_e \geqq \exp\{-NE_{sp}(R)\}$$

を満足する．ただし，

$$E_{sp}(R) \triangleq \max_{\substack{\rho:\ \rho>0 \\ Q}} [-\rho R + E_0(\rho, Q)]$$

である．

$E_{sp}(R)$のことを「球充てんの指数（sphere packing exponent）」と呼ぶ．$E_{sp}(R)$と$E_r(R)$の定義を比べることで，ある伝送速度R_cが存在して，

$$E_{sp}(R) = E_r(R) \quad R_c < R < C$$

が成り立つことが分る．従って，高伝送速度においては，復号誤り率を最小にする最適な符号によって達成できる復号誤り率の指数部が完全に決定できることになるが，低伝送速度においてはまだ上界と下界のギャップが残っている．この問題は現在も解けておらず，40年以上にわたる未解決問題である．図3に，誤り率$P_0 = 0.01$の二元対称通信路に対する球充てんの指数$E_{sp}(R)$を示す．

5. Forneyの連接符号

Gallagerの信頼性関数の導出法では，復号法として最ゆう復号法を仮定していた．最ゆう復号法は優れた復号誤り率を達成できるものの，その計算量は符号長の指数関数となり，符号長が短い場合を除いて実用性はほとんどない．従って，復号法の計算量に何らかの制限を与えたとき，どの程度の復号誤り率が得られるのかについて調べる必要がある．この問題について，66年にMITのForneyは実用的な計算量によって符号化・復号化が行える符号で，通信路容量よりも小さい伝送速度において誤り率が零に漸近する符号として連接符号を提案した[12]．

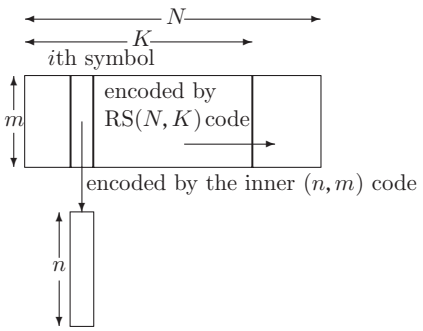

図4　連接符号の構成

連接符号は$GF(p^m)$上の符号長$N = p^m - 1$，次元Kのリードソロモン（RS）符号でメッセージを符号化した後，RS符号の符号語$(w_1, w_2, \ldots, w_N)$を構成する各記号$w_i \in GF(p^m)$を$GF(p)$上のm次元ベクトルとみなし，これを更に$GF(p)$上の符号長n，情報記号数mの(n, m)符号で符号化して通信路に送信する方法である（図4）．このとき，最初に符号化を行うRS符号のことを通信路から見て外側に位置する符号なので外部符号といい，2度目の符号化を行う符号のことを内部符号という．連接符号は$GF(p)$上で符号長$N_o = nN$，伝送速度$R_o = Km/Nn$を有している．Forneyの論文中には明示されてはいないが，連接符号はEliasの繰り返し符号のアイデアを利用している．しかしながら，繰り返し符号とは異なり，繰り返しの段数を2段に固定できたのは，強力な誤り訂正能力を有するRS符号の恩恵による．従って，60年のRS符号の発明なしには連接符号はなかったといっても過言ではない．

連接符号の復号は，まず内部符号を最ゆう復号法によって全て復号した後，外部符号を一般化最小距離復号法[13]で復号することによって行われる．このとき，内部符号語1個を最ゆう復号する際の計算量は高々p^m（$= N + 1$）回のゆう度の比較で済み，これは符号長$O(N)$の計算量で行える．従って，内部符号全体の復号の計算量は高々$O(N^2)$で済む．ここに連接符号の最大のトリックがある．一方，外部符号の一般化最小距離復号法は，高々$D = N - K + 1$回の代数的復号法の繰り返しで行えるから，高々$O(N^3)$の計算量で行える．従って，連接符号の復号法の計算量は高々$O(N^3)$である．このように，Forneyは外部符号の符号語の各記号を内部符号で符号化するという2段階符号化と，最小距離までは効率的な復号が可能なRS符号を外部符号に利用することで符号長を長くしても十分に実用的な計算量で復号が行える符号を提案したのである．

次に，連接符号の誤り率を計算してみよう．内部符号として，Gallagerの信頼性関数を達成する伝送速度Rの符号を用いたとすれば，RS符号語の各記号の誤り率pは，

$$p \leqq \exp\{-nE_r(R)\}$$

を満足し，外部符号では最小距離Dの半分にあたる$t = \lfloor (D-1)/2 \rfloor$個までの誤りを訂正可能なので，限界距離復号法を用いたときの誤り率は，RS符号語の$t+1$個以上の記号に誤りが生じる確率

$$\begin{aligned} p_e &\leqq \sum_{j=t+1}^{N} \binom{N}{j} p^j (1-p)^{N-j} \\ &\leqq \sum_{j=t+1}^{N} \binom{N}{j} \exp\{-njE_r(R)\} \\ &\leqq 2^N \exp\{-n(t+1)E_r(R)\} \\ &\leqq \exp\{-N_o(1-r)E_r(R)/2 + (\ln 2)/n\} \end{aligned}$$

によって抑えられる．ただし，$N_o = nN$は連接符号全体の符号長であり，$r = K/N$は外部符号の伝送速度である．これから，連接符号の復号誤り率は符号長N_oの指数関数で減少することが分る．一方,外部符号を一般化最小距離復号法によって復号した連接符号の復号誤り率については，次の定理が成り立つ．

