リード・ソロモン符号の半世紀

—デジタル情報通信・記録技術発展の歴史の中で総合的に考える—

Reed-Solomon Code in the Last Half Century

—A Survey of Digital Transmission and Storage Systems from a Global Point of View—

笠原正雄 Masao KASAHARA

アブストラクト リード・ソロモン (RS: Reed-Solomon) 符号誕生後、半世紀の歳月が経過している。本稿では RS 符号が情報通信・記録技術発展の歴史の中で、マイナーな存在からやがて私たちの生活の中に最も深く溶け込んだ符号、すなわち総合的に考えて最上位にランクされる符号として高く評価され、位置付けられていく過程をデジタル情報通信・記録技術の発展の歴史の中で幅広く捉えて解説する。更に RS 符号には高信頼度の情報通信記録システムを構築する上での大きな貢献に加えて、情報セキュリティ分野への応用をはじめとする多様な分野への応用が期待されることを述べる。

キーワード RS 符号, BCH 符号, ゴッパ符号, ファイア符号, 最大距離分離性, 公開鍵暗号, 秘密分散保管システム

1. ま え が き

ベル電話研究所の若き研究者 Shannon によって、1948 年に発表された論文「A mathematical theory of communication」は通信の本質を見事に捉えており、情報理論の誕生を告げるものであった⁽¹⁾。

情報理論のテーマは

- (1) 情報源符号化 (帯域圧縮, 高能率符号化),
- (2) 通信路符号化 (誤り訂正),

に大別される。

1950 年に Shannon と同じベル電話研究所の研究者 Hamming によって発表された論文「Error detecting and error correcting code」は通信路符号化問題の支柱ともいえるべき符号理論に関する研究の嚆矢となった⁽²⁾。

図 1 に符号理論発展の背景を要約しよう。

図 1 に示すように 1972 年、リード・マラー符号を用いることによって人類は火星表面の鮮明な写真を伝送することに成功した⁽³⁾。ガリレオの時代には到底想像することのできなかった“電子望遠鏡”を実現するために誤り訂正符号が威力を発揮したのであり、このことによって符号理論の研究者は大いに勇気付けられた。

ちなみにインターネットの母胎、コンピュータコミュニケーションを可能にしたものは誤り制御技術の力であった。コンピュータ分野の関係者は、コンピュータ関連の幾つかの国際会議の場で、コンピュータデータにとって到底耐え難い劣悪な通

信環境 (音声専用加入者線) が誤り制御技術によって見事に克服されることを実証した。

しかし私が記憶する限り、このような動きは符号理論の研究者には伝わってこなかったし、またコンピュータ関係者から符号理論研究者に助言を求めるといったようなこともなかった。私たちはこのような傾向を反省しなければならないと思う。専門分野の細分化と同時に専門分野の合従連衡を積極的に図ることが、オリジナリティ創出のために今後ますます希求されよう。

符号理論は

- (1) 代数的符号:

代数的構造を有するブロック型の符号。巡回符号, Bose-Chaudhuri-Hocquenghem (BCH) 符号, リード・ソロモン (RS: Reed-Solomon) 符号, ゴッパ符号等。

- (2) 非代数的符号:

必ずしも代数的構造を有さない非ブロック型の符号。畳込み符号, LDPC (Low-Density Parity-Check) 符号等に大別される。

本稿のテーマである RS 符号は BCH 符号とほぼ同じ年、1960 年に誕生している⁽⁴⁾⁻⁽⁶⁾。

誕生後半世紀という節目を迎えた RS 符号は理論上の特筆す

- 1952年: AA(American Airline)座席予約システム。
- 1961年: 米国T1 (T-one) PCMシステム。
- 1964年: 日本PCM24方式。
- 1960~1970年: 誤り訂正符号, コンピュータコミュニケーションに可能性を与える。(インターネットの胎動。)
- 1972年: マリナー計画, 火星表面の写真電送に成功。符号長32の1次リード・マラー符号が使用された。
- 1970年代~: インターネット誕生, 発展への道。

図 1 符号理論発展の背景

笠原正雄 名誉員: フェロー 大阪学院大学情報学部
E-mail kasahara@ogu.ac.jp
Masao KASAHARA, Fellow, Honorary Member (Faculty of Informatics, Osaka Gakuin University, Suita-Shi, 564-8511 Japan).
電子情報通信学会 基礎・境界ソサイエティ
Fundamentals Review Vol.5 No.1 pp.28-41 2011 年 7 月
©電子情報通信学会 2011

べき数々の特徴を有するとともに、実用上最も大きな貢献をしている符号であり、総合的に考えて、数々の誤り訂正符号の中で最上位にランクされる符号として位置付けることができる。

本稿では、RS 符号が最上位に位置付けられていく経緯を、より広い視野に立って、Shannon 以降半世紀を越えるデジタル情報通信・記録技術の発展の歴史の中で、総合的に捉えて解説してみたい⁽⁷⁾。

2. BCH 符号と RS 符号

2.1 BCH 符号と RS 符号

BCH 符号と RS 符号はほぼ同時期である 1960 年前後に独立に提案されている。

RS 符号と BCH 符号とは、

- (1) RS 符号は BCH 符号の特別なクラスにすぎない、
 - (2) BCH 符号は RS 符号を一般化したにすぎない、
- として一方が他方に吸収されかねない微妙な関係にあった。本節ではこのことについて解説しよう。

(1) BCH 符号

Bose と Chaudhuri 及び彼らと独立に Hocquenghem によって発見された BCH 符号は、巡回符号における重要なクラスの符号である。BCH 符号は複数個の誤りを訂正することが可能であり、したがってこの符号は単一誤り訂正巡回ハミング符号を一般化したものと考えることができる。

q を素数のべき m を自然数として $\mathbb{F}_{q^m}$ の任意の元を β とし、 β の位数を n とする。任意の整数を l とするとき、

$$\beta^l, \beta^{l+1}, \beta^{l+2}, \dots, \beta^{l+d-2} \quad (1)$$

を根として有する符号長 n の巡回符号を考える。ただし $d-1 < n$ とする。

β^i の $\mathbb{F}_q$ 上の最小多項式を $M_i(X)$ とすると $\mathbb{F}_q$ 上の BCH 符号は次の生成多項式 $G(X)$ によって生成される符号長 n の巡回符号である。

$$G(X) = LCM(M_l(X), M_{l+1}(X), \dots, M_{l+d-2}(X)) \quad (2)$$

ただし LCM は最小公倍数を意味する。□

この BCH 符号のパリティ検査行列 H は

$$H = \begin{bmatrix} (\beta^l)^{n-1} & (\beta^l)^{n-2} & \dots & \beta^l & 1 \\ (\beta^{l+1})^{n-1} & (\beta^{l+1})^{n-2} & \dots & \beta^{l+1} & 1 \\ \vdots & \vdots & & \vdots & \vdots \\ (\beta^{l+d-2})^{n-1} & (\beta^{l+d-2})^{n-2} & \dots & \beta^{l+d-2} & 1 \end{bmatrix} \quad (3)$$

で与えられる。行列 H の任意の $d-1$ 列からなる小行列式 D は Vandermonde 行列式の定数倍である。 β の位数は n であるから

$$\beta^{i_j} \neq \beta^{i_k}, i_j \neq i_k; \quad l \leq i_j, i_k \leq l+d-2. \quad (4)$$

であり、したがって $D \neq 0$ であることからパリティ検査行列の

任意に選んだ $d-1$ 個以下の列は一次独立であることが分かる。これにより上述の BCH 符号の最小距離は少なくとも d であることが分かる。以上のようにして与えられる最小距離 d を最小距離に関する BCH 限界 (BCH bound) という。

(2) RS 符号

BCH 符号の定義において $m=1$ とし、 β を $\mathbb{F}_q$ の原始元 α に選んだ特別な場合に得られる符号が RS 符号である。すなわち $\mathbb{F}_q$ の原始元を α とし、 $\alpha^l, \alpha^{l+1}, \dots, \alpha^{l+d-2}$ を根として有する符号長 $n=q-1$ の巡回符号が $\mathbb{F}_q$ 上の RS 符号である^(注1)。

RS 符号の生成多項式 $G(X)$ は

$$G(X) = (X - \alpha^l)(X - \alpha^{l+1}) \dots (X - \alpha^{l+d-2}) \quad (5)$$

で与えられる。式 (5) よりこの RS 符号の検査記号数 g は

$$g = d - 1 \quad (6)$$

である。また、情報記号数 $k = n - g$ は

$$k = q - d \quad (7)$$

で与えられる。一般に検査記号数が g であるような線形符号においてはその最小距離 d_L は、シングルトン限界式によって

$$d_L \leq g + 1 \quad (8)$$

である。式 (5) で生成される RS 符号の最小距離は BCH 下界より少なくとも d であり、しかも式 (6)、(8) より d 以下であることが分かる。したがって式 (5) の生成多項式で生成される RS 符号の最小距離はちょうど d に等しい。

以上のように RS 符号の最小距離は式 (8) を等号で満たしている。このように式 (8) を等号で満たす符号を一般に最大距離分離符号 (maximum distance separable code) という。

RS 符号が他の符号には見られない最大距離分離性を有すること、この長所こそが RS 符号の地位を符号理論の世界で高める最大の要因であった。本稿ではこのことを焦点の一つとして論じることにしてしよう。

