リード マラー符号の重み分布式および最適な修正ハミング符号に関する研究

山村三朗

報告番号・甲第　号

論　文　目　録

大阪大学

報告番号	甲第1846号	氏名	山　村　三　朗

主論文

題名　リード　マラー符号の重み分布式　および
最適な修正ハミング符号に関する研究

参考論文

題名　Reed-Muller符号の重み分布について
電子通信学会インホメーション理論研究会資料
昭和45年4月28日
嵩忠雄他1名と共著

題名　Reed-Muller符号の重み分布構造
電子通信学会インホメーション理論研究会資料
昭和47年1月19日
嵩忠雄他1名と共著

題名　Reed-Muller符号の重み分布公式（$2d \leq w < 2.5d$）
電子通信学会オートマトンと言語研究会資料
昭和48年1月22日
嵩忠雄他1名と共著

題名　On the Weight Enumeration of Weights less than 2.5d of Reed-Muller Codes
（リードマラー符号の重み2.5d未満の重みの数え上げについて）
阪大・基礎工・報告
昭和49年6月
嵩忠雄他1名と共著

題名 リードマラー符号の重み分布式の導出 —$2d \leq w < 2.5d$—
電子通信学会論文誌 A （投稿中）
原稿 30枚
嵩忠雄 他1名と共著

題名 On the Weight Enumeration of Weights less than 2.5d of Reed-Muller Codes
（リードマラー符号の重み2.5d未満の重みの数え上げについて）
Information and Control （to appear）
原稿 53枚
嵩忠雄 他1名と共著

題名 最適な修正ハミング符号について
電子通信学会論文誌 A
原稿 24枚
昭和50年6月掲載の予定
嵩忠雄と共著

リード マラー符号の重み分布式 および
最適な修正ハミング符号に関する研究

1975年 2月

山 村 三 朗

内　容　梗　概

本論文は、筆者が大阪大学大学院基礎工学研究科（物理系専攻）に在学中当研究室において行った符号理論に関する研究のうち、リード　マラー符号の重み分布式に関する研究を第１編６章に、最適な修正ハミング符号に関する研究を第２編７章にまとめたものである。

緒論および各編第１章は、本研究の意義、本分野における研究の歴史、本研究により得られた結果について概説している。

各編第２章では諸定義といくつかの既知の性質をまとめてあり、また各編の最後の章と結論は各編で得た諸結果と今後の問題点がまとめられている。

第１編第３章は、$GF(2)$ の上の m 変数で r 次以下の多項式の集合に含まれる重み $2^{m-r+1}+2^{m-r-1}$ 未満の多項式を特性づけて、ある制限のもとに互いにアフィン等価でない各アフィン同値類の代表多項式を求めている。

第１編第４章は、第３章で求めた各代表多項式に対し、これとアフィン等価な多項式の数を数え上げている。

第１編第５章では従来の研究で既知となった結果と本研究で求められた結果により、符号長256で次数３および４次のリード　マラー符号のすべての重み分布を求めている。そしてこの重み分布と前章の結果および既知の諸結果から、任意の次数で重み $2d$ 以上 $2.5d$ 未満（d は符号の最小重み）の重み分布式を導出している。

第２編第３章では、拡大ハミング符号から適当なベクトル成分を除去して修正ハミング符号を構成する場合に、誤って復号する確率が最小という意味で最適な符号を探索するため、除去するベクトル成分を組織的に能率良く決定する方法について述べられている。

第２編第４章は、最適性の判定に重み４の符号語数を求める必要性から、与えられた修正ハミング符号よりその符号語数を能率良く求める方法を与えている。

第２編第５章は実際に使用された符号探索法についてその要点を説明している。

第２編第６章には、本論文で求められた最適あるいはすぐれた修正ハミング符号を示し、これらの符号と他の構成法により得られた符号との比較を行っている。

リード　マラー符号の重み分布式および最適な修正ハミング符号に関する研究

目　　次

緒　　論

本論文は符号理論における２つの問題としてリードマラー符号の重み構造に関する問題および最適な修正ハミング符号を探索する問題を扱っている。これら両者は互いに関連する部分が少なくない。