[定理6]（文献（12），Chapter 4）

伝送速度Rを有する符号長nの内部符号の復号誤り率pが

$$p \leqq \exp\{-nE_r(R)\}$$

を満足するならば，外部符号として符号長N，情報記号数KのRS（N，K）符号を用いた連接符号全体の復号誤り率は，

$$p_e \leqq \exp\{-N_o(1-r)E_r(R)\}$$

を満足する．

ここで，内部符号の伝送速度Rと外部符号の伝送速度rは，全体の伝送速度$R_o = rR$を満足する範囲で任意に定めることができるので，復号誤り率p_eが

$$p_e \leqq \exp\{-N_o E_c(R_o)\}$$

を満足するような符号が構成できる．ただし，

$$E_c(R_o) = \max_{r,R:rR=R_o}(1-r)E_r(R)$$

である．この信頼性関数$E_c(R_o)$のことを「Forneyの信頼性関数」あるいは「連接符号の信頼性関数」と呼ぶ．簡単な計算によりForneyの信頼性関数は

$$0 < E_c(R) \leqq E_r(R) \quad 0 \leqq R < C$$

を満足する．この結果から,連接符号は,$0 \leqq R < C$において，復号誤り率が符号長の指数関数的に減少する符号であることが分る．また，信頼性関数の大きさと復号の計算量はトレードオフの関係になっており，復号の計算量を制限したことにより，連接符号の信頼性関数はGallagerの信頼性関数に及ばない（図3）．

連接符号は，短い符号長の良い符号を用いて十分長い符号長の符号を構成する方法と見ることもできる．短い符号長においては，復号誤り率の小さい（例えばGallager の信頼性関数を満たす）良い符号を見つけることは比較的容易なので，実用的な範囲の符号長において強力な符号構成法となる．文献（12）においては，復号誤り率が指定されたとき，符号長が数10 ～数100 のBCH符号を内部符号に用いて，全体の符号長が数1000 から数100 万までの連接符号の構成例が二元対称通信路とAWGN（Additive White Gaussian Noise）通信路について示されている．

Forneyの連接符号の提案から約15年後の80年に，Hirasawa，Kasahara，Sugiyama，Namekawa [14] によって，伝送速度の異なる外部符号を複数個用意し，内部符号と外部符号を交互に復号することで，連接符号の信頼性関数が改善できることが示されている．この復号法は現在のLDPC 符号等で用いられている繰り返し復号法に通じるところがあり，今から見ると大変興味深い．

Forney による連接符号の提案以降，符号理論の発展にもかかわらず，符号長を長くしたとき，任意に誤り率を小さくできる符号としては，繰り返し符号と連接符号の2種類しかないという状態が約30年間続くことになる．

6．ユニバーサル符号化の波

70年代に入るとシャノン理論の研究者の間で情報源のユニバーサル符号化が盛んに議論されるようになった．情報源のユニバーサル符号化とは，情報源のクラス（無記憶情報源，マルコフ情報源，定常エルゴード情報源など）が分っていれば，情報源の確率分布を一切知らなくても，入力列が長くなるにつれて,1 入力記号当りの符号長の期待値がエントロピーに漸近するような符号化法である．73年のDavissonの論文[15]を皮切りに，ユニバーサル符号の決定版となるZivとLempelによる2種のZiv-Lempel符号の提案[16]，[17]まで，多くの研究者によって情報源のユニバーサル符号化は研究された．

情報源のユニバーサル符号化問題がひと区切りついたとき，自然に浮かぶ次の問題は，通信路のユニバーサル符号化問題である．すなわち，通信路の統計的性質をあらかじめ知らなくても，符号化や復号化を行うことができ，その符号の伝送速度が通信路容量よりも小さければ，符号長を長くすることで，任意に小さい復号誤り率を達成できるような符号が存在するかということである．

通信路のユニバーサル符号化問題を初めて解いたのはハンガリーの研究者Csiszár，Körner，Martonの3人であり，77年のCornell大学で開催されたIEEE ISIT（Int．Symp．on Information Theory）で彼らは次の定理を示した．

[定理7]（文献（18），（19））

入力アルファベット$\mathcal{X}$，出力アルファベット$\mathcal{Y}$を有する無記憶通信路Wにおいて，任意の$\delta > 0$と十分大きな符号長Nに対して復号誤り率p_eが

$$p_e \leqq \exp\{-N(E_r(R) - \delta)\}$$

を満足する符号で，符号化および復号化が通信路Wに依存しないものが存在する．

Csiszárらは，このユニバーサルな通信路符号がタイプ一定符号[8]（符号語中における各記号の経験分布が符号語によらず一定）とGoppaによって提案された最大相互情報量復号法[20]を組み合わせることによって得られることを示した．しかしながら，彼らの証明はランダム符号化に基づくものであり，Gallagerの成果同様に何ら具体的な符号構成法を示唆するも

のではない．

この後，ユニフィラーな有限状態通信路に対するユニバーサル通信路符号化定理が85年にZiv [21]によって，ユニフィラーでない一般的な有限状態通信路に対するユニバーサル通信路符号化定理が98年にLapidothとZiv [22]によって示されている．また著者らは，通信路のユニバーサル符号化における復号器として，情報源のユニバーサル符号化器が利用できるための十分条件を与えている[23]．この成果は，情報源と通信路の双対性を示す成果とも考えられ，興味深い．

通信路のユニバーサル符号化については，紙面の都合もありこれ以上述べることはできない．しかしながら，ユニバーサル性は情報理論の本質の一つでもあり，シャノン理論では個々の符号化問題において，ユニバーサル符号の存在について調べることは常に重要な問題である．

7．通信路容量を達成する符号の代数的構成法

Forneyの連接符号は，通信路容量より小さい伝送速度に対して実用的な計算量で任意に小さい復号誤り率を達成できる．しかしながら，連接符号の構成には，Gallagerの信頼性関数を達成する良い内部符号を見つける必要があり，連接符号の符号長を長くすると内部符号の符号長も長くなるため，実際に良い内部符号を見いだすことは困難である．従って，連接符号では，Forneyの信頼性関数を達成する符号の存在は示せるものの，具体的な符号の構成には内部符号の探索が必要である．