(3) RS 符号の具体例

q を素数のべき、例えば $q=2^2$ として以下に RS 符号の具体例を考えよう。

例題 1: 最小距離が 3 であるような $\mathbb{F}_{2^2}$ 上の RS 符号を構成し、その符号語を全て示せ。

〔解〕 $\mathbb{F}_2$ 上の既約な多項式 $X^2 + X + 1$ によって導かれる体 $\mathbb{F}_{2^2}$ を $\{0, 1, \alpha, \alpha^2\}$ とする。ただし α を原始元として $\alpha^2 = \alpha + 1$ である。最小距離 3 の RS 符号の生成多項式の一つは、式 (5) より $l=1$ とすると $G(X) = (X - \alpha)(X - \alpha^2) = X^2 + X + 1$ である。式 (7) より情報記号数は 1 である。この情報記号を一

(注1): 笠原らによって見出された二重テイル構成法 (double tail construction) を RS 符号に適用すると、最小距離、検査記号数を一定にしたまま、符号長 n を $n = q + 1$ と 2 シンボルだけ伸長すること、すなわち二次伸長することが可能である⁽³⁾。二次伸長 RS 符号は様々な観点から非常に有用である。後ほどこのことについて触れることにしよう。

般に m_0 とすると, m_0 は $m_0 \in \mathbb{F}_{2^2}$ であるから, $0, 1, \alpha, \alpha^2$ なる値の任意の一つを取り得る. これらの情報記号に対応する検査記号は, $m_0 X^2$ を $G(X) = X^2 + X + 1$ で割った余りの X の係数と定数項として求められる. すなわち符号語は

$$\begin{array}{ll} 0 & 0 \quad 0 \quad (00 \ 00 \ 00) \\ 1 & 1 \quad 1 \quad (01 \ 01 \ 01) \\ \alpha & \alpha \quad \alpha \quad (10 \ 10 \ 10) \\ \alpha^2 & \alpha^2 \quad \alpha^2 \quad (11 \ 11 \ 11) \end{array}$$

となる. 括弧内は $0 = (0 \ 0), 1 = (0 \ 1), \alpha = (1 \ 0), \alpha^2 = (1 \ 1)$ を対応させたものである. $\square$

(4) BCH 符号とゴッパ符号

符号長 n の BCH 符号 C を一般に $\{(s_0, s_1, \dots, s_{n-1})\}$ と表す. このとき式 (3) で与えられるパリティ検査行列を $l = 1, d-1 = w$ として参照すると, 結局

$$\sum_{i=0}^{n-1} \frac{s_i}{z - \beta^{-i}} \equiv 0 \pmod{z^w} \quad (9)$$

が導かれる⁽⁸⁾.

以上を次の定理に要約しよう.

【定理 1】 $\beta_0, \beta_1, \dots, \beta_{n-1}$ を $\mathbb{F}_{q^m}$ の相異なる非零の元とする. ただし

$$\beta_i = \beta^{-i}, \quad i = 0, 1, \dots, n-1 \quad (10)$$

とし, $0 < n \leq p-1$ である.

このとき $s_i \in \mathbb{F}_q$ として

$$\sum_{i=0}^{n-1} \frac{s_i}{z - \beta_i} \equiv 0 \pmod{z^w} \quad (11)$$

が満たされるとき, $s = (s_0, s_1, \dots, s_{n-1})$ を符号語とする符号 $C = \{s\}$ は符号長 n の BCH 符号であり, その最小距離は式 (11) によって $w+1$ 以上である. $\square$

式 (11) で与えた BCH 符号の定義を一般化すること, すなわち

$$z^w \rightarrow G(z) \quad (12)$$

とすることにより BCH 符号を特別なクラスとして含むゴッパ符号 (Goppa code) を以下のように定義することができる⁽⁹⁾.

まず始めに必要な記号として

$$\begin{array}{ll} G(z) & : \mathbb{F}_{q^m} \text{ 上の } w \text{ 次の多項式} \\ L & : G(z) \text{ の根を除いた } \mathbb{F}_{q^m} \text{ の元の集合} \\ n & : L \text{ の元の個数, } 0 < n \leq q^m - 1 \\ \beta_i & : L \text{ の元, } i = 0, 1, \dots, n-1 \end{array}$$

とする. q 元ゴッパ符号を次のように定義する.

【定義 1】 $s_i \in \mathbb{F}_q$ とする.

$$\sum_{i=0}^{n-1} \frac{s_i}{z - \beta_i} \equiv 0 \pmod{G(z)} \quad (13)$$

図 2 BCH, RS, ゴッパ各符号の相互関係^(注2)

が満たされるとき, $s = (s_0, s_1, \dots, s_{n-2}, s_{n-1})$ を符号語とする符号 $C = \{s\}$ を $G(z)$ で生成されるゴッパ符号という. $G(z)$ をゴッパ多項式 (Goppa polynomial) という. $\square$

式 (11) 及び定義 1 によってゴッパ符号は BCH 符号を特別な場合として含むことが明らかである. 定義よりゴッパ符号の最小距離は少なくとも $w+1$ であることが導かれる.

以上に述べてきた BCH 符号, RS 符号, ゴッパ符号の定義を参照して, これらの符号の相互関係を図 2 に示す.

1970 年代初頭に発見されたゴッパ符号は, この相互関係によって非常に広いクラスの符号であることが認識された. 極めて大きな注目を集め, より広く, 代数幾何符号発展への歴史が刻み始められた.

式 (13) で示されるゴッパ符号の定義は極めて美しく深淵である. しかし個々のメンバーについてはどうであろうか.

符号としての“良き性質”は

- 完全符号性 (ハミング符号等)
- 最大距離分離性 (RS 符号等)
- 均一重み性 (最大周期系列符号等)

である. 誤り訂正符号全体から見れば, これらの性質を満たす符号は極めて少ない. しかし符号化, 復号が非常に容易という BCH 符号のクラスの中にこれらの良き性質を満たす符号を見いだすことができるということは注目に値する.

“良きものには良きものが集まる”これは広く数学の世界の真理である. 工学的応用の分野でもこのことは真理である. すなわち“数学的良き性質”を有する符号によって, 良き工学的成果が編み出されることは自然な流れのように思われる. 私たちはこのことを後ほど具体例で見たいと思う.

2.2 BCH 符号と RS 符号, それぞれの評価

幸いなことに BCH 符号は $\mathbb{F}_2$ 上の優れたランダム誤り訂正符号として, また RS 符号は拡大体 $\mathbb{F}_{2^m}$ 上の最大距離分離符号として, それぞれが符号理論の世界で不動の地位を占めていることは真に喜ばしいことである.

RS 符号に対する評価と BCH 符号に対する評価を比較すると現時点では RS 符号に対する評価が圧倒的に高いように思われる. しかし 1960~1970 年代においては以下のような見方が支

(注2): BCH 符号は RS 符号の部分体部分符号として論じられている場合も多い. ここでは文献⁽¹⁰⁾の 9.3 に従う.

配的であった。

(1) BCH 符号はランダム誤りを効率良く訂正することができる優れた符号である。事実、符号長 512 以下、最小距離 29 以下の符号に限ると多くの BCH 符号が最良符号 (best code) として、MacWilliams と Sloane が編さんした最良符号表 (best code table) にリストアップされている⁽³⁾。ここに最良符号とは与えられた符号長と最小距離に対し、現存する符号の中で最小の検査記号数で実現される符号のことをいう。線形符号だけでなく、多くの非線形符号が含まれる。

(2) RS 符号は主として電話回線等のバースト誤りの生じする通信路で有効であるにすぎず、BCH 符号に比べ有用性が低い符号である。

といった評価が一般的であったと思われる。

Peterson は 1961 年に出版した名著『Error-correcting codes』⁽¹⁰⁾において、RS 符号については第 9 章「BCH 符号」の一つの節、すなわち 9.3 で、僅かなスペースを割いて述べているにすぎない。RS 符号が BCH 符号に比べ、過小評価されているとの印象は否めない。その後の 10 数年の RS 符号の研究対象としての歩みの差、BCH 符号に対し大きく水を空けられる差、をこの時点で想像させるものであった。今日の目から見れば、首をかしげたくするような評価との印象を与えるかもしれない。

しかし事実は当時もっと厳しかったのである。この RS 符号に対する低い評価には以下のような時代的な背景があった。

- 1950~1960 年代、一般加入者線を利用する座席予約システムあるいは計算機の時分割使用システム (Time Sharing System, TSS) 等においては、通信速度は 50~100bit/s 程度であり、生じるバースト誤りも相対的に短く、数 bit 程度と考えられていた。
- 上記を訂正するために、ファイア符号という優れた単一バースト誤り訂正巡回符号が存在していたこと。
- RS 符号は拡大体 $\mathbb{F}_{2^r}$ 上の符号である。 $\mathbb{F}_{2^r}$ の単位シンボル長 r が $r \gtrsim 8$ の範囲では RS 符号は上記数 bit 程度のバースト誤りを訂正する符号としては極めて不適切であること。すなわち図 3 に示したように拡大体 $\mathbb{F}_{2^r}$ 上の 2 シンボルの隣接部に生じた素体上長さ 2bit の単一バースト誤りは、拡大体上では $2r = 16\text{bit}$ という長い単一バースト誤りに拡大されてしまうこと。

以上の理由が RS 符号に対する評価の低さに結び付いていた。ちなみに上記 Peterson の名著『Error-correcting codes』において、RS 符号に関する記述は 1 ページ半にすぎないのに対し、ファイア符号については 5 ページにわたって解説されている。通信速度の向上、大容量メモリの登場等々、時代の背景がすっかり変わるまで、誤り訂正符号の中でもマイナーな存在であった

図 3 2 シンボルにわたるバースト誤り

RS 符号は華やかな脚光を浴びるまで、誕生後 20 年に近い歳月を辛抱強く待たねばならなかった。

しかしながら、ランダム誤りを訂正する BCH 符号あるいは単一バースト誤りを訂正するファイア符号もまた実用的な面からの評価は必ずしも高くはなく、主として理論的興味からの研究が続けられていたというのが実態であった。

2.3 誤り訂正方式か、誤り検出再送要求方式か — ランダム誤りか、バースト誤りか —

元々誤り訂正符号は 1960 年代当時は、理論的な興味はともかく実用性の点では非常に悲観視されていた。実用的な面から、誤り訂正符号に対し、誤り検出自動再送要求 (Automatic Repeat Request, ARQ) 方式が圧倒的な差を付けて重要視されていた。

筆者は大阪大学大学院に在学中、Proceedings of IRE (現 IEEE) に掲載された下記論文：

R. G. Gallager and A. B. Fontaine: “Error statistics and coding for binary transmission over telephone circuits”, Proc. of the IRE. June 1961.