第１編では、リード　マラー符号の重み分布式に関する研究が発表論文（１）～（８）を中心にまとめられている。

符号理論において、符号の重み構造の研究はそれが正確な復号の誤り確率を与えることなどの理由から関心を持たれている分野の一つである。リード　マラー符号は、1954年 Muller と Reed により導入された線形群符号である。この符号の特徴は、i）符号化および復号化が比較的容易であること，ii）冗長度が可変で多重誤りも訂正可能であることなどがあり、理論的に興味ある点としてiii）各符号語がGF(2)の上の各多項式に１対１に対応していることである。この多項式に対応するという性質を利用して、リード　マラー符号の重み構造に関するいくつかの研究が1960年代後半より続けられていた。リード　マラー符号の重み構造の研究は、この符号自体の知識を与えるのみならず、関連する符号の重み構造の手がかりも与えることが期待される。実際過去のBCH符号の重み構造に関するいくつかの結果は、リード　マラー符号との関連で示されている。現在までに、リード　マラー符号の重み構造に関しては、符号長128以下のすべての重み分布と重み$2d$未満（dは最小重み）の重み分布式とそのほかいくらかの性質が知られている。

本論文では、重み分布式の拡張として、任意の次数で重み$2.5d$未満の重み分布式を導出している。GF(2)

の上の多項式に対して可逆アフィン変換を導入し、多項式の集合をアフィン同値類に分割する。そして各同値類に対し一つの代表多項式を決める。多項式をその性質で適当に分類することにより、ある制限を持つ同値類の代表多項式を求めて、その同値類の元の数を数え上げることにより、重み分布式が導出できる。しかし、重み2.5d未満全体の重み分布式の導出に必要なすべての代表多項式を調べることは必ずしも容易でないので、一部の重み分布式の結果から符号長256以下のすべての重み分布を求め、逆にある種の同値類の元の数を求めておく。これと必要な代表多項式の数え上げの結果を併用することにより、重み分布式などの新しい結果が得られた。

第2編には、最適な修正ハミング符号の探索に関する研究が発表論文(9)をもとに述べられている。

近年、計算機組織などが複雑になりかつ高信頼性が要求されるにつれて、誤り訂正符号の導入が見られるようになった。一重誤り訂正，二重誤り検出可能な符号の一つに拡大ハミング符号がある。計算機の記憶装置などにこの符号を適用する場合、そのシステムに応じた情報点数を持つように符号を短縮化する。短縮化符号は元の符号からどの成分を除くかにより、復号化の手続きの複雑さや誤り確率などが異なる。適当な意味で良い符号を見つけることは符号理論における重要な問題である。拡大ハミング符号を短縮化して得られる修正ハミング符号に関しては、復号化に要する全物の費用最小の意味で最適な符号を求める研究がある。

本論文ではこれと異なり、受信した符号語を誤って復号する確率を最小にする意味で最適な符号を探索する方法を考察している。本論文で示されたアルゴリズムにより、実際に計算機を用いて探索し、いくつかの符号長に

ついて最適あるいはすぐれた修正ハミング符号が示されている．さらにこれらの符号を評価する目的で，他のいくつかの構成法による修正ハミング符号との比較を行っている．具体的な結果については第2編第1章などに示されているので，ここでは言及しない．

なお各編では，式番号，定理などの番号および参考文献はそれぞれ独立して記載されている．

関連発表論文

(1) 嵩，都倉，安積
"Reed-Muller符号の重み分布について"，電子通信学会インホメーション理論研究会資料（昭和45年4月）．

(2) 嵩，都倉，安積
"Reed-Muller符号の重み分布構造"，電子通信学会インホメーション理論研究会資料（昭和47年1月）．

(3) 嵩，都倉，安積
"Reed-Muller符号の重み分布公式（$2d \leq w < 2.5d$）"，電子通信学会オートマトンと言語研究会資料（昭和48年1月）．

(4) T. Kasami, N. Tokura and S. Azumi
"Weight Enumerator Formulas of Reed-Muller Codes for $2d \leq w < 2.5d$", Proc. of the 3rd International Symposium on Information Theory, Tallinn, USSR (June 1973).

(5) T. Kasami, N. Tokura and S. Azumi
"On the Weight Enumeration of Weights less than $2.5d_{min}$ of Reed-Muller Codes", IEEE International Symposium on Information Theory, Ashkelon, ISRAEL (June 1973).

(6) T. Kasami, N. Tokura and S. Azumi
"On the Weight Enumeration of Weights less than $2.5d$ of Reed-Muller Codes", Rept. of Faculty of Eng. Sci., Osaka Univ. (June 1974).

(7) 安積，嵩，都倉
"リード マラー符号の重み分布式の導出 — $2d \leq w < 2.5d$ —"，電子通信学会論文誌A（投稿中）

(8) T. Kasami, N. Tokura and S. Azumi
"On the Weight Enumeration of Weights less than $2.5d$ of Reed-Muller Codes"，
Information and Control (to appear).

