

特集 / 符号化理論の新時代

符号化理論の研究動向

萩原 学・今井 秀樹

1. 序文

符号化理論もしくは符号理論は、広い意味での情報理論の一分野である。ここで、符号化とは情報の形態の変換を意味している。符号化理論には大きく分けて3つの重要なテーマ「効率向上のための符号化」「信頼性向上のための符号化」「セキュリティ向上のための符号化」がある。それぞれのキーワード「圧縮」「誤り訂正」「暗号」を耳にしたことのある方も多いだろう。

符号化理論は1948年のShannonの論文に端を発し、現在までに急激な進歩を遂げてきた。一般に符号化理論と言うと「信頼性向上のための符号化」にスポットを当てる。つまり、誤り訂正符号の理論を指すことが多い。誤り訂正符号研究のこの10年間の動向は目覚ましいものがある。代数幾何学・確率論・グラフ理論が交錯し、符号化理論の最も重要な課題「シャノン限界」がほとんど達成された。しかし符号化理論の研究は終わらず、むしろ様々な理論が交錯しながら他分野へ影響を与え発展し続けている。そこで、この記事はシャノン限界を中心に符号化理論が発展していく様子を歴史に沿って書くことにしよう。

ところで、符号化理論は通信路符号化の理論と呼ばれている。冒頭で述べた「効率向上のための

符号化」は情報源符号化の理論と呼ばれている。これらは密接に関係し、互いに理論発展を進めてきた。情報源符号化に関する詳しい内容は、本特集の山本氏の記事を読んで頂きたい。

今回の特集では従来の符号化理論がどのように進歩してきたかだけにとどまらず、周辺の話題も取り上げている。符号理論のもつ懐の深さ、そして次の研究テーマが垣間見れることだろう。

2. 大きな最小距離

まず符号化理論の研究が始まってから約20年間の流れをざっと見ていく。この時期の研究成果が与えた符号化理論への影響は計り知れない。多くの主要な符号が登場し、最新の研究の発端が垣間見れる。代数幾何符号などの登場が必然に感じられる。実は、LDPC符号はこの時期すでに登場していた。それでは、符号化理論の始まりから、基本的に時系列に従い、歴史を追っていこう。

先にも述べたが、符号化理論は1948年のShannonの論文から始まったと言える³²⁾。Shannonにより情報の伝送速度が通信路によって定まる限界(通信路容量)以下のとき、またそのときに限り、幾らでも高い信頼性で情報伝達できることが示された。この限界はシャノン限界と呼ばれ、シャノ