を「大阪大学通信工学科雑誌会」で紹介した。この Gallager らの論文内容は以下のものであった。

“Abstract

About 2000 hours of noise data on various digital data telephone links are analyzed with respect to the applicability of coding theory to such links.

The analysis indicates that coding for error correction is inefficient for such systems, but that coding for error detection, along with feedback, is remarkably simple and effective.” (From IEEE Xplore)

筆者はこの論文内容に従って、実用的、工学的立場から誤り検出・自動再送要求 (ARQ) 方式の研究が急務であることを確信し、強く主張した。そして、主張するにとどまらず、その後数年間 ARQ 方式の研究に没頭することとなった。

しかし、興味深いことに当の Gallager は ARQ 方式の研究には全く関心がなかったことが、その後の彼の研究によって示されている。事実、Gallager は発表当時の 1963 年の時点ではほとんど注目されなかったけれど、ここ 10 数年華やかな脚光を浴びている LDPC 符号の嚆矢となった論文を世に問うている⁽¹¹⁾。

Gallager が実用的な ARQ 方式には全く興味を示さず、ランダム誤りを対象とする FEC (Forward Error Correction) の道を着実に歩んでいたことは、LDPC 符号の発表にとどまらず 1965 年、彼によって出版された論文：

“A simple derivation of the coding theorem and some applications,” IEEE Trans. Inf. Theory, IT-11, 1965.

によって強烈な印象で示されている⁽¹²⁾。

すなわち、Gallager はこの論文で次のような定理を明らかに

した。

【定理 2】 J 入力, K 出力の離散的無記憶通信路において

$$0 \leq R \leq C$$

なる情報伝送速度において, 復号誤り確率 $< P_e >$ が

$$< P_e > \leq \exp\{-nE(R)\} \quad (14)$$

を満たす符号が少なくとも一つ存在する。ただし

$$E(R) = \max_{\rho, P} [-\rho R + E_0(\rho, P)] \quad (15)$$

$$E_0(\rho, P) = -\log_e \sum_{k=0}^{K-1} \left\{ \sum_{j=0}^{J-1} P_j P(k|j)^{\frac{1}{1+\rho}} \right\}^{1+\rho}, \quad 0 \leq \rho \leq 1 \quad (16)$$

である。ここに $E(R) > 0$ はレート R に関し下に凸の単調減少関数である。また P_j は記号 j の生起確率であり, $P(k|j)$ は記号 j が記号 k に遷移する確率である。□

Gallager が導いたこの定理は任意の符号長 n に対し, 式 (14) を満たす符号の存在を (厳密に) 明らかにした。美しい定理である。この定理はブロック符号研究者に大きな勇気を与え, そして Gallager を Shannon 以来の情報理論の中興の祖として位置付けるものとなった。

この定理に至る議論の重要なポイントを 1959 年 Shannon も, 任意の符号長 n に対し, 誤り指数を導いた際に, 既に示している⁽¹³⁾。しかし天才 Shannon でもってしてもこの誤り指数は厳密 (タイト) ではなかった。すなわち任意の符号長, そして任意のレートにおいて, ランダム符号化平均復号誤り確率をより高い値に見積もらねばならなかった。

Gallager の定理は情報理論の世界で, Shannon の定理に次ぐ重要な定理として位置付けることができる。しかしこの定理の主張する点が必ずしもしっかり理解されていないと思う場にしばしば筆者は遭遇している。

Gallager のランダム符号化誤り指数は任意の符号長, 任意のレートにおいてあらゆる可能な符号を考え, その符号集合の平均復号誤り確率の上界を厳密に与える。ランダム符号化平均復号誤り確率に比べて, より小さな復号誤り確率を有する符号を組織的な手法で見いだすことは符号長が短くなるほど容易な問題になることを理解し, 注意しなければならない。

Gallager の考え方の基本は, 上述のように 1959 年の Shannon の論文の考え方の踏襲であったが, 確率式における厳密な上界式の導出が際立っていた。タイトルが示すとおり論文で使われている手法は, シンプルであるが非常に深い。実に深い。

Gallager は 100% 厳密な上界式を与えたことによって, 情報理論の中興の祖と位置付けられることとなった。この厳密な上界式の導出はもちろん Gallager 一人の天才によるものではあるけれど, Shannon, Elias, Fano, Wozencraft, Forney, Berlekamp 等々 MIT が輩出しつづけた情報理論研究の巨大な流れが, その背景にあったことは疑う余地のないことである。

Viterbi もまた MIT 情報理論研究グループの中で現れた逸材である。彼は 1967 年, Gallager のブロック符号に対し, 畳込み符号の誤り指数を導出し, 任意のレート, 任意の符号長におい

て, ブロック符号に対し, 畳込み符号が優れることを示した⁽¹⁴⁾。この Viterbi の論文は畳込み符号の研究者を勇気付けることとなったけれど BCH 符号, RS 符号等のブロック符号研究者に少なからぬ悲観的見方を与えることとなった。誤り検出再自動送要求方式の高い評価に加えて, ブロック符号に対する畳込み符号の優位性が明らかにされたわけである。RS 符号にとって厳しい時期が到来したのであった。

コーヒープレイク

電子情報通信学会の中に大きな新しい流れを作るべく情報理論とその応用学会が 25 年以上も前に誕生したのであったが, 果たして上記のような巨大な流れを作るのに貢献し得たであろうか。

情報理論とその応用学会の前身, 情報理論とその応用研究会が 1978 年に発足したが, その大きな目標は当時形骸化しつつあった電子情報通信学会に新風を吹き込むことであった。その後幸いなことに電子情報通信学会にソサイエティ化の構想が練られ, 今日の体制が出来上ったのである。このような経緯によって情報理論とその応用学会は, 初期の目標を達成し, 電子情報通信学会に“里帰り”することとなったのであると, 同学会創始者の一人としての筆者は考えている。

この里帰りを機に電子情報通信学会に, より斬新かつ, よりスケールの大きい研究の流れが作り出されることを心より期待したい。

2.4 Nyquist 問題隆盛の中での誤り訂正符号

Viterbi が論文の中で, 畳込み符号に対して想定していた復号法はやがてビタビ復号法として知られるようになった。興味深いことにビタビ復号法はパーシャルレスポンス通信路に対する優れた受信法として用いられることとなり, 誤り訂正符号の分野よりも, 1965 年に劇的な復活を遂げた Nyquist 理論の分野, すなわち波形伝送の分野で長く活躍することとなった⁽¹⁵⁾。ちなみにビタビ復号法のパーシャルレスポンス通信路に対する適用を最初に考えたのは IBM の小林と Tang であった⁽¹⁶⁾。

1960 年代に入ってコンピュータコミュニケーションのネットワークが誕生した。しかしこのコンピュータネットワークの前途に, 50~100bit/s が通信速度の限界という大きな障害が立ちわだかまっていた。

劣悪な加入者線環境下での上限値である 50~100bit/s の通信速度を改善するための最良の選択は, 符号間干渉 (intersymbol interference) を克服して通信速度を 10 倍, 100 倍に改善することである。符号間干渉をでき得る限り, 少なくするための取り組みが喫緊の課題となった。

符号間干渉を零にするという研究の嚆矢は, 古く 1924 年の昔にさかのぼる。すなわち 1924 年, Nyquist は Heaviside の理論 (1892 年) を革命的に改革し, 有限帯域幅 W の通信路において, $T = \frac{1}{2W}$ 秒の間隔で符号間干渉を完全に克服した通信が可能であることを示した⁽¹⁶⁾。驚くべき洞察である。

図4 ナイキスト理論の再発展とビタビ復号法の登場

彼は更に帯域幅 W の理想的低減フィルタの特性を $2W$ まで拡幅した全余弦下降特性 (full cosine roll-off characteristics) に修正すれば、時間間隔は依然として $T = \frac{1}{2W}$ 秒のままではあるけれど、低域フィルタの設計が容易になるという実用面での重要な手法を与えていた。Nyquist によって半世紀という“時”を超えた先駆的研究がなされていた。