(9) 安積，嵩
"最適な修正ハミング符号について"，電子通信学会論文誌A（採録決定）.

第1編　リード マラー符号の重み分布式

第1章　序言

符号の重み構造に関する問題は、符号理論における興味ある問題の一つである。符号の重み分布により復号における正確な誤り確率を知ることができる。近年になって、リード　マラー符号[1],[2]（以下、RM符号という）の重み構造がしだいに解明され始めている。Berlekamp－Sloaneは2次のRM符号の重み分布式を導びいた[3]。最小重みをdとしたとき、2d未満の重みについては、Kasami－Tokuraが任意の次数の重み分布式を導出し、重み分布式の結果を拡張した[4]。この結果を用いて符号長128で3次のRM符号の重み分布がSuginoらにより求められている[5]。本論文はRM符号の重み2d，次数3次の符号語数を導びき、符号長が256の3次および双対符号である4次のRM符号の重み分布を見いだした[6],[7]。この結果は、同じ頃Sarwate－Berlekampによっても独立に求められた[8],[9]。またvan Tilborgも文献(6)の結果を追認し、本稿と同じ重み分布を得ている[10]。さらにこれまでの結果の拡張として、任意の次数で重み2.5d未満のRM符号の符号語について特性づけを行い，アフィン同値類の代表多項式を決定し、各代表多項式の同値類の元の数を数え上げた。これと既知の重み分布などから、任意の次数で重み2d以上2.5d未満の重み分布式を導出した[11]~[14]。代表多項式，重み分布式，符号長256の3次および4次の重み分布などを表に示している。

第2章　準備

符号長2^m，次数rのRM符号を$RM(2^m, r)$とかく．このとき情報点数kは

$$k = \sum_{i=0}^{r} \binom{2^m}{i}$$

である*．また重み$w = 2^{m-r}$は最小重みで，これをdと表わす．$1 \leq r \leq m$に対し，m変数でr次以下のGF(2)の上の多項式の集合をP_rとし，$f(x_1, \cdots, x_m) \in P_r$に対して，$f(a_1, \cdots, a_m) = 1$となるようなGF(2)の上の$m$次元ベクトル$(a_1, \cdots, a_m)$の個数を$f$の重みといい，$|f|_m$とかく．このとき，RM符号の定義(1)から，$RM(2^m, r)$の各符号語は$P_r$の各多項式に1対1に対応し，符号語の重みは多項式の重みに等しいので，RM符号の符号語の重み分布の代りに多項式の重み分布を考えることができる．m個の一次式

$$y_i = \sum_{j=1}^{m} a_{ij} x_j + a_{i0}, \quad a_{ij}, a_{i0} \in GF(2) \quad ^{**}$$

$$1 \leq i \leq m \qquad (1)$$

の係数行列$[a_{ij}]$が正則であれば，これらの一次式による変換は可逆アフィン変換（以下，A変換という）である．多項式fがA変換で多項式gに変換できるとき，fとgはA等価であるといい，これを$f \approx g$と記す．もし$f \approx g$ならば，$|f|_m = |g|_m$である．多項式fを不変に保つA変換で，独立な一次式を加え込む操作をR変換という．たとえば，$f = x_1 x_2$に関して$x_2 \to x_1 + x_2 + 1$という変換はfを不変に保つR変換である．また2次の

---

*　通常，符号は符号長と情報点数で表現するが，ここでは便宜上kのかわりにrを使う．

**　＋はGF(2)の上の加算つまり排他的論理和である．

多項式

$$x_1 x_2 + x_3 x_4 + \cdots + x_{2s-1} x_{2s}$$

を不変に保つA変換

$$x_{2i-1} + x_{2j-1} \to x_{2i-1},\quad x_{2i} + x_{2j} \to x_{2j} \quad (i \neq j)$$

をT変換という。A等価性により、P_r はアフィン同値類に分割され、各同値類に対し、最少個の変数をもつ多項式の一つを代表多項式とする。f を含むアフィン同値類の代表多項式の変数の個数を $\mu(f)$ とする。n 個の一次式 $x_1, \cdots, x_n$ に対し、このうちで一次独立な個数を $\#(x_1, \cdots, x_n)$ と表わす。$f \in P_r$ の中の独立な n 個の一次式 $u_1, \cdots, u_n$ を0にしたとき、$f = 0$ になれば、$f \in P_{r,n}$ とかく。たとえば、$f \in P_{r,2}$ の必要十分条件は