この問題点を解決し，内部符号の探索を一切行わずに，実用的な計算量で任意に小さい復号誤り率を有する連接符号を構成する方法が82年にDelsarteとPiretによって提案された[24]．

Delsarte と Piret は漸近的に性能の良い(注1) Justesen符号[25]の構造に着想を得て，内部符号を1種類だけではなく複数種類を取り換えて用いることで，良い内部符号を探すことなく連接符号が構成できることを示した．彼らの符号構成法は次のように述べられる．同一の符号長n，伝送速度Rを有する内部符号の集合をGとし，内部符号$g \in G$に対する復号誤り率を$p_e(g)$とするとき，Gに属する符号全部にわたる復号誤り率の平均値が

$$\frac{1}{|G|}\sum_{g\in G} p_e(g) \leqq \exp\{-nE_r(R)\}$$

を満たすものとする．このとき，符号長$|G|$を有するRS符号の符号語$(w_1, w_2, \ldots, w_{|G|})$の$i$$(=1, 2, \ldots, |G|)$番目の記号$w_i$を$G$に属する$i$番目の符号$g_i$で符号化した連接符号を構成すれば，対称通信路に対して，符号長を長くすることで任意に小さい誤り率が達成できることを示した．ただし，$|G|$は内部符号の集合Gの要素の総数を表す．このことは，一つ一つの内部符号の復号誤り率が分らなくても集合Gに属する符号全体の復号誤り率の平均値が信頼性関数$E_r(R)$を達成すれば，連接符号の構成には十分であることを意味しており，ランダム符号化と具体的符号構成法の掛け橋となるすばらしい成果である．

DelsarteとPiretは内部符号の集合Gの構成法を2種提案し，次の定理を示した．

[定理8]（文献(24)）

q元入力対称通信路（qは素数のべき乗）に対して，復号誤り率p_eが

$$p_e \leqq \frac{2s}{1-r}\left(\frac{s\log_g N_0}{2N_0}\right)^{\frac{E_r(R)}{2}}$$

を満足する連接符号が代数的に構成できる．ただし，rは外部符号の伝送速度，Rは内部符号の伝送速度，N_oは連接符号全体の符号長を表し，$s \geqq \lceil 2/r \rceil$である．他方，$q$元入力の正規通信路(注2)に対しては，任意の$\epsilon > 0$と十分大きな$N_o$に対し，復号誤り率が

$$p_e \leqq \exp\{-N_o(1-r)(E_r(R)-\epsilon)/(2t)\}$$

を満足する連接符号が代数的に構成できる．ただし，$t = \lceil 1/r \rceil - 1$である．

なお，DelsarteとPiretの構成法では常に$t \geqq 1$となるので，ここで構成された連接符号は常にForneyの信頼性関数より小さいことに注意しておく．

8．連接符号の最ゆう復号

Forneyの連接符号は，復号化を2段階によって行うことで復号の計算量を減少させていた．それでは，復号の計算量に一切制約を与えず，連接符号全体を最ゆう復号した場合の復号誤り率はどうなるのだろうか．連接符号はGallagerの信頼性関数を達成できるのであろうか．この問題は実用的な面からはほとんど興味はない．しかしながら，シャノン理論の立場から見ると，Gallagerの信頼性関数を達成できる「ランダム」ではない符号がどのような構造を有しているのかを知ることの一助であり，Gallagerの信頼性関数を達成できる符号のクラスを制限する重要な問題である．

Thommesenは，87年にこの問題について考察し，DelsartとPiretによる連接符号と同様に，RS符号を外部符号とし，すべ

(注1)：符号長を長くしても，最小距離と符号長の比ならびに伝送速度が共に零に漸近しない符号のクラスを漸近的に性能の良い符号と呼ぶ．

(注2)：入力アルファベット$\mathcal{X} = GF(q)$を有する離散的無記憶通信路において，$a \in \mathcal{X}$に対して$\mathcal{Y}$上の置換Ψ_aが存在して，

$$\Psi_a(\Psi_{a'}(b)) = \Psi_{a+a'}(b)\ \forall a, a' \in \mathcal{X},\ b \in \mathcal{Y}$$

が成り立つとする．このとき，通信路の遷移確率$W(b|a)$が$\Psi_a(b)$によってのみ定まるとき，この通信路を正規通信路という．正規通信路の例として，二元対称通信路や二元対称消失通信路等がある．

ての内部符号をランダム符号化によって選んだときの平均復号誤り率を評価し，次の結果を得た．

[定理9]（文献（26），Theorem 3 and 4）

離散的無記憶通信路に対し，内部符号を可変とする符号長N_o，伝送速度R_oを有する連接符号が存在して，

$$p_e \leqq \exp\{-N_o E_r(R_o)\}$$

を満足する．特に，正規通信路に対しては，修正信頼性関数を達成する連接符号が存在する．すなわち

$$p_e \leqq \exp\{-N_o E_{ex}(R_o)\}$$

を満たす連接符号が存在する．

Thommesenの成果により，連接符号は最ゆう復号によって復号しても優れた符号であることが確認された．なお，Thommesenの論文には明記されてはいないが，Gallagerのランダム符号化では，符号長N_o，伝送速度R_oの符号の構成に，分布Pを有する無記憶情報源からの長さ$N_o \exp\{N_o R_o\}$の系列が必要であったが，Thommesenの構成法では，同一の無記憶情報源からの長さ$nN\exp\{nR\} = N_o \exp\{nR\}$の系列があれば良い．このことは，連接符号を利用することで，ランダム符号の構成に必要なランダム列の長さを大幅に減少できることを示している．