上述のようにコンピュータネットワークの高速化が強く希求されたことにより、ナイキスト理論は図4に示したように鮮やかに復活し、開花した。符号間干渉を除去するという研究が極めて多様な側面から一気に開始された⁽¹⁵⁾。

図4に示したように、畳込み符号のランダム符号化誤り指数を導出する際に用いられたビタビ復号法は、誤り制御技術の世界を離れデジタル通信の抜本的高速化を図るために中心的役割を果たすこととなった。

コンピュータの TSS による利用が普及していた米国は、コンピュータネットワークの高速化の恩恵を享受できるという点で諸外国に比べ群を抜いていた。一方、当時我が国においては、コンピュータに関してはバッチ処理の態勢を維持したまま、ハード面での努力が重ねられており、“世界最高速コンピュータの実現”がその大きな目標であった。通信回線の高速化に対しても、ほぼ同じ思想で、ソフト面よりもハード面の立場からの努力が重ねられていた。

1960年代後半以降、デジタル情報通信記録システムの高速化のための研究が隆盛する中で、誤り訂正符号の研究は細々と続けられていたとの印象が否めなかった。そしてこの傾向は古い加入者線を利用せざるを得ないデジタル通信ネットワークを対象にして、可及的高速化を急ぐ米国及び日本において特に強かった。

符号間干渉のある通信路に対する最適受信法であるビタビ復号法の登場によって、デジタル情報通信の高速化を目指すソフト面重視の研究開発が、米国を中心に極めて活発に展開されることになった。このような研究の流れの中で、BCH 符号、RS 符号等のブロック符号に関する研究はマイナーな存在であったとの印象を否むことはできなかった。

これに対し、ヨーロッパでは誤り訂正符号研究の分野が着実に成長しているという印象があった。すなわち、1970年、ヨーロッパにおいてゴッパ符号が誕生し、代数幾何符号を中心とする符号理論の研究が、1970年以降、ヨーロッパを枢軸にして強力に展開されることとなった⁽⁹⁾。

コーヒープレイク

1967～1969年、筆者は米国ベル電話研究所に滞在し、超高速デジタル通信の研究に携わっていた。当時米国では TSS によるコンピュータの使用が日常化していたので、電話加入者線で結ばれたテレタイプの前に座って遠隔地にある大形コンピュータを会話型で使用していた。当時我が国ではバッチ処理による使用が日常化していたので、筆者は20年ぐらい先の未来のオフィスに座っている感覚で仕事をしていた。

プログラミングミスをリアルタイムで教えてくれるのでコンピュータを使うことが実に楽しい。TSS サービスを提供するベンチャー企業の人たちが、まるで保険のセールスのように毎月オフィスにやってきて、“こんな新しい便利な使い方ができますよ”と言って分厚いマニュアルを置いていく。

しかし、19世紀以来、音声伝送を考えるだけでよいということでも品質がほとんど改善されておらず、50～100bit/s の通信速度が精一杯という加入者線が一般に使用されているため、1枚のグラフを描くだけのデータを出力するのに1時間以上を要することが、仕事をする上での大きな障害であった。50～100bit/s の通信速度を短期間で抜本的に改善すること、これが全米の企業、大学研究機関に課せられた喫緊のテーマとなった。すなわち、高速化を強く望む全米の企業、大学研究者からの声に応えるために（加入者線はそのままにして）送受信端末のみを改善するという手法によって50～100bit/s の通信速度を可及的短期間で10倍、100倍あるいはそれ以上にするための努力が、1965年以降、国家的スケールで展開されることとなった。

図4に示した Zador, Gibby, Smith, Sunde, Lucky, Kretzmer, Tuft, Viterbi, 全てが米国の研究者である。“必要は発明の母”の典型的具体例の一つといえよう。

2.5 RS 符号に訪れた転機

デジタル通信高速化を目指す圧倒的な研究の流れに加えて、誤り検出自動再送要求方式そして畳込み符号が有力視されるという状況が一変したのは、フィリップスとソニーが、コンパクトディスク (CD) の誤り制御のために RS 符号を採用したことであった⁽¹⁷⁾⁽¹⁸⁾。

このステップを力強く支えたものは、RS 符号が

- (1) 多重バースト誤り訂正に本質的に適合すること、
- (2) 最大距離分離符号であること、
- (3) 拡大体上の符号であること、
- (4) 完全符号、均一重み符号等と組み合わせることにより、 $\mathbb{F}_2$ 上において BCH 符号を凌駕するランダム誤り訂正能力を有する符号に修正 (modify) することが可能であること⁽³⁾、
- (5) ユークリッド復号法⁽¹⁹⁾等の優れた復号法が存在すること、

(6) $\mathbb{F}_{2^8}$ 上の RS 符号は ASCII 符号に適合すること、
にあった。

リマーク 1：上記の文章，“デジタル通信高速化 … に合った”は実は極めて不確かで、ほとんど筆者の勝手な想像に基づくものである。

念のため文献⁽¹⁷⁾、⁽²⁰⁾に目を通してみたけれど、誤り訂正符号とその復号法については、高品質の録音再生を実現するために致命的に重要な役割を果たしているにも関わらず記述されていない。^(注3)

2.6 組織符号表現と非組織符号表現

Reed と Solomon は RS 符号を非組織符号の形で定義している。すなわちメッセージ多項式 $m(x)$ を拡大体 $\mathbb{F}_{2^r}$ 上で

$$m(x) = m_1 + m_2x + \cdots + m_kx^{k-1} \quad (17)$$

と表し、符号語 F を

$$F = (m(1), m(\alpha), \dots, m(\alpha^{2^r-2})) \quad (18)$$

として定義している。

しかし Peterson は 1961 年に出版した前述の名著『Error-correcting codes』において、早くもこれを組織符号として捉えている⁽¹⁰⁾。Peterson は RS 符号を前述のように $\mathbb{F}_{2^m}$ 上の多項式

$$G(x) = (x - \alpha)(x - \alpha^2) \cdots (x - \alpha^{d-1}) \quad (19)$$

によって生成される最小距離 d の巡回符号として定義している。まさに Peterson の面目躍如といえよう。そして、RS 符号の注目すべき点として

- (1) 最大距離分離符号であること、
- (2) パースト誤り訂正に適した符号であること、

を挙げている。

RS 符号の歩みにブレーキをかけた大きな要因の一つとして多くの著書あるいは論文が RS 符号を非組織符号の形で定義して議論を進めていることを挙げることができる。いち早く、巡回符号の形で捉えた Peterson をはじめ卓越した符号理論の研究者の多くが RS 符号を巡回符号の形で捉えていることに注目してほしい。

(注3)：本稿の読者から文献⁽²¹⁾に記載されているとの貴重な御教示があった。文献⁽²¹⁾によると、ソニーから RS 符号使用の提案がされ、フィリップスからは畳込み符号の提案がされた。更に上記文献⁽²¹⁾によると、これらの提案 2 方式を比較した結果、RS 符号の方が

- 効率の点で優れること
- 誤り訂正能力が高いこと

によって、ソニー提案の RS 符号が採用された。まさに RS 符号そしてその復号法の命運を左右する決定がなされたのであった。貴重な文献⁽²¹⁾を御教示下さった読者に深く感謝したい。

学部学生を含む若い研究者層が一般に巡回符号に習熟し、しかもより深く RS 符号を理解できることを考えると、筆者は RS 符号を教える際には最初から巡回符号の形で習得させることを強く奨めたい。このことによって RS 符号を深く理解することができ、より広い応用の道を切り開くことができよう。

次章では RS 符号の半世紀を広がりゆく応用性という立場から考えて解説してみたい。なお、RS 符号は上述した理由を考慮して、組織符号として捉えて議論を進める。

3. 広がりゆく RS 符号の応用性

3.1 通信路符号化法への応用

1966 年、Forney によって提案された接続符号 (Concatenated code) は積符号の一つのクラスである⁽²²⁾。1970 年代、接続符号は

- (1) 通信路符号化への応用
- (2) 漸近的に良好な符号を構成することへの応用
- (3) $\mathbb{F}_2$ 上ランダム誤り通信路における最良符号構成への応用

によって符号理論の世界で最も注目される符号の一つとして位置付けられることとなった。接続符号の構造を図 5 に示す。

この Forney による接続符号に類似した構造を有する符号が、1964 年という早い時期に電気通信学会 (現電子情報通信学会) 雑誌に掲載されている⁽²³⁾。読者の興味のため同雑誌 p.596 に記述されている文章を以下に転載しよう。

— 以下、文献⁽²³⁾p.596 より引用 —

“前節の所論にしたがって、著者らはつぎに述べる重複巡回符号を提案する。 k 次の重複巡回符号 $F^{(k)}$ をつぎのようにベクトル的に表わして定義する。

$$F^{(k)} = (F_1^{(k-1)}, F_2^{(k-1)}, \dots, F_{N_k}^{(k-1)}, C^{(k-1)}) \quad (25)$$

$F_r^{(k-1)}$ ($r = 1, 2, \dots, N_k$) は $(k-1)$ 次の重複巡回符号であって、符号長はいずれも相等しく $n = n_{k-1}$ である。 $C^{(k-1)}$ は N_k 個の $(k-1)$ 次の重複巡回符号 $F_1^{(k-1)}, F_2^{(k-1)}, \dots, F_{N_k}^{(k-1)}$ に対する検査点である。”

