

書 評

Error-Correcting Codes

W. Wesley Peterson: M.I.T. Press and John Wiley, New York, 1961. 285 pp. \$ 7.75

誤り訂正および検出符号に関する最初のまとまった本である。1959 年以降、符号理論の研究は再び活潑になったが、本書はその新しい成果を古典的理論とあわせて統一したものである。Peterson 自身符号理論の分野で多くの業績をあげている研究者であり、本書の相当部分（とくに 6～10 章）はその内容あるいは方法において全く新しく独自のものである。1～10 章は著者の M.I.T. における講義ノート（1960）に基づいている。もともと特殊な問題に関するものであるが、例題や練習問題が多くあげられており、この方面に興味をもつ一般の読者にも近づきやすいように配慮されている。

主に取扱われているのは、対称な誤りに対するブロック符号であり、代数学の諸概念を利用して、統一的に理論が展開されている。2 章と 6 章で本書を読むのに直接必要な程度に、群、環、体、ベクトル空間、行列イデアル、剰余類、多項式環、有限体などについて要領よく説明されている。1～5 章は古典理論をまとめたもので、符号理論についてざっと知りたい読者はそこだけ読めばよい。付録に各節を読むのにあらかじめ読んでおくべき節の表がのっているので、興味のある部分だけをひろい読みする場合に便利である。

まず 1 章では、通話路、2 元対称通話路、ブロック符号ハミング距離などの基礎概念が説明されている。第 3 章では群符号を p^m 元 (p : 素数) の場合も含めて一般化した線形符号について、その定義、生成行列、パリティ検査行列、等価な符号の定義などが説明されている。5.7 節を除く 4～11 章はすべて線形符号に関するものである。4 章に符号が誤りを犯す確率の上・下限式、符号のもち得る訂正能力の上・下限式の主要なものがまとめられている。5 章では Hamming 符号、Golay 符号、計算機などを使って求められた独立な誤りに対する最適符号、Reed-Muller 符号、MacDonald 符号、くり返し符号 (iterated code) など主要な線形符号が説明されている。また load sharing matrix switch の設計などに利用されている Hadamard 行列に由来する符号も述べられている。これは本書が取扱っている線形でないブロック符号の唯一の例である（なお p. 81 の上から 2～3 行 “except 116 and 156” は “except 116, 156 and 188” とすべきである。A.L. Duquette, Trans. IRE, IT-8, p. 268）。

6 章以下は主として 1959 年以降の新しい結果に関するものである。7 章では 8～12 章で取扱われている巡回符号、擬巡回符号、回帰符号の符号器、復号器の主要部分をなす線形な逐次時限回路がくわしく説明されている。8 章には巡回符号の一般的性質について著者独自の理論が展開されている。簡単な符号化法、巡回符号としての Hamming 符号、擬巡回符号、短縮された巡回符号などが説明されている（なお, p. 147, 4～16 行に適切でない記述がある。B. Elspas, Trans. IRE, EC-11, p. 102）。

9 章は現在知られている符号のなかでもっとも広範囲な t 重誤り訂正符号である Bose-Chaudhuri 符号を取扱っている。定義と誤り訂正能力、符号例、著者による代数的な復号法などが解説されている（p. 181 の誤りと消失 (erasure) が混合した場合の訂正問題に関する部分に若干の誤りがある (Elspas)）。10 章は密集した誤りを訂正する巡回符号、擬巡回符号に関するものであり、Fire 符号、簡単な復号法などが説明されている。8～10 章では一貫して多項式表現が使われ、符号器、復号器も多項式の掛算または割算回路として説明されているから、わかりやすく本書の特色となっている。

11 章には Meggitt の方法, step by step decoding, Reed の方法などの復号法が紹介されている。12 章には、線形符号の一種の拡張である回帰符号 (recurrent code) について Hagelberger の符号を中心にした解説がのっている。

13 章は 1～12 章とことなり演算回路の誤りを訂正または検出する問題に関するごく短い解説である。加算回路の誤りを訂正または検出する Garner-Diamond-Brown 符号はその基本的な考えにおいて擬巡回符号と極めて類似していることなどが示されている（なお p. 239 の定理 13.3 の (13.5) 式は $M_2(A, 3) =$

$$\left\lfloor \frac{(\pm 2)^{\frac{4-1}{2}} + 1}{A} \right\rfloor \text{ の間違いと思われる}.$$

付録には、2 項係数を含んだ式の評価式、エントロピー関数とその微係数の数値表、GF(2) の上の既約多項式の広範囲にわたる表などがある。また 1960 年までの文献リストもなっている。

誤植はかなりあるが（たとえば, p. 183 の Fire 符号の例, $g(x) = (x^7 + x^2 + 1)(x^{16} + 1)$ は $g(x) = (x^7 + x + 1)(x^{16} + 1)$ の間違いと思われる）、その大部分は少し注意すれば容易にわかる。

符号理論を勉強または利用しようとする人にとって本書は貴重な存在である。（嵩 忠雄）