9. 代数幾何符号とシャノン理論

80年代後半の符号理論の中心的なテーマは符号化変調方式と代数幾何符号の二つであった．このうち符号化変調方式は，通信路容量まで1 dB程度以上の信号対雑音比を有するAWGN通信路に対しては，畳込み符号と多値変調方式を一体化して設計することで実用的な計算量で符号化と復号化が行えることを示しており，高速モデムや高速無線通信等でよく利用された．一方，代数幾何符号[27]は，多元ではVarshamov-Gilbert限界（文献（28），p. 557 Theorem 31）を越える符号が構成できるということでRS符号に代わる高性能符号として注目されたが，その後の90年代のターボ符号とLDPC符号の台頭により，未だ実用化には至ってはいない．この理由の一端は，代数幾何符号の復号の計算量がRS符号と同様に符号長の二乗以上のオーダになっているためと思われる．ここでは，この代数幾何符号のシャノン理論への応用例について述べる．

DelsarteとPiretによる連接符号の代数的構成法において，信頼性関数がForneyの信頼性関数よりも小さくなってしまう原因は次の2点にある．

(1) 外部符号を一般化最小距離復号ではなく限界距離復号法によって復号していること

(2) 使用する内部符号の種類が多い場合（低伝送速度の場合），$p^m < |G| \leqq p^{m'}$を満足する有限体$GF(p^{m'})$においてRS符号を構成するため，RS符号の符号語の各記号を$t = m'/m$（>1）個に分割して，同一の内部符号をt回用いて符号化していること

このうち，(1)については外部符号を一般化最小距離復号に変更すれば，直ちに改良できるが，(2)についてはRS符号を使っている限り，定義体を保ったまま符号長を無制限に長くすることはできないので改良は望めない．

著者らは，RS符号の代りに代数幾何符号の一つである一般化エルミート曲線符号（generalized Hermitian code）[29]を用いることで(2)の改良を行った．一般化エルミート曲線符号とは$GF(2^{2m})$上の線形符号であり，符号長N，情報点数K，最小距離Dが

$$\begin{aligned} N &< 2^{m(l+1)} \\ K &\leqq N - g(l,m) \\ D &\geqq N - K + 1 - g(l,m) \end{aligned}$$

を満足する．ただし，$g(l, m) \geqq 0$は種数と呼ばれ

$$\lim_{m\to\infty} \frac{g(l,m)}{2^{m(l+1)}} = 0$$

を満足する．ここで，符号長$N = 2^{m(l+1)} - 1$の一般化エルミート曲線符号は，mが十分大きければ$g(l, m)/N \approx 0$であるので，

$$R \approx 1 - \frac{D}{N}$$

が成り立ち，最大距離分離符号（RS符号）とほぼ同様な性質を有することが分る．著者らは，DelsarteとPiretによる符号構成法における外部符号に一般化エルミート曲線符号を用い，一般化最小距離復号法で復号することにより次の定理を得た．

[定理10]（文献（30），定理4）

任意の$\epsilon > 0$と十分大きな符号長N_oについて正規通信路における復号誤り率が

$$p_e \leqq \exp\{-N_o(E_c(R) - \epsilon)\}$$

を達成する連接符号が代数的に構成できる．

この定理は，Forneyの信頼性関数を達成する連接符号が代数的に構成できることを示しており，連接符号の構成問題に終止符を打つものである．この後，著者らは，この成果の一般の無記憶通信路に対する拡張も行っている[31]．また，Thommesenの成果と同様に，外部符号に代数幾何符号（モジュラー符号）を用い，内部符号をランダム符号化したときに得られる連接符号を最ゆう復号したとき，Gallagerの信頼性関数が達成できることも示した[32]．

10. LDPC 符号とシャノン理論

90 年代に入るまでは，良い符号について，“There are few known constructive codes that are good, fewer still that are practical, and none at all that are both practical and very good.” [33] という共通の認識があった．これを打ち破ったのが，93 年に出現したターボ符号 [34] と，95 年に MacKay と Neal [35] によって再発見された Gallager の LDPC（Low-Density Parity-Check）符号 [36] である．これらの符号は，何らかのランダム性を用いて構成されているため，必ずしも美しい代数的構造を有するものではないが，ランダム符号に近い性質を有するため，優れた性能を持つと理解されている．99 年に MacKay が数値計算とシミュレーションによって，LDPC 符号が通信路容量に漸近する性質を有することを示し [33]，シャノン理論の問題として，これらの符号のクラスで通信路容量を達成できるかということが議論されるようになった．

この問題について重要な役割を果たすのが，99 年に Shulman と Feder によって得られた成果である [37]．彼らは，与えられた確定的な符号から，符号の集合（アンサンブル）を作り，Gallager のランダム符号化をこの符号の集合について適用することで元の符号の復号誤り率を求める方法を提案した．この手法は，後に，通信路容量よりも真に小さい伝送速度を有する LDPC 符号が任意に小さい誤り率を達成できることを示すのに用いられた．以下では，Shulman と Feder の手法 [37] を述べる．

入力アルファベット $\mathcal{X}=\{0, 1\}$，出力アルファベット $\mathcal{Y}=\{-M, \cdots, 0, \cdots, M\}$ を有する無記憶通信路 W が

$$W(b|0)=W(-b|1) \quad \forall b\in\mathcal{Y}$$

を満足するとき，この通信路を「二元入力対称出力通信路（binary-input output-symmetric channel）」という．二元入力対称出力通信路において，二元線形符号 C を用い，最ゆう復号によって復号した場合，次の三つの操作に対して，復号誤り率は不変である．