$k = 1$ とした特別な場合、すなわち

$$F^{(1)} = (F_1^{(0)}, F_2^{(0)}, \dots, F_{N_1}^{(0)}, C^{(0)}) \quad (20)$$

図 5 接続符号

では、内部巡回符号 $F_i^{(0)}; i = 1, 2, \dots, N_1$ を新たに情報記号とみなして、外部符号化の検査記号 (1964 年当時は上記のように検査点という用語が使用されていた) $C^{(0)}$ を付している。

式 (20) で示した一次重複巡回符号の構造は Forney が提案した接続符号の構造にぴったり一致している。2 年も早い時期に接続符号の基本的な構造は日本の学術雑誌に既に掲載されていた。この完全な一致性を後ほど図 7 の具体例で理解することにしてしよう。

なお、 $k \geq 2$ 以上の重複巡回符号は現在の用語に合わせるならば k 重接続符号と呼ばなければならない。

コーヒーブレイク

1968 年米国ニュージャージー州のローカルな会議において地元研究者が Forney の接続符号について解説し、この接続符号の有用性を強調した。たまたまこのとき、筆者はニュージャージー州のベル研究所で超高速 PCM 通信の開発研究をしていたので、この会議への出席の機会が与えられていた。筆者は上記重複巡回符号と接続符号の類似性を直ちに指摘したのであったが、結局議論に結論が出ないまま終わったように記憶している。

筆者がこの後、それ以上追及しなかった理由は一つにはデジタル通信ネットワークにおける重要な課題としての“ネットワーク同期”の研究に、興味の中心がすっかり移っていたことにもあるけれど、Forney がランダム誤りの通信路を仮定し、誤り指数を導出するのに秀逸な議論を展開していたことに深く感動したことも他の大きな理由の一つであった。

Shannon, Gallager 等々、MIT 研究者たちによって伝統的に受け継がれた情報理論の力強い研究の流れが、Forney の接続符号考案の背景にあった。これに対し重複巡回符号の背景には現実的なバースト誤り通信路を主対象とする我が国における実用的研究優先主義、学会における有用性重視主義の背景があった。大きな差であったと考えられる。

1972 年、デンマークの若き大学院学生 Justesen は漸近的良質な符号を構成することに見事成功し、情報理論の世界に非常に大きな衝撃を与えた⁽²⁴⁾。Justesen を見いだしたのは当時ヨーロッパに滞在していた著名な研究者 Massey 博士であった。この時期がちょうど ISIT'72 が米国ノートルダム大学で開催される直前であった。Massey 博士の働きかけもあって Justesen は急きょこの国際会議に特別講演者として招かれることとなり、彼にとって最高の晴れ舞台が用意されることとなった。会場は熱気にあふれ Justesen の講演に熱心に耳を傾けていた様子が、筆者の脳裏に今も強く残っている。

彼の素晴らしい着想を成功させた最大の理由は RS 符号の最大距離分離性であり、その最大距離分離性を最大限に引き出すことを可能にした接続符号の存在であった。満場の会場は彼の構成法の成功を支えた RS 符号の秀逸性を、符号理論研究者に強く印象付けるものともなった。

一方、Clark と Cain は 1980 年代初頭、接続符号のパフォーマンスを詳細に解説し、RS 符号の有用性を必ずしも明示的では

ないが示している⁽²⁵⁾。

RS 符号を外部符号とする $\mathbb{F}_2$ 上の最良符号の構成は非常に興味深く、文献⁽³⁾に詳しく解説されている。

代数的符号の分野では

- 符号構成問題
- 復号問題

がテーマとしての双璧である。また純粋数学的な立場からも興味深い問題である。

代数的符号の持つべき“良き性質”の代表は前述のように

- 完全性
- 最大距離分離性
- 均一重み性

である。

全ての成分が零である符号語 v_0 と全ての成分が非零の成分である符号語 v_1 からなる自明な符号 $\{v_0, v_1\}$ は完全性、最大距離分離性両方の性質を有している。非自明な完全符号としては最小距離 3、符号長 $2^a - 1$ ($a: 3$ 以上の正整数) のハミング符号と最小距離 7、符号長 23 のゴレー符号及び $\mathbb{F}_3$ 上の最小距離 5、符号長 11 のゴレー符号のみである。しかしいずれも最大距離分離符号ではない。均一重み性を有する符号の代表は最大周期系列 (maximum period sequence) であって、相関特性がインパルスに近い、様々な工学的応用の道が開かれている。

一方 RS 符号は完全符号ではないけれど最大距離分離性を有するという点で“良き符号”である。

そして上述のように、この最大距離分離性によって一般に $\mathbb{F}_{2^r}$ ($r \geq 2$) 上の RS 符号が $\mathbb{F}_2$ 上のいわゆる最良符号 (best code) を生み出すことができる。接続符号における不動の外部符号として、組織符号の形で定義された拡大体上の RS 符号は、素体上の最良符号構成問題においても威力を発揮し、その最大距離分離性がこれらの成果において生かされた。RS 符号の秀逸性を符号理論の世界に強く印象付けることとなった。次節でこのことを解説してみたい。

3.2 RS 符号と完全符号の組合せ

ここでは図 6 に示したような“良き符号”の組合せを考えてみよう。

RS 符号、パリティチェック符号、繰返し符号 $\{(0, 0, \dots, 0), (1, 1, \dots, 1)\}$ は最大距離分離性を有するという意味で“良き符号”である。一方、ハミング符号、ゴレー符号そして繰返し符号は完全性を有するという意味で“良き符号”である。“良きもの”が集って“良きもの”が生まれるということは数学の世界における一つの哲学である。なお、その典型的な具体例の幾つかが文献⁽²⁶⁾に記述されているので参照して頂ければ幸いである。

筆者らは 1977 年、後ほどアレー符号と呼ばれることとなった KS 符号化法をこの考えに従って与えている。この KS 符号化法は MacWilliams と Sloane の著書⁽³⁾p.590 に詳細に記述されている。以下 KS 法について p.590 に記載されている具体例を

図 6 良い符号の組合せ

図 7 KS 符号化の原理図。

— 二次伸長 (17, 11, 7) RS 符号の場合 —

参照して解説しよう。 $\mathbb{F}_{2^r}$ ($r > 1$) 上の最大距離分離符号である RS 符号が $\mathbb{F}_2$ 上の最良符号を生み出すという興味深い具体例の一つである。ランダム誤り訂正において、ランダム誤り訂正のスペシャリストたる BCH 符号を上回る符号に変身する事実注目したい。

図 7 に KS 構成法の原理を示す。

$\mathbb{F}_{2^4}$ 上の二次伸長 (17, 11, 7) RS 符号, (17, 1, 17) 繰返し符号, (5, 4, 2) パリティチェック符号を図 7 に示したように組み合わせると (17・5, 4・11 + 1, 2・7) 符号すなわち (85, 45, 14) 符号が構成される。この符号を 1bit 短縮すると (84, 45, 13) 符号となるが、この符号は MacWilliams と Sloane が編さんした最良符号表の中に $n = 84$, $d = 13$ としたときの最良符号として収められている。式 (21) において $F_1^{(0)}, \dots, F_{11}^{(0)}$ を (5, 4, 2) 符号とし, $F_1^{(0)}, \dots, F_{11}^{(0)}$ を改めて情報記号とみなして検査記号 $C^{(0)}$ を導く。これは我が国で 1964 年に提案されていた一次重複巡回符号の具体例であるが、MacWilliams と Sloane⁽³⁾ の表現を借りれば“ This is a simple form of concatenation ”ということになる。2 年後に米国で提案された接続符号の具体例でもあるわけである。この一次重複巡回符号の検査記号の部分に完全符号であり、かつ均一重み符号でもある (17, 1, 17) 繰返し符号を重畳すると図 7 に示したような最良符号の一例を導くことができる。

RS 符号に基づく KS 符号化法によって導かれる符号は最良符号表で KS 符号として引用されているが、同表において BCH 符号とは数の上ではほぼ同数である。RS 符号は最大距離分離符号 (パリティチェック符号) と完全符号 (奇数長の繰返し符号) を伴うことによって、BCH 符号を上回る符号に変身する。符号構成問題において注目すべき事実である。

符号長、最小距離が大になるほど KS 符号は BCH 符号に比べ有利になることが予想される。ちなみに $d = 29$, $n \leq 512$ の範囲での最良符号の数は BCH 符号に基づくものが 3 であるのに対し、KS 符号は 5 となっている⁽³⁾。最小距離 d , 符号長 n が大になるほど RS 符号の最大距離分離性が発揮されることが容

易に想像される。

では、符号長が数万、最小距離が数千といった非常に大きい符号の使用が許容されるであろう将来のランダム誤り通信路上で活躍するブロック符号はどんな符号であろうか。

MacWilliams と Sloane 編さんの表を参照すると

- KS 符号
- GP 符号
- XQ 符号

が三大候補として挙げられる (上記の符号名は MacWilliams と Sloane に従う)。いずれもその構成法に筆者が関わっているもので、いずれの符号が最も推奨されるかと問われても、答え難い一面がある。しかしこの思いを振り切って答えるならば KS 符号が薦められる。その理由は

- 符号長が非常に大になっても、RS 符号は符号長に関係なく最大距離分離性が発揮されること。
- KS 符号化は原理が非常に単純で、その原理を図 7 のように図示することができるため、技術者の直観的理解が容易であること。

