研究ノート

誤り訂正符号の研究

滑川敏彦*
笠原正雄**

現代情報理論の先駆的研究を行った人としてC.E. Shannon, N. Wiener の2名をあげることに異論を唱える人は少ないであろう．なかでも1949年に Shannon が発表した著名な論文“A Mathematical Theory of Communication”は現代情報理論の驚異的な発展を呼ぶ導火線となったものであり，このために Shannon が情報理論の創始者であると考える人も少なくないのである．電子通信学会雑誌前編集長の喜安善市博士の言葉を借りれば Shannon の理論は情報理論の背峻山脈を形成している．Shannon の理論には第一定理・第二定理と言われる2つの重要な定理がある．第一定理は情報源符号化定理とも呼ばれ，画像情報理論の基礎としてその重要性が最近とみに再認識されている．第二定理は通信路符号化定理とも呼ばれるが，この定理の重要性は筆者らが如何に強調しても十分でなく，その通信方式を中心とする通信技術に及ぼした影響から見て，真に計り知れないものがある．この定理は通信方式の理論的限界を与えるとともに，通常の通信路においては任意に高い信頼度の誤りのない通信が可能であることを数学的に証明したのである．

以来，通信路符号化定理に対する具体的な解答を見出す問題，すなわち符号理論が情報理論の1つの大きな流れを形づくってきた．符号理論の主要なテーマは，言うまでもなく誤り訂正符号の構成の問題である．誤り訂正符号の本来の目的は高信頼度の通信を実現することにあるが，計算機のメモリィあるいは論理回路だけでなく本質的にはあらゆるシステムの高信頼度化に関連しているために今後ますますその発展が見込まれている．ここでは誤り訂正符号を簡単に紹介するとともに，筆者らの最近の研究ノートのなかから誤り訂正に関する2，3の話題を拾ってみたい．

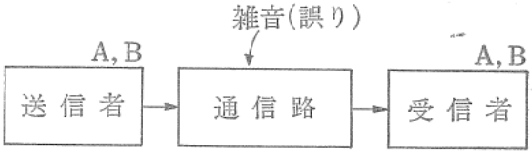

図1　通信の1モデル

図1に通信路の1モデルを示す．送信者はAおよびBの2つのアルファベットのうち，何れか1つを誤りなく受信者に伝えたい．通信路には雑音が存在し送信されたアルファベットはA→B，B→Aというふうに誤まって受信されうるとしよう．Shannon が提起した情報理論の1つの問題はAという送信アルファベットを十分高い信頼度で伝送する方法は何かということである．1つのきわめて単純な方法はAというアルファベットを繰り返し反復して伝送することであり，受信側では多数決をとって送信アルファベットを推定する．図2はこの原理にもとずく2元符号の号符化—復号化法を示している．もし通信路に誤りが全く生起しなければ

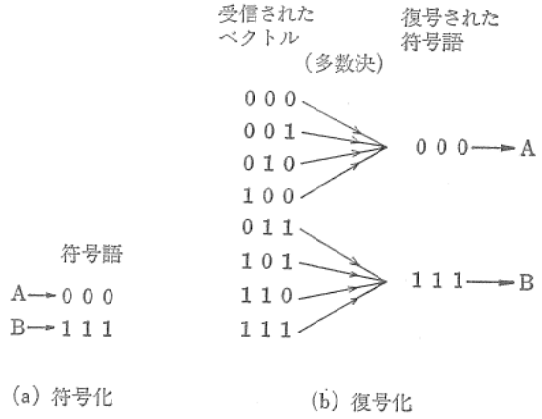

図2　符号化，復号化の一例

* 滑川敏彦 (Toshihiko Namekawa)，大阪大学，工学部，通信工学科，第三講座，教授，工学博士，電子回路・通信理論
** 笠原正雄 (Masao Kasahara)，大阪大学，工学部，通信工学科，第三講座，助教授，工学博士，通信理論

A→0，B→1なる符号化ですむから図2(a)の符号（000，111）は2ビットの冗長記号を有することになる．図2の符号は符号理論的表現をすれば符号長n＝3，情報記号数k＝1，冗長記号数g＝n－k＝2，情報率k/n＝0.66……，訂正能誤り数t＝1ということになる．