(1) 符号語中の各記号の順序を置換すること
(2) 情報系列と符号語の一対一対応を取り換えること
(3) すべての符号語に同一の二元ベクトルを加えること

そこで，符号 C に上記の (1)，(2)，(3) の操作を順に行うことで得られる符号全体の集合を $\mathcal{C}$ によって表す．このとき，$\mathcal{C}$ に含まれる符号 $C'\in\mathcal{C}$ の復号誤り率はすべて等しい．他方，符号の集合 $\mathcal{C}$ については，Gallager のランダム符号化のテクニックによって復号誤り率を容易に評価することができ，次の定理が得られる．

[定理 11]（文献 (37)）

二元 (N, K) 符号 C を 2 元入力対称出力通信路に適用したときの復号誤り率は

$$p_e\leqq\exp\{-NE_r(R+(\ln\alpha)/N)\}$$

によって上から抑えられる．ただし，

$$\alpha=\max_{0<l\leqq N}\frac{A_l}{2^K-1}\cdot\frac{2^N}{\binom{N}{l}}$$

であり，A_l は符号 C の重み l の符号語の総数を表す．

この定理から，二元符号 C の重み分布が，ほぼ 2 項分布ならば，すなわち

$$A_l\approx\binom{N}{l}2^{K-N}$$

を満足するならば，この符号 C の復号誤り率は

$$p_e\leqq\exp\{-NE_r(R)\}$$

を満足し，Gallager の信頼性関数を達成できることになる．従って，符号の重み分布から，その符号を最ゆう符号したときの復号誤り率の上界が求まり，その符号の性能を評価できる．このような点で，Shulman と Feder は，二元符号の最ゆう復号に対して，測り知れない影響を与えた．

2001 年に Miller と Burshtein は，Shulman と Feder による定理 11 を LDPC 符号に応用し，ある種の LDPC 符号を最ゆう復号したときの復号誤り率について次の定理を示した．

[定理 12]（文献 (38)，Theorem 6）

$N-K$ 行 N 列から成る全零行列の各列において，一様分布に従い重複を許して t 回ランダムに要素を選び，その要素の 1 と 0 を反転して得られるパリティ検査行列によって定まる伝送速度 R（$\geqq K/N$）の二元 LDPC の集合を考えよう．このようにして作られる LDPC 符号を二元入力対称出力通信路に用い，最ゆう復号したときの復号誤り率 p_e とするとき，任意の $E<E_r(R)$ に対し，t を十分大きく選べば

$$\lim_{N\to\infty}\Pr\left\{\frac{-\ln p_e}{N}\geqq E\right\}=1$$

が成り立つ．ただし，Pr は条件 $-(\ln p_e)/N\geqq E$ を満足する符号が，上記のランダムな符号構成法によって得られる確率を表す．

この結果は，各列の 1 の数が高々 t 個のパリティ検査行列によって定まる LDPC 符号によって Gallager の信頼性関数が達成できることを示している．しかしながら，LDPC 符号の最大の特長である Sum-Product アルゴリズムなどの効率的な復号法によって同様の性能が得られるかについては不明であり，今後の研究が望まれる．

なお，Bennantan と Burshtein によって，Miller-Burshtein の成果の一般の無記憶通信路への拡張が行われており，そこで

は，q元のLDPC 符号と最ゆう復号法を組み合わせることで，Gallager の信頼性関数を達成できることが示されている[39]．

11．RA 符号

98 年にDivsalar，Jin，McEliece はターボ符号に類似の符号として，繰り返し符号とインタリーバとアキュムレータから構成される repeat accumulate（RA）符号と呼ばれる簡単な構成を有する高性能な符号を提案した[40]．Divsalar らは，RA 符号を最ゆう復号した場合，符号長を長くしたとき復号誤り率が零に近づくことを示して，簡単な構造の符号でも良い性能が得られることを示した．

Divsalar らの成果に触発されたPfister とSiegel はアキュムレータと一様インタリーバ（uniform interleaver）を多段に接続することでGallagar の信頼性関数を達成する符号が得られることを示した[41]．以下では，Pfister とSiegel の成果について述べる．

いま，符号長n，情報記号数kの二元符号の生成行列Cが与えられたとする(注3)．この符号の符号語を図5のようにインタリーバとアキュムレータに順に通して得られる二元線形符号の生成行列$C^{(1)}$は

$$C^{(1)} = C\,\Pi_1 C^{(o)}$$

である．ただし，Π_1はインタリーバを表す置換行列であり，$C^{(o)}$は，アキュムレータに対応する伝送速度1の符号の生成行列

$$C^{(o)} = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ 0 & 1 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix}$$

である．このインタリーバとアキュムレータの部分をm段縦続して得られるCA^m符号と呼ばれる符号のクラス

$$C^{(m)} = C\,\Pi_1 C^{(o)}\,\Pi_2 C^{(o)} \cdots \Pi_m C^{(o)}$$

を考えよう．インタリーバΠ_i $(i=1,\cdots,m)$ をすべてのインタリーバから一様分布に従って独立に選んだとき，Pfister とSiegel は次の成果を示した．

[定理13]（文献（41），Theorem 3）

二元符号Cが与えられたとき，$A_l^{(m)}$によって，インタリーバをランダムに取り換えて得られるCA^m符号の重みlの符号語数の平均を表す．このとき，

$$\lim_{m\to\infty} A_l^{(m)} = \begin{cases} (2^k-1)\cdot\frac{\binom{n}{l}}{2^n-1} & \text{if } l \geqq 1 \\ 1 & \text{if } l = 0 \end{cases}$$