にある。

なお、情報記号数が 2~10 というような特にレートが低い範囲での符号構成問題は BCH 符号, RS 符号, ゴッパ符号の延長線上では議論することが困難であり、別なアプローチを考えねばならない。広い範囲の符号長に対して、情報記号数が 2~10 と少ない場合の (最適線形符号の下界を満たす) 線形符号の組織的構成法が 2010 年、笠原、平澤によって与えられている⁽²⁷⁾。

3.3 RS 符号の能力

誤り訂正符号においては実用的立場から復号の容易さが優先されるために誤り訂正能力は一般に低く見積もられる。RS 符号においてもこのことは例外ではなく、代数的復号が容易な限界距離復号法で保証された誤り訂正個数 t を

$$2t + 1 = d \quad (21)$$

と設定し、実用上はこの値が用いられている。ただし d は最小距離である。本節では式 (21) で与えられる t を超えた $t + 1$ 以上の誤りが RS 符号に生じた場合についての振舞いを考察してみたい。

1964 年、筆者は、当時符号理論の分野で大きな注目を集めていたファイア符号、つまり一般に長さ b 以下の単一バースト誤りを訂正するファイア符号を対象にして、訂正能力を超えた $b + 1$ 以上のバースト誤りが生じた場合、この誤りを b 以下のバースト誤りとして誤って訂正する確率を理論的に解析するとともに、全 NOR 回路によって組み立てられた専用コンピュータによるシミュレーション結果を与えた⁽²³⁾。

この結果は訂正能力 b を超えた近辺 $b + 1 \sim 2b - 1$ のバースト誤りを長さ $2b$ 以上のバースト誤りに比べて、より高い確率で訂正することを予想させるものである。RS 符号においても誤り

訂正能力 t を超えた $t+1$ 以上 $t+\delta$ (δ は t に対し十分小さな値) 以下という比較的 t に近い個数の誤りを高い確率で訂正することは、この結果より十分に期待される。

RS 符号が限界距離を超えた誤りを検出する確率、あるいはその一部を訂正する確率も上記考察の延長線上で求めることができる。

1986 年, McEliece と Swanson⁽²⁸⁾, 1989 年, 羽田, 森井, 笠原⁽²⁹⁾そして 1991 年, 森井⁽³⁰⁾によって, これらの確率はより厳密に解析され報告されている。限界距離を超えた誤りをリスト復号する手法が近年注目を集めており, 文献⁽³¹⁾に興味深い解説が与えられている。

RS 符号に ε 個の誤りが生起する確率を $P[\varepsilon]$ と表記する。このとき RS 符号が限界距離復号法によって式 (21) で与えられる t 個以下の誤りを訂正すると考えると一般に

$$1 \gg P[t] > P[t+1] > \dots \quad (22)$$

が成立する。確率 $P[\varepsilon]$ は上式に示したように, 一般に $1 \gg P[t]$ の関係が成り立つこと, 及びこの関係のもとでは $t+\delta$ 個の誤りの生起確率はシンボル誤り率を p とすると $P(t)$ に対しほぼ p^δ 倍に減少すること, 及び元々 $P[t]$ は十分小さな値に設定されることを考えると, 限界距離を超えた誤りを訂正することは通信路の信頼度改善に関しては必ずしも劇的な効果が期待されないことが明らかである。

しかし私たちが非常に注意しなければならないことは, 比較的大きな t に対し $t+1$ 以上の誤りのうちごく一部, 例えば 10^{-18} 程度であったとしても, これらを容易に復号できる手法が確立されれば (t が比較的小さければ常に容易), RS 符号を用いた秘密分散保管方式においてはしきい値をより安全側に設定するといった万全の注意を払わなければならないということである (3.9 参照)。

3.4 通信路符号化への応用, それを支えた復号法

1980 年代, CD において高品質の再生を実現するために RS 符号は広範に使用され始めた (リマーク 1 参照)。RS 符号について当初から指摘されていた長所の一つ, パースト誤り訂正に適合していることが, ようやく実用の世界で認められたのである。

1960~1970 年代, 符号理論の分野では符号構成法と並ぶ二大テーマの一つ, 復号法の研究も極めて活発であった。その成果として, 雑音を取り除くために CD, DVD プレーヤの心臓部に

- (1) ユークリッド復号法 (E 法)⁽³⁾
- (2) パーレカンブ・マッシュ法 (BM 法)⁽³⁾
- (3) ピーターソン法 (P 法)⁽³⁾

が使用されているが, 世界的に見てユークリッド復号法が主流となっている。ちなみにこれら E 法, BM 法, P 法に関する特許件数は内外のものを合わせるとほぼ 10 : 3 : 3 となっており, このことを裏付けている⁽¹⁹⁾。ユークリッド復号法はその名も示すとおり, ユークリッド互除法という“良きもの”にその原理が従うことに注意したい。

各種誤り訂正符号を支える優れた復号法の存在を私たちは忘

図 8 公開鍵暗号構成への期待度

れてはならないと思う。

3.5 情報源・通信路同時符号化への応用

多重パースト誤りの形で出力される情報源の符号化には RS 符号が威力を発揮する。離散的に生成される $\mathbb{F}_{2^m}$ 上のデータ $B_1, B_2, \dots, B_k$ を $\mathbb{F}_{2^m}$ 上のランダム誤りとみなし, RS 符号のシンδροーム $H(S)$ を導く。このとき $H(S)$ は情報源・通信路同時符号化の符号語として用いることができる。すなわち, 情報源符号化符号語に生じた

$$2(k+t)+1 \leq d \quad (23)$$

を満たす t 重の通信路誤りを訂正することが可能である。

RS 符号の同時符号化への応用がいつ頃に提唱されていたか。筆者自身も同時符号化への応用という考えは 1975 年頃 (自明な考えとして) 持っていたけれど, 誰もが思いつくアイデアという印象を持っていたので, このことに言及した文献は筆者自身の著書も含めて, 内外の文献に周知していない。この件について読者諸賢より御教示頂ければ大変有難いと思う。

3.6 公開鍵暗号構成への応用

非常に大きなクラスの符号であるゴツパ符号が, McEliece によって首尾良く公開鍵暗号に応用されて以来, 誤り訂正符号の公開鍵構成への応用が注目されている⁽³²⁾。しかし, 図 8 に示したようにゴツパ符号に比べると非常に小さなクラスの符号である BCH 符号の更に一つのサブクラスにすぎない RS 符号は, 攻撃者側から見ると使用生成多項式が推定容易な符号であることによって, 始めから危たい視される傾向にあり, 現状ではほとんど無視された存在である。

通信路誤り訂正には大きなクラスの符号でありかつ強力な誤り訂正能力を有することが一般に望まれよう。しかし, 注意すべきことは, 暗号の分野ではこのような符号であることは明らかに必要条件でも十分条件でもないということである。

事実, 公開鍵暗号構成の際には, 良き符号の代表

- (1) $\mathbb{F}_{2^m}$ 上の RS 符号
- (2) $(7, 4, 3)$ ハミング符号, $(3, 1, 3)$ 符号等の小さなサイズの完全符号

を有効, かつ安全に利用し得ることが筆者によって示され, 誤り訂正符号応用公開鍵暗号 (Code Based PKC, CBPKC) の新しいクラスとして構成されている⁽³³⁾ (34)。

2010 年, 筆者は RS 符号を用いて公開鍵暗号 K(IV)SE(1)PKC を構成したが, この公開鍵暗号は現時点で想定できる攻撃に耐

えるほか以下のような特徴を有している．

- McEliece 暗号の符号化レート ρ が $\rho = 0.5$ であるのに対し，RS 符号に基づく K(IV)SE(1)PKC は $\rho = 0.8 \sim 0.9$ の高い符号比率が達成可能であること．
- McEliece 暗号に比べ公開鍵サイズを小さくし得ること．
- 上記符号比率の改善によってデジタル署名の実現が McEliece 暗号と比べると容易になること．

他符号に比べ実用面において抜群の実績を有する RS 符号には，ハード及びソフト両面において膨大なノウハウの蓄積が期待される．これらの貴重な資産を背景にした RS 符号が，最大距離分離性という符号としての良き性質をフルに発揮することによって公開鍵暗号の分野で，将来，先導的に利用されることは火を見るより明らかなことである．RS 符号に基づく将来の公開鍵暗号が McEliece 暗号あるいは K(IV)，K(V)SE(1)PKC とは全く異なった発想に基づくものであることもまた明らかなことである．

3.7 秘密分散保管への応用

1979 年，Shamir と Blakley は独立に秘密分散法という興味深い暗号手法を提案した^{(35) (36)}．数年後，McEliece と Sarwate は Shamir の手法を非組織的 RS 符号を用いて実現した⁽³⁷⁾．

2002 年，Juels と Sudan は，RS 符号を応用してファジーボールドスキーム (Fuzzy Vault Scheme) という秘密分散法に関連した興味深い手法 (JS 法) を提案した⁽³⁸⁾．この手法は近年バイオメトリクスの分野において大きな注目を集めているが，この手法においてもやはり非組織的 RS 符号を用いている．以下，この Juels と Sudan の手法について解説しよう⁽³⁹⁾．

$\{S_i\}$ を $\mathbb{F}_{2^m}$ 上のアリスの秘密 (例えば指紋認証におけるマニューシャ) の集合とし， $P(x)$ は鍵情報多項式，すなわち他の秘密を開錠するための秘密鍵を係数とする多項式である．