$f = xg + yh + xyk$, $x, y \in P_1$,
$g, h \in P_{r-1}$, $k \in P_{r-2}$ かつ g, h, k は x, y に独立

になることである。$f, g \in P_r$ で $f - g \in P_{r-1}$ つまり f, g の最高次の項が等しいとき、$f \sim g$ とかく。

次に、今までに知られている主な性質で、以後の議論に必要となるものをあげる[3],[4],[15]。

〔補題1〕 f ($\neq 0$) が次の様に2通りに表されたとする。

$$f = x_1 \cdots x_i\, g(x_{i+1}, \cdots, x_m) = y_1 \cdots y_j\, h(y_{j+1}, \cdots, y_m)$$

ただし、$\#(x_1, \cdots, x_m) = \#(y_1, \cdots, y_m) = m$ で、$y_1, \cdots, y_m$ は $x_1, \cdots, x_m$ の線形和とし、g と h は一次因数を持たないとする。このとき

$i = j$ かつ $x_1 \cdots x_i = y_1 \cdots y_j$.

［補題２］　$r \geq 3$ かつ

$$x_1 \cdots x_r + x_{r+1} \cdots x_{2r} = y_1 \cdots y_r + y_{r+1} \cdots y_{2r}$$

ただし、$\#(x_1, \cdots, x_{2r}) = \#(y_1, \cdots, y_{2r}) = 2r$.

このとき

$x_1 \cdots x_r = y_1 \cdots y_r$（または $y_{r+1} \cdots y_{2r}$），

$x_{r+1} \cdots x_{2r} = y_{r+1} \cdots y_{2r}$（または $y_1 \cdots y_r$）.

［補題３］

1）　もし $f \in P_2$ かつ $0 < |f|_m < 2^m$ ならば、$|f|_m$ は次の形をとる.

$$2^{m-1} + \varepsilon 2^{m-1-\ell}$$

ただし、$1 \leq \ell \leq m/2$ で、ε は -1，0，1 のいずれかである.

1.1）　$|f|_m = 2^{m-1} - 2^{m-1-\ell}$（または $2^{m-1} + 2^{m-1-\ell}$）となる必要十分条件は

$$f \approx x_1 x_2 + \cdots + x_{2\ell-1} x_{2\ell}$$

（または　$x_1 x_2 + \cdots + x_{2\ell-1} x_{2\ell} + 1$）

となることである. ただし、$x_1, \cdots, x_{2\ell}$ はどれも互いに独立な一次式である.（以下同様である.）

1.2）　$|f|_m = 2^{m-1}$ となる必要十分条件は

$$f \approx x_1 x_2 + \cdots + x_{2\ell-1} x_{2\ell} + x_{2\ell+1}$$

となることである. ただし、$0 \leq \ell \leq (m-1)/2$.

2）　$f \in P_r$ で $0 < |f|_m < 2^{m-r+1}$ とする. このとき、$|f|_m$ は

$$2^{m-r+1} - 2^{m-r-\ell},$$

$$0 \leq \ell \leq \max(m-r, (m-r+2)/2)$$

である.

2.1）　$|f|_m = 2^{m-r}$ の必要十分条件は

$$f \approx x_1 \cdots x_r$$

となることである.

2.2）　$|f|_m = 2^{m-r+1} - 2^{m-r-\ell}$ の必要十分条件は

$$f \approx x_1 \cdots x_{r-\ell} \left(x_{r-\ell+1} \cdots x_r + x_{r+1} \cdots x_{r+\ell} \right)$$
$$(m \geq r + \ell)$$

または

$$f \approx x_1 \cdots x_{r-2} \left(x_{r-1} x_r + \cdots + x_{r+2\ell-3} x_{r+2\ell-2} \right)$$
$$(m \geq r + 2\ell - 2)$$

となることである.