であり，この収束はlによらず一様である．

この定理とShulman-Federの成果を組み合わせることで，Pfister とSiegel は次の定理を得た．

[定理14]（文献（41），Corollary 3）

二元入力対称出力通信路に対し，最ゆう復号法を用いたときの復号誤り率p_eが

$$p_e \leqq \exp\{-nE_r\,(R+O\,(1/n))\,\}$$

を満足するものがCA^m符号の中に存在する．ただし，Rは符号の伝送速度を表す．

Pfister とSiegel は，CA^m符号を繰り返し復号によって復号した場合も，優れた誤り率を有することをシミュレーションによって示した[41]．しかしながらCA^m符号が繰り返し復号によってGallagarの信頼性関数を達成できるかについては，LDPC符号と同様に未知であり，今後の解決が待たれる．

図5　$CA^{(1)}$符号の構成

(注3)：通常，生成行列を表す記号はGだが，文献（41）の記法に従い，ここではCを用いる．

12．連接符号の線形時間での復号

96 年に，Sisper とSpielman は，漸近的に良い性能を有する線形符号で，符号長に比例する計算量で復号が行える符号の具体的な構成法を示た[42]．彼らの符号は，Ramanujan グラフに基づく符号であり，一般にexpander 符号と呼ばれる．

2002 年に，Barg とZémor はexpander 符号によって，連接符号よりも復号の計算量が少なく，かつ復号誤り率が符号長の指数関数で減少する符号が得られることを示した[43]．以下では，expander 符号の構成法とBarg とZémor による復号法について述べる．

いま，節点集合$A \cup B$ $(|A|=|B|=m)$ を有し，すべての枝がAに属する節点とBに属する節点を結んでいる 部グラフ$\mathcal{G}$を考えよう．Aに属する節点を左節点，Bに属する節点を右節点と呼ぶ．グラフ$\mathcal{G}$の枝集合をEとし，節点$v \in A \cup B$に接続されている枝の集合をE_vによって表す．また，すべての節点$v \in A \cup B$にはΔ本の枝が接続されているとする．すなわち

$$|E_v| = \Delta \quad \forall v \in A \cup B$$

が成り立つとする．このとき，$\mathcal{G}$の枝の総数は$|E|=\Delta m$である．そこで，枝に番号を付加し，枝集合を$E=\{1,2,\cdots,N\}$ $(N=\Delta m)$ によって表し，任意の節点$v \in A \cup B$について，E_vに属する枝を$v\,(1)$，$v\,(2)$，$\cdots$，$v\,(\Delta)$によって表す．また，$x=(x_1,\ x_2,\cdots,\ x_N) \in \{0,\ 1\}^N$を二元ベクトルとするとき，$E_v$に対応する$x$の部分ベクトルを

$$x_v = (x_{v(1)}, x_{v(2)}, \cdots, x_{v(\Delta)}) \in \{0, 1\}^{\Delta}$$

によって表す．

さて，2部グラフ$\mathcal{G}$としてRamanujanグラフを選び，符号長Δ，情報記号数$k = r_e\Delta$，最小距離$d = \delta\Delta$を有する二元符号C_0を考える．このとき，任意の$v \in A \cup B$について，x_vがC_0の符号語であるようなベクトル$x \in \{0, 1\}^N$の集合をexpander符号と言う．一つの節点vに対して，その節点に接続されている枝E_vに対応するxの部分列x_vに対するパリティ検査行列が対応するので，expander符号は線形符号であり，伝送速度rは

$$r \geqq 2r_e - 1$$

を満足する．

次に，expander符号の復号法について述べる．いま，$y \in \{0, 1\}^N$を受信ベクトルとする．このとき，まずすべての左節点$v \in A$について，$y_v = (y_{v(1)}, \cdots, y_{v(\Delta)})$を最も近い距離にある符号語$x_v^{(1)} = (x_{v(1)}^{(1)}, \cdots, x_{v(\Delta)}^{(1)}) \in C_0$に復号する．この操作を$L(\cdot)$によって表し「左復号」と呼ぶ．次に，すべての右節点$v \in B$について，$x_v^{(1)}$を最も近い距離にある符号語$y_v^{(2)} \in C_0$に復号する．この操作を$R(\cdot)$によって表し「右復号」と呼ぶ．実際の復号は，左復号と右復号を交互に行うことによって行われる．すなわち操作

$$x^{(0)} = y,\ x^{(1)} = L(x^{(0)}),\ x^{(2)} = R(x^{(1)}),\ x^{(3)} = L(x^{(2)}),\ \cdots$$

を行い，$x^{(i)} = x^{(i-1)}$となるか，一定回数実行した段階で終了する．

このexpander符号を二元対称通信路に用いたときの復号誤り率について，BargとZémorは次の定理を示した．

[定理15]（文献(43)，Theorem 3）

任意の伝送速度R，任意の$\epsilon > 0$，$\alpha < 1$に対し，十分長い符号長Nのexpander符号が存在して，復号誤り率

$$p_e \leqq p^{\alpha m(\delta/2 - \epsilon)}$$

を満足する．ただし，pは符号C_0の2元対称通信路における復号誤り率を表す．

この後，2005年にGuruswamiとIndykは，expander符号を利用することで，符号長の線形時間で符号化および復号化が行え，Singleton限界（文献(28)，p. 33）をほとんど満足する高性能符号が作れることを示した[44]．彼らの成果を次の定理に示す．

[定理16]（文献(44)，Theorem 3）

任意のr $(0 < r < 1)$と十分小さな$\epsilon > 0$に対して，アルファベットサイズ$2^{O(\epsilon^{-4}r^{-1}\log(1/\epsilon))}$の有限体上で，伝送速度$r$ならびに相対距離$(1 - r - \epsilon)$を有する符号が構成できる．しかも符号長の線形時間で，符号化ならびに相対距離までの誤りとイレージャーの同時訂正が可能である．