送信すべきアルファベットの個数MがM＝2で符号長が3の場合には図2のような符号化がもっとも理想的であり，これに優る方法は存在しない．しかしアルファベット数Mは通常M≫1であり，このような場合には任意のMに対し理想的な符号を見出すことは一般にきわめて困難である．誤り訂正符号の究極の目標はこのような理想的な符号を見出すことにあると言えよう．

過去10数年，誤り訂正符号の広い分野で活躍されている本学基礎工学部の嵩教授の業績は著名である．

最近，符号長n≦500，誤り訂正個数t≦14の範囲で，現在知られている符号のなかで最大の情報率を有する符号の一覧表がBell研究所のSloane博士によって編纂された．百近くあろうと思われる文献の中から集められた符号の数は数百にのぼるが，幸いなことにその約の20％，150近くは筆者らのグループが一昨年夏から，約1年間に投稿した4編の論文から選ばれている．

高情報率の符号を発見する仕事は多分に忍耐を要する．見込みのありそうな方法，あるいは考えに恵まれれば徹頭徹尾追いつめねばならない．たとえ，2，3日であっても，このこと以外は頭の中にはないという無我夢中の瞬間がなければならない．しかしながらそのような苦労の末，生まれた符号が既存の符号に優れるか否かは，ある程度“運”にもよるものではないかとさえ思われる．たとえば，訂正可能な誤り数t＝4，冗長記号数g＝26に対し，既存の符号がn＝75であったが，新しい符号はn＝76であり，僅かに1ビット情報記号数が上まわっただけである．大幅に上まわった例としてもt＝9，g＝70で既存の符号のn＝271に対し新しい符号でn＝310というのがあるものの組織的な方法でどの程度まで良好な符号が見出し得るのかという保証は今のところ全くない．筆者らが150近くも高情報率の符号を発見し得たのは“just lucky”であったと言えよう．しかしながらもちろんこれらのうち，理論上の最適な符号は，ほんの2，3個に過ぎないから将来他の優れた符号に大部分が置き換えられる可能性は多分にあることをことわっておきたい

1950年のHamming符号の発見以来，実に膨大な量の誤り訂正符号の研究のなかで，Bose-Chaudhuri-Hocquenghem（BCH）符号，Reed-Solomon符号，Reed-Muller符号などは燦然と輝く誰もが認める偉大な符号である．1970年に発見されたGoppa符号は情報理論の世界で，最近では最も多くの注目を集めたが真に理論的に美しい優れた符号である．筆者らが多数の高情報率の符号を見出し得たのは，Hamming符号からGoppa符号に至る素晴しい“乗物”があったからである．いわば新幹線とい素晴しい乗物の中で走ったとき，地上から見た速度が新幹線以上であったのではあるまいか．

符号理論の研究は，これから成熟期を迎えようとしているとの声を多く聞く．果してそうであろうか．誤り訂正符号の世界には，あまりにも多くの問題が未解決のまま横たわっているというのが現状であると思う．若手の研究者を含めて今後ますますの努力が望まれる次第である．

さて，誤り訂正符号の符号化の問題と並んで重要な問題は言うまでもなく復号化の問題である．筆者らのグループが一昨年秋に，米国インディアナ州ノートルダムにおける情報理論国際シンポジウムで発表した“ユークリッド復号法”は幸いなことに，筆者らの期待以上の注目を集めた．これはユークリッドの互除法を誤り訂正符号の復号に応用したものであって，紀元前300年のアイディアを現代の情報理論に借りてきたところに，意外な発展の可能性が秘められていた．しかしこのユークリッド復号法の発見当時の一昨年春をふり返ってみると，“果してこんな簡単な方法にオリジナリティは残されているのか”という不安な疑問があったと思う．BCH符号に対する優れた復号法の発見者

であるカリフォルニア大学の Berlekamp 教授との文通，Bell 研究所の Sloane，Mac Williams 両博士その他多数の研究者との討論でオリジナリティに対する自信を深めていったが，将来この方法が符号理論の世界でどのように成長していくかはやはりある程度，今後の“努力”と“運”によろうと思う昨今である．