認証センター C はアリスを認証するため $\{(S_i, P(S_i)); (T_i, Z_i)\}$ を保有している．ただし (T_i, Z_i) は秘密ペア $\{S_i, P(S_i)\}$ を隠蔽するためのダミーペアであって， T_i, Z_i は $T_i \in \mathbb{F}_{2^m}$ ， $Z_i \in \mathbb{F}_{2^m} - \{S_i\}$ と設定されている．アリスは本人であるために多数の正当なペア $\{(S_i, P(S_i))\}$ を選択できるので秘密多項式 $P(x)$ を復元することができる．JS 法は非組織符号の形で定義された RS 符号を深く洞察した結果編み出された手法であることが了解される．

しかし，RS 符号を組織符号の形で捉えたと JS 法とは全く異なった別な手法が視界に入ってくる．筆者は 2000 年前後から，秘密分散法においては組織的 RS 符号を用いるべきことを主張してきている^{(40)~(43)}．非組織符号の形では捉えきれなかった RS 符号の有用性がより鮮明に顕在化されると思う．

更に注意しなければならないことは，誤り訂正符号の良さは優れた復号法とともに並存して発揮されるという事実である．例えば，組織的 RS 符号に基づく秘密分散保管法を K 復元法を通して眺めると，圧倒的に深い意味を伴って理解することができるよう⁽⁴⁴⁾．

ちなみに K 復元法をバイオメトリック認証に応用すると，

- (i) 被検証者は自己の秘密 (例えばマニューシャ) を全く提示することなく，代わりに秘密 (マニューシャ) のハッシュ値の更にハッシュ値，すなわち 2 ステップのハッシュ値を用いることによって，自己を検証することが可能，
- (ii) 秘密 (マニューシャ) に関わる条件付エントロピーを十分大にしたまま，すなわち秘密に対し，限界距離復号法のみが実用上可能という条件のもとで情報理論的に十分な安全性を保証することが可能，

という認証システムを構築することができる^{(45) (46)}．JS 法においてはランダムペアを混ぜているとはいえ，秘密そのもの，すなわち $\{S_i\}$ を検証者に預けていることに注意したい．

3.8 RS 符号の応用に際しての留意事項

RS 符号の応用範囲は将来ますますその裾野を広げていくであろう．RS 符号の有用性が，強く認識されることが期待されるが，RS 符号の応用に際しては以下の 2 点に留意しなければならない．

- (1) RS 符号は最大距離分離符号ではあるが完全符号ではないこと．
- (2) 完全符号ではないことによって，最小距離で保障された誤り個数以上の誤りを小さな確率ではあるが訂正可能であること．

(1) は 3.6 で述べた誤り訂正符号応用公開鍵暗号 (CBPKC) を構成する際にデジタル署名が CBPKC の嚆矢となった McEliece 暗号に比べて容易になるというものの実用面という点からは必ずしも十分ではないという問題を提起する．(2) は 3.7 で述べた秘密分散保管問題において，しきい値をより安全側に設定することを要求する．

(1) 及び (2) は RS 符号の応用にあって留意すべき基本的なことであるので，以下，節を改めて解説しよう．

3.9 RS 符号応用に関わる問題

— 新たに関ける可能性 —

(I) RS 符号は最大距離分離符号ではあるが完全符号ではないこと

誤り訂正符号に基づく公開鍵暗号，すなわち CBPKC を構成する問題について，McEliece 暗号とは全く異なったアプローチをとることにより，以下のことが可能となることが明らかにされている^{(33) (34)}．

- RS 符号を用いると安全性を損うことなく，McEliece 暗号よりもレートの高い CBPKC を構成し得ること．
- RS 符号を用いると McEliece 暗号に比較し，デジタル署名がより容易に実現されること．

以上において RS 符号は最大距離分離符号であるが，完全符号ではないことに注意しなければならない．ちなみに最大距離分離性は有さないが完全性を満たす符号を用いた場合はどうで

あろうか．ハミング符号，ゴレーイ符号等の完全符号を用いるとレート厳密に 1.0 とし，それゆえにデジタル署名が非常に容易に実現されるという特徴を有する CBPKC として $K(IV)SE(1)PKC$ が提案されている⁽³³⁾⁽³⁴⁾．RS 符号の最大距離分離性を 100 % 生かし，かつ $K(IV)SE(1)PKC$ とは全く異なったアプローチをとることにより， $K(IV)SE(1)PKC$ を凌駕する RS 符号応用 CBPSK を考案することが強く望まれる．

(II) RS 符号は限界距離復号法的能力を超えた誤りを効率良く訂正し得ること．

RS 符号において t を十分大として限界距離を超えた誤りを効率良く訂正できる実用的な手法が広く普及すれば，RS 符号に基づく秘密分散保管システムはしきい値をより安全側に設定することを念頭において，その設計方針を大きく変更する必要がある．

RS 符号にとって不利となるこの問題は，将来，克服されるであろうか．より明るい方向への具体的な手法が見いだされるであろうか．筆者はここ 1, 2 年この問題への考察を深めているが，十二分に可能という確信を得ている．ここではその考え方，原理を容易に理解し得る有限環上の連立方程式を用いた秘密分散保管システムの例⁽⁴⁷⁾⁽⁴⁸⁾で考えてみることにしよう．

この連立方程式を

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1N}x_N &= w_1 \bmod H \\ &\vdots \\ a_{i1}x_1 + a_{i2}x_2 + \cdots + a_{iN}x_N &= w_i \bmod H \\ &\vdots \\ a_{K1}x_1 + a_{K2}x_2 + \cdots + a_{KN}x_N &= w_K \bmod H \end{aligned} \quad (24)$$

と表す．ただし $x_1, x_2, \dots, x_N$ は秘密とし，また $w_1, w_2, \dots, w_K$ は復元用公開データとする．また係数行列は Vandermonde 行列式とする．

上式において任意の $(N - K)$ 個の秘密が与えられれば残る K 個の秘密は公開データ $w_1, w_2, \dots, w_K$ を用いることにより正しく復元される．このとき，以下の自明な定理が成立する．

【定理 3】復元すべき任意の K 個の秘密に対する係数行列式 (Vandermonde 行列式) を D とする． D と法 H の最大公約数を L とすると式 (22) の解は L とおりに与えられる⁽⁴⁷⁾⁽⁴⁸⁾．□

【系】 H が素数のとき解は 1 通りに与えられる． □

K 個の秘密のいかなる組合せに対しても，均一に L とおりの解を与える理想的な例を求めることは必ずしも困難ではなく， $K = 2, N = 4$ 程度であれば手計算で求めることができる．

上記有限環上の連立方程式を用いた秘密分散システムの例を RS 符号を用いた秘密分散システムに翻訳することによって新しい秘密分散保管システムを構築することが可能と思われ，現在検討を深めている．将来，機会があれば報告したい．

限界距離を超えた誤りを実用上効率良く訂正する手法が確立されれば RS 符号を用いた秘密分散保管システムに大きな可能性が与えられることは明らかなことである．すなわちこの新

しい秘密保管システムが，近年とみに注目を集めているバイオメトリクス，特に多モードのバイオメトリクス (multi-modal biometrics) に適合することは明白なことである⁽⁴⁶⁾．RS 符号のバイオメトリクスへの応用の道が将来大きく開けよう．

4. む す び

本稿では，RS 符号の半世紀をデジタル情報通信記録技術の発展の歴史の中で捉え，RS 符号の幅広い応用性について解説した．

本稿では誤り訂正符号に望まれる“良き性質”として

- 完全性
- 最大距離分離性
- 均一重み性

を挙げた．

RS 符号が他の非自明な符号には見られない最大距離分離性を有することこそが，RS 符号を誤り訂正符号の中で最高の地位にランク付ける最大の理由であることを指摘するとともに，“最大距離分離性を有する RS 符号”という切り口からの解説を試みた．また RS 符号が符号理論の分野で最高の評価を受けるに至った経緯を情報通信・記録システムの過去半世紀を越える発展の歴史の中で幅広く鳥瞰して捉えた．

誕生後 20 年近く，ランダム誤り訂正符号の代表格である BCH 符号あるいは単一バースト誤りを訂正する優れた符号として知られたファイア符号に比べると，RS 符号はマイナーな存在であった．しかしながら，以下の事実，すなわち

- 最大距離分離符号である RS 符号が他の完全符号であり，かつ最大距離分離符号であるパリティチェック符号，繰返し符号を伴うことによってランダム誤り訂正能力において BCH 符号を凌駕する符号へと姿を変えたこと
- 通信回線の高速化，メモリの大容量化に伴い，長大な複数個の誤りを訂正するのに RS 符号は本質的に適合していること

という事実によって，RS 符号は

- ランダム誤り通信路
- バースト誤り通信路

の両者において，最も適合する代数的誤り訂正符号として位置付けられることとなった．このことは通信路の統計的性質の変化，すなわちバースト性，ランダム性のいかに問わず，常に通信路の変化に時々刻々適応し得ることを意味する．RS 符号が代数的誤り訂正符号の中で最上位にランク付けされる理由である．