第3章　多項式の特性づけと代表多項式

代表多項式を求めるために、P_r の多項式の特性づけを行う。

［定理1］　$f \in P_r$ かつ $|f|_m < 2^{m-r+1} + 2^{m-r-1}$ とする。

1）　もし $r \geq 4$ ならば、$f \in P_{r,2}$ である。

2）　もし $r = 3$ ならば、$f \in P_{3,2}$ または

$$f \approx x_1 x_2 x_3 + x_4 x_5 x_6 + x_7 g, \quad g \in P_2$$

ただし、$\#(x_1, \cdots, x_7) = 7$ で g は x_7 に独立。

さらに、もし $\mu(f) \geq 9$ ならば

$$f \approx x_1 x_2 x_3 + x_4 x_5 x_6 + x_7 (x_8 x_9 + a x_1 x_4), \quad a \in GF(2).$$

3）　もし $r = 3$ かつ $|f|_m < 2^{m-2} + 2^{m-5}$ ならば、$f \in P_{3,2}$ である。

この証明は長くなるので、別稿（20）にゆずる。

重み $2d \leq |f|_m < 2.5d$ の範囲で $P_r - P_{r,1}$ の多項式 f のアフィン同値類による代表多項式を求める場合には、定理1により、未知の $f \in P_{r,2}$ の多項式を考えれば十分である。f は次式の様に展開できる。

$$f = xg + yh + xyk \qquad (2)$$

ただし、$g, h \in P_{r-1}$, $k \in P_{r-2}$, $x, y \in P_1$ で、g, h, k は x, y に独立である。このとき

$$|f|_m = |g|_{m-2} + |h|_{m-2} + |g+h+k|_{m-2} \qquad (3)$$

である。ここで必要なら、$x \to x+1$, $y \to y+1$ のA変換を考えることにより、一般性を失うことなく

$$|g|_{m-2} \leq |h|_{m-2} \leq |g+h+k|_{m-2} \qquad (4)$$

と仮定すると、補題3により、次の場合のみになる。

(i) $|g|_{m-2} = 2^{m-r-1}$, $|h|_{m-2} = 2^{m-r} - 2^{m-r-s}$,
$|g+h+k|_{m-2} < 2^{m-r} + 2^{m-r-s}$ $(s \geq 2)$,

(ii) $|g|_{m-2} = |h|_{m-2} = 2^{m-r-1} + 2^{m-r-2}$,
$|g+h+k|_{m-2} < 2^{m-r}$.

g とんの重みはその最小重みの2倍より小さいので、補題3からこれらの多項式の形が決定する。また $|g+h+k|_{m-2}$ の制限により、g とんの間に密接な関係ができる。一方後述のように、$\mu(f) < 9$ かつ $|f|_m > 2^{m-r+1}$ であるような多項式は求める必要がない。これらの条件の下で代表多項式を求めることができるが、ここでは証明を省略し、結果のみを次に示す*。

[定理2] $f \in P_r - P_{r,1}$ $(r \geq 3)$, $2^{m-r+1} \leq |f|_m < 2^{m-r+1} + 2^{m-r-1}$ かつ、もし $r \geq 4$ または $|f|_m \geq 2^{m-r+1} + 2^{m-r-2}$ ならば $\mu(f) \geq 9$ とする。このとき、f は表1に示す代表多項式の一つとA等価である。

(表1は次頁に示す。)

[系1] $f \in P_3 - P_{3,1}$ とする。

1) もし $|f|_m = 2^{m-2}$ ならば、f は次の多項式のいずれか一つとA等価である。

$x_1 x_2 x_3 + (x_1 + 1) x_4 x_5$
$x_1 x_2 x_3 + x_4 (x_2 x_5 + x_3 x_6)$
$x_1 x_2 x_3 + x_4 (x_3 x_5 + x_6 x_7)$

2) もし $2^{m-2} < |f|_m < 2^{m-2} + 2^{m-5}$ ならば
$|f|_m = 2^{m-2} + 2^{m-6}$ かつ
$f \approx x_1 x_2 x_3 + x_4 (x_5 x_6 + x_7 x_8)$
である。