GuruswamiとIndykによる符号では，定義体を保ったまま，符号長Nを任意に長くすることが可能である．従って，この符号を外部符号に用いてDelsarte-Piretの連接符号を構成すれば，内部符号の符号長nを一定にしたまま十分長い符号を構成することができる．しかも得られた連接符号の内部符号全体の復号化の計算量は$O(N)$で済み，上の定理から外部符号は一般化最小距離復号法によって復号したとしても$O(N)$で済む．この事実から，次の成果が得られる．

[定理17]（文献(44)，Theorem 8）

任意の$\epsilon > 0$と十分大きな符号長N_oについて二元対称通信路における復号誤り率が

$$p_e \leqq \exp\{-N_o(E_c(R) - \epsilon)\}$$

を達成する連接符号が構成できる．また，この連接符号は，符号長N_oの線形時間で符号化ならびに復号化が行える．

この定理は，Forenyの信頼性関数を線形時間の復号法で達成できる符号が構成できることを示しており，連接符号に対する決定的な成果である．なお，GuruswamiとIndykは，上記定理を二元対称通信路についてのみ証明しているが，任意の正規通信路への拡張は自明である．

13. 宿題

次のシャノン理論の問題を解き，解答を学会で発表せよ．なお，A，B，Cの順で問題は難しくなる．

A　問題

- 最近の通信路符号の構成法の成果を利用して，シャノン理論における他の符号化問題（マルチアクセス通信路，放送型通信路など）に対しても，通信路符号化と同様の成果を導け．
- ユニバーサルな通信路符号によって達成できる信頼性関数を低伝送速度において改良せよ．

B　問題

- 線形時間で符号化・復号化が行え，符号化・復号化の両方または片方がユニバーサルな符号を構成せよ．
- expander符号やGuruswami-Indykの符号を最ゆう復号したときの復号誤り率はGallagerの信頼性関数を達成できるか．
- LDPC符号をSum-productアルゴリズムなどの繰り返し法で復号したとき，Gallagerの信頼性関数を達成できるか．
- Gallagerの信頼性関数を達成する今までに得られていない符号のクラスを見いだせ．