本稿ではこのような優れた性質を有する RS 符号について，誤り訂正の分野だけではなく

- 公開鍵暗号
- 秘密分散保管システム
- バイオメトリクス

等々の分野における応用の道が，大きく広がりつつあること

を指摘し、解説した。

過去 60 年、誤り訂正符号の分野で蓄積された膨大な知識、ノウハウを背景にした RS 符号が「誤り訂正符号」の分野だけでなく「情報セキュリティ」等の分野で創造的な新分野を切り開くことを祈念して本稿を欄筆したい。

謝 辞 本稿をまとめるに当たり多々御尽力頂いた工学院大学斎藤秀俊先生、そして懇切に御査読下さいました 3 人の閲読者の方々に深く感謝したい。また本稿企画の段階より、多数の方々から労をいとわぬ温かいサポートを頂いた。ここに記して感謝の意を表したい。

文 献

- (1) C. E. Shannon, "A mathematical theory of communication," Bell Syst. Tech. J., vol.27, pp.379-423 and 623-656, Jul. and Oct. 1948.
- (2) R. W. Hamming, "Error detecting and error correcting codes," Bell Syst. Tech. J., vol.29, no.2, pp.147-160, April 1950.
- (3) F. J. MacWilliams and N. J. A. Sloane, The theory of error-correcting codes, North-Holland, 1977.
- (4) I. S. Reed and G. Solomon, "Polynomial codes over certain finite fields," J. SIAM, vol.8, no.2, pp.300-304, June 1960.
- (5) A. Hocquenghem, "Codes correcteurs d'erreurs," Chiffres (Paris), vol.2, pp.147-156, Sept. 1959.
- (6) R. C. Bose and D. K. R. Chaudhuri, "On a class of error correcting binary group codes," Inf. Control, No.3, no.1, pp.68-79, Mar. 1960.
- (7) 笠原正雄, "リード・ソロモン符号の 50 年 - 広がり行くその応用性 -, " 2010 信学ソ大 (基礎・境界), no.AT-2-1, pp.SS-41-SS-44, Sept. 2010.
- (8) 笠原正雄, 田崎三郎, 小倉久直, "情報理論," 昭晃堂, 東京, 1985.
- (9) V. D. Goppa, "Rational representation of codes and (L, g) -codes," Probl. of Inf. Transm., vol.7, no.3, pp.223-229, 1971.
- (10) W. W. Peterson, Error-correcting codes, MIT press, 1961.
- (11) R. G. Gallager, Low-density parity-check codes, MIT Press, Cambridge, Mass., 1963.
- (12) R. G. Gallager, "A simple derivation of the coding theorem and some applications," IEEE Trans. Inf. Theory, vol.IT-11, no.1, pp.3-18, Jan. 1965.
- (13) C. E. Shannon, "Probability of error for optimal codes in a Gaussian channel," Bell Syst. Tech. J., vol.38, no.3, pp.611-656, 1959.
- (14) A. J. Viterbi, "Error bounds for convolutional codes and an asymptotically optimum decoding algorithm," IEEE Trans. Inf. Theory, vol IT-13, no.2, pp.260-269, April 1969.
- (15) 笠原正雄, "符号化変調方式 (I) , デジタル変調方式とその発展を支えたテクノロジー , " 信学誌, vol.72, no.1, pp.97-106, Jan. 1989.
- (16) H. Kobayashi and D. T. Tang, "Application of partial-response channel coding to magnetic recording systems," IBM Journal of Research and Development, vol.14, no.4, pp.368-375, July 1970.
- (17) Sony Japan, "第 2 部, 第 8 章 レコードに代わるものはこれだ," Sony History, 1995.
- (18) Sony Japan, "第 2 部, 第 7 章 デジタルをものにしてみせる," Sony History, 1996.
- (19) 平澤茂一, 笠原正雄, "ユークリッド復号法," IEICE Fundamentals Review vol.4, no.3, pp.183-191, Jan. 2011 .
- (20) H. Nyquist, "Certain factors affecting telegraph speed," Bell Syst. Tech. J., vol.3, no.2, pp.324-346, 1924.
- (21) K. A. S. Immink, "Shannon, Beethoven, and the compact disc," IEEE Inf. Theory Society Newsletter, Dec. 2007.
- (22) G. D. Forney, Jr., Concatenated Codes, MIT press, Cambridge, MA., 1966.
- (23) 笠原芳郎, 笠原正雄, "バースト誤りを訂正する巡回符号に関する考察," 信学誌, vol.47, no.4, pp.590-598, April. 1964.
- (24) J. Justesen, "A class of constructive asymptotically good algebraic codes," IEEE Trans. Inf. Theory, vol.IT-18, no.5, pp. 652-656, Sept. 1972.
- (25) G. C. Clark, Jr and J. B. Cain, Error-correction coding for digital communications, Plenum Press, 1981.
- (26) 笠原正雄, "格子理論とその応用へのガイダンス," 信学論 (A) , vol.J82-A , no.8 , pp.1239-1252, Aug. 1999.
- (27) M. Kasahara and S. Hirasawa, "Constructions of a large class of optimum linear codes for small number of information symbols," 信学技報, IT2009-137, ISEC2009-145, WBS2009-116, pp.419-426, March 2010.
- (28) R. J. McEliece and L Swanson, "On the decoder error probability for Reed-Solomon codes," IEEE Trans. Inf. Theory, vol.IT-32, no.5, pp.701-703, Sept.1986.
- (29) 羽田 享, 森井昌克, 笠原正雄, "Reed-Solomon 符号に対する拡張シンドローム復号法とその評価", 第 12 回情報理論とその応用シンポジウム資料, no.2, pp. 523-528, Dec. 1989.
- (30) 森井昌克, "リードソロモン符号のシンボル誤り訂正能力について," 信学論 (A) , vol.J74-A , no.1 , pp.96-103, Jan. 1991.
- (31) 松本隆太郎, "リードソロモン符号のリスト復号," 2010 信学ソ大 (基礎・境界) , no.AT-2-2, pp.SS-45-SS-46, Sept. 2010.
- (32) R. J. McEliece, "A public-key cryptosystem based on algebraic coding theory," DSN Progress Report, 42-44, pp. 114-116, Jan. and Feb. 1978.
- (33) M. Kasahara, "A construction of new class of linear multivariate public key cryptosystem constructed based on error correcting codes," 信学技報, ISEC2009-127, IT2009-135, WBS2009-106, pp.361-366, March 2010.
- (34) M. Kasahara, "New class of public key cryptosystems constructed based on error-correcting codes, using K(I II) scheme -Appendix, Proposal of K(IX)SE(g)PKC-, " 信学技報, ISEC 2010-7, pp.41-48, May 2010.
- (35) A. Shamir, "How to share a secret", Commun. ACM, vol.22, no.11, pp.612-613, 1979.
- (36) G. R. Blakley, "Safeguarding cryptographics keys," Proceedings of AFIPS National Computer Conference, pp.313-317, June 1979.
- (37) R. J. McEliece and D. V. Sarwate, "On sharing secrets and Reed-Solomon codes," Commun. ACM, vol.24, no.9, pp.583-584, 1981.
- (38) A. Juels and M. Sudan, "A fuzzy vault scheme," ISIT 2002, p.408, June 30-July 5 2002.
- (39) A. Juels and M. Sudan, "A fuzzy vault scheme," Design, Codes and Cryptography, vol.38, no.2 pp.237-257, Feb. 2006.
- (40) 笠原正雄, "パスワード忘却防止問題," 信学基礎・境界サイエティ・ニューズレター, Sept. 2000.
- (41) 笠原正雄, "有限体上の新しい積和暗号について (付 パスワード忘却防止問題の一つの解) ," SCIS 2001 , 3B-3, 2001.
- (42) 笠原正雄, "忘却情報復元問題," SCIS 2002, 2A-3, pp.13-18, 2002.
- (43) 笠原正雄, "符号と暗号 - その織りなす世界に見られる共通点と相違点 -, " 数学セミナー, vol. 45, no.10, pp.12-15, Oct. 2006.
- (44) 辻井重男, 笠原正雄 (編著) , "暗号理論と楕円曲線," 森北出版, 東京, 2008.
- (45) 笠原正雄, "忘却秘密復元法とファジィボルトスキーム - 新しいバイオメトリクス方式の提案 -, " ISEC 2009-43, pp.23-27, Sept. 2009.
- (46) 笠原正雄, "新しい秘密分散保管法 KSS(I) と, その生体認証方式への応用," IT2010-120, ISEC2010-124, WBS2010-99, pp.349-352, March 2011.
- (47) M. Kasahara, "Construction of error correcting codes based on multivariate polynomials of degree 1," Memorandum for File at Kasahara Lab, Osaka Gakuin Uni-

versity, Dec. 15, 2008.

- (48) 笠原正雄, “RS 符号を用いた秘密分散保管法に関する考察,”
Memorandum for File at Kasahara Lab, Osaka Gakuin
University, Jan. 2011.

(IT 研究会提案, 平成 23 年 4 月 11 日受付 6 月 2 日最終受付)

笠原正雄 (名誉員: フェロー)

昭 40 阪大大学院博士課程了。阪大助手, 講師, 助
教授を経て昭 62 京都工繊大・教授。平 12 同大学名
誉教授。阪学院大・教授。符号・暗号理論, 情報倫
理, 情報理論の研究に従事。平 5 年度本会小林記念
特別賞, 平 16 年度本会功績賞等各受賞, IEEE ラ
イフフェロー, 著書「情報技術の人間学」など。