C　問題

信頼性関数の上界の下界の間には低伝送速度においてギャップがある．このギャップを埋め，最良の符号で達

成できる信頼性関数をすべての伝送速度において定めよ．

謝　　辞

この解説論文のもとになる招待講演の機会を与えて頂いた情報理論研究専門委員会ならびに若手研究者のための講演会の各位に深謝する．

文　献

(1) 韓　太舜, “極道としての学問,” 情報理論とその応用学会ニューズレター，no. 23, pp. 3-6, April 1996.
(2) 有本　卓，平澤茂一，“通信路符号化と信頼度関数,” 信学論（A），vol. J73-A, no. 2, pp. 188-195, Feb. 1990.
(3) 平澤茂一，有本　卓，“通信路符号化の歴史と展望,” 符号理論とその応用，情報理論とその応用学会（編），pp. 1-26，培風館，東京，2003.
(4) S. Verdú, “Fifty years of Shannon theory, ” IEEE Trans. Inf. Theory, vol. 44, no. 6, pp. 2057-2078, Oct. 1998.
(5) C. E. Shannon, “A mathematical theory of communication, ” Bell Syst. Tech. J., vol. 27, pp. 379-423, 623-656, July-Oct. 1948.
(6) P. Elias, “Error-free coding, ” IRE Trans. Inform. Theory, vol. PGIT-4, pp. 29-37, Sept. 1954.
(7) P. Elias, “Coding for noisy channels,” IRE WESCON Convention Record, vol. 2, pp. 94-104, 1955.
(8) R. M. Fano, Transmission of Information, A Statistical Theory of Communications, Wiley, 1961.
(9) R. G. Gallager, “A simple derivation of the coding theoremand some applications,” IEEE Trans. Inf. Theory, vol. IT-11, no. 1, pp. 3-18, Jan. 1965.
(10) G. D. Forney, Jr. “Exponential error bounds for erasure，list, and decision feedback schemes,” IEEE Trans. Inf. Theory, vol. IT-14, no. 2, pp. 206-220, March 1968.
(11) C. E. Shannon, R. G. Gallager, and E. R. Berlekamp, “Lower bounds to error probability for coding on discrete memoryless channles. I, ” Inf. Control vol. 10, no. 1, pp. 65-103, Jan. 1967.
(12) G. D. Forney, Jr., Concatinated codes, MIT Press, 1966.
(13) G. D. Forney, Jr., “Generalized minimum distance decoding,” IEEE Trans. Inf. Theory, vol. IT-12, no. 3, pp. 125-131, April 1966.
(14) S. Hirasawa, M. Kasahara, Y. Sugiyama, and T. Namekawa, “Certain generalizations of concatenated codes – Exponential error bounds and decoding complexity,” IEEE Trans. Inf. Theory, vol. IT-26, no. 5, pp. 527-534, Sept. 1980.
(15) L. Davisson, “Universal noiseless coding, ” IEEE Trans. Inf. Theory, vol. IT-19, no. 6, pp. 783-795, Nov. 1973.
(16) J. Ziv and A. Lempel, “A universal algorithm for sequential data compression,” IEEE Trans. Inf. Theory, vol. IT-23, no. 3, pp. 337-343, May 1977.
(17) J. Ziv and A. Lempel，“Compression of individual sequences via variable-rate coding,” IEEE Trans. Inf. Theory, vol. IT-24, no. 5, pp. 530-536, May 1978.
(18) I. Csiszár, J. Körner, and K. Marton, “A new look at the error exponent of a discrete memoryless channel, ” IEEE ISIT, Cornell Univ. Ithaca, N. Y. , Oct. 1977.
(19) I. Csiszár and J. Körner, Information Theory: Coding Theorems for Discrete Memoryless Systems, Academic, 1981.
(20) V. D. Goppa, “Nonprobabilistic mutual information without memory,” Probl. of Control Inf. Theory, vol. 4, pp. 97-102, 1975.
(21) J. Ziv, “Universal decoding for finite-state channels,” IEEE Trans. Inform. Theory, vol. IT-31, no. 4, pp. 453-460, July 1985.
(22) A. Lapidoth and J. Ziv, “On the universality of the LZ-based decoding algorithm,” IEEE Trans. Inf. Theory, vol. 44, no. 5, pp. 1746-1755, Sept. 1998.
(23) T. Uyematsu and S. M. Kisra, “On the universality of channel decoders constructed from source encoders for finite-state channels,” IEICE Trans. Fundamentals, vol. E84-A, no. 10, pp. 2447-2456, Oct. 2001.
(24) P. Delsarte and P. Piret, “Algebraic constructions of Shannon codes for regular channels,” IEEE Trans. Inf. Theory, vol. IT-28, no. 4, pp. 593-599, July 1982.
(25) J. Justesen, “A class of constructive asymptotically good algebraic codes,” IEEE Trans. Inf. Theory, vol. IT-18, no.5, pp. 652-656, Sept. 1972.
(26) C. Thommesen, “Error-correcting capabilities of concatenated codes with MDS outer codes on memoryless channels with maximum-likelihood decoding,” IEEE Trans. Inf. Theory, vol. IT-43, no. 5, pp. 632-640, Sept. 1987.
(27) M. A. Tsfasman, S. G. Vlăduţ, and T. Zink, “Modular curves and goppa codes, better than Varshamov-Gilbert bound,” Math. Nachr., vol. 109, pp. 21-28, 1982.
(28) F. J. MacWilliams and N. J. A. Sloane, The Theory of Error-Correcting Codes, North-Holland, 1977.
(29) B. -Z. Shen, “A Justesen construction of binary convatenated codes that asymptotically meet the Zyablov-bound for low rate,” IEEE Trans. Inf. Theory, vol. IT-39, no. 1, pp. 239-242, Jan. 1993.
(30) 植松友彦, 水野　亮，スティチャイノッパナケェポン, “優れた信頼性関数を有する符号の代数的構成法と光通信への応用,”信学論（A）, vol. J77-A, no. 11, pp. 1537-1545, Nov. 1994.
(31) T. Uyematsu and E. Okamoto, “A construction of codes with exponential error bounds on arbitrary discrete memoryless channels,” IEEE Trans. Inf. Theory, vol. IT-43, no. 3, pp. 992-996, May 1997.
(32) T. Uyematsu, J. Kaga, and E. Okamoto, “Relaibility functions for concatenated codes employing modular codes with maximum likelihood decoding,” IEICE Trans. Fundamentals, vol. E78-A, no. 9, pp. 1160-1169, Sept. 1995.
(33) D. J. C. MacKay, “Good error-correcting codes based on very sparse matrices,” IEEE Trans. Inf. Theory, vol. 45, no. 2, pp. 399-431, March 1999.
(34) C. Berrou, A. Glavieux, and P. Thitimajshima, “Near Shannon limit error-correcting coding and decoding: Turbo-codes,” Proc. 1993 IEEE Int. Conf. on Commun., pp. 1064-1070, 1993.
(35) D. J. C. MacKay and R. M. Neal, “Good codes based on very sparse matrices,” Cryptography and Coding 5th IMA Conf., pp. 100-111, Springer, 1995.
(36) R. G. Gallager, Low Density Parity Check Codes, MIT Press, 1963.
(37) N. Shulman and M. Feder, “Random coding techniques for nonrandom codes,” IEEE Trans. Inf. Theory, vol. 45, no. 6, pp. 2101-2104, Sept. 1999.
(38) G. Miller and D. Burshtein, “Bounds on the maximum likelihood decoding error probability of low-density parity-check codes,” IEEE Trans. Inf. Theory, vol. 47, no. 7, pp. 2696-2710, Nov. 2001.
(39) A. Bennatan and D. Burshtein, “ On the application of LDPC codes to arbitrary discrete-momoryless channels,” IEEE Trans. Inf. Theory, vol. 50, no. 3, pp. 417-438, March 2004.
(40) D. Divsalar, H. Jin, and R. J. McEliece, “Coding theorems for ’turbo-like’ codes,” Proc. 36th Annu. Allerton Conf. Communications, Control, and Computing, pp. 201-210, Sept. 1998.
(41) H. D. Pfister and P. H. Shiegel, “The serial concatenation of rate-1 codes through uniform random interleavers,” IEEE Trans. Inf. Theory, vol. 49, no. 6, pp. 1425-1438, June 2003.
(42) M. Sisper and D. A. Spielman, “Expander codes,” IEEE Trans. Inf. Theory, vol. 42, no. 6, pp. 1710-1722, Nov. 1996.
(43) A. Barg, and G. Zémor, “Error exponents of expander codes,” IEEE Trans. Inf. Theory, vol. 48, no. 6, pp. 1725-1729, June 2002.
(44) V. Guruswami and P. Indyk, “Linear-time encodable/decodable codes with near-optimal rate,” IEEE Trans. Inf. Theory, vol. 51, no. 10, pp. 3393-3400, Oct. 2005.

植松　友彦（正員）

昭57東工大・工・電気電子卒．昭59同大学院修士課程了．同年同大学助手，同講師を経て平3同大学助教授．平4北陸先端大助教授．平9東工大助教授．平15同大学教授．工博．情報理論，特にシャノン理論の研究に従事．昭63年度篠原記念学術奨励賞受賞．平4年度，平7年度，平13年度，並びに平18年度論文賞受賞．著書「現代シャノン理論」など．