次に表1の各多項式がそれぞれのアフィン同値類において最少個の変数をもつ多項式であることを確める。

* 証明は文献(20)に詳しく述べられている。

表1. 代表多項式とその重み

重み	(No.) 代表多項式
$2^{m-r+1}+2^{m-r-2}+2^{m-r-4}$ (10.0101d)	(1) $X_1X_2X_3+X_4X_5X_6+X_7X_8X_9$
$2^{m-r+1}+2^{m-r-2}+2^{m-r-3}$ (10.011d)	(2) $X_1(X_2X_3+X_4X_5)+X_6(X_7X_8+X_9X_2)$
$2^{m-r+1}+2^{m-r-2}+2^{m-r-3}+2^{m-r-4}$ (10.0111d)	(3) $X_1X_2X_3+X_4X_5X_6+X_7(X_8X_9+X_1X_4)$ (4) $X_1(X_2X_3+X_4X_5)+X_6(X_7X_8+X_9X_{10})$
$2^{m-r+1}+2^{m-r-1}-2^{m-r-s+3}$ (10.01$\underbrace{\cdots}_{s-2}$1d)	(5) $X_1X_2X_3+X_4(X_2X_5+X_3X_6+X_7X_8+\cdots+X_{2s+1}X_{2s+2})$ $(s\geq 4)$ (6) $X_1X_2X_3+X_4(X_3X_5+X_6X_7+\cdots+X_{2s+2}X_{2s+3})$ $(s\geq 3)$
$2^{m-r+1}+2^{m-r-1}-2^{m-r-s+1}+2^{m-r-s-1}$ (10.01$\underbrace{\cdots}_{s-2}$101d)	(7) $X_1X_2X_3+X_4(X_5X_6+\cdots+X_{2s+3}X_{2s+4})$ $(s\geq 3)$
$2^{m-r+1}+2^{m-r-1}-2^{m-r-s}$ (10.01$\underbrace{\cdots}_{s-1}$1d)	(8) $X_1X_2X_3+X_4((X_3+1)X_5+X_6X_7+\cdots+X_{2s+2}X_{2s+3})$ $(s\geq 3)$ (9) $X_1X_2X_3+X_4(X_1X_5+X_2X_6+X_3X_7+X_8X_9+\cdots+X_{2s+2}X_{2s+3})$ $(s\geq 3)$
$2^{m-r+1}+2^{m-r-1}-2^{m-r-s-1}$ (10.01$\underbrace{\cdots}_{s}$1d)	(10) $X_1X_2X_3+X_4(X_5X_6+\cdots+X_{2s+3}X_{2s+4}+X_1)$ $(s\geq 3)$
2^{m-r+1} (10d)	(11) $X_1X_2\cdots X_r+(X_1+1)X_{r+1}\cdots X_{2r-1}$
$2^{m-r+1}+2^{m-r-2}+2^{m-r-3}$ (10.011d)	(12) $X_1X_2X_3X_4+X_5(X_3X_6X_7+X_4X_8X_9)$ (13) $X_1X_2X_3X_4+X_5X_6(X_3X_4+(X_2+1)X_7+X_8X_9)$ (14) $X_1X_2X_3X_4+X_5(X_3X_6X_7+(X_4+X_7)X_8X_9)$ (15) $X_1X_2X_3X_4X_5+X_6X_7(X_3X_4X_8+X_2(X_5+X_8)X_9)$
$2^{m-r+1}+2^{m-r-2}+2^{m-r-3}+2^{m-r-4}$ (10.0111d)	(16) $X_1X_2X_3X_4+X_5(X_4X_6X_7+X_8X_9X_{10})$ (17) $X_1X_2X_3X_4+X_5X_6(X_3X_4+X_7X_8+X_9X_{10})$ (18) $X_1X_2X_3X_4X_5+X_6X_7(X_3X_4X_8+(X_5+X_8)X_9X_{10})$
$2^{m-r+1}+2^{m-r-1}-2^{m-2r+3}$ (10.01$\underbrace{\cdots}_{r-4}$1d)	(19) $X_1\cdots X_r+X_{r+1}\cdots X_{2r-2}(X_{r-3}X_{r-2}+X_{r-1}(X_r+1))$ $(r\geq 6)$ (20) $X_1\cdots X_r+X_{r+1}\cdots X_{2r-2}(X_{2r-1}(X_r+1)+X_{r-2}X_{r-1})$ $(r\geq 5)$

表1 つづき

$2^{m-r+1}+2^{m-r-1}$ -2^{m-2r+2} $(10.01\underbrace{\cdots}_{r-3}1d)$	(21) $X_1\cdots X_r+X_{r+1}\cdots X_{2r-2}(X_{2r-1}X_{r-2}+X_{r-1}X_r)$ $(r\geq 5)$ (22) $X_1\cdots X_r+X_{r+1}\cdots X_{2r-2}(X_{2r-1}X_{r-1}+X_{2r}X_r)$ $(r\geq 5)$ (23) $X_1\cdots X_r+X_{r+1}\cdots X_{2r-2}(X_{2r-1}X_{2r}+X_{2r+1}X_r)$
$2^{m-r+1}+2^{m-r-1}$ -2^{m-2r+1} $(10.01\underbrace{\cdots}_{r-2}1d)$	(24) $X_1\cdots X_r+X_{r+1}\cdots X_{2r-2}(X_{2r-1}X_{2r}+X_{r-1}(X_r+1))$ $(r\geq 5)$ (25) $X_1\cdots X_r+X_{r+1}\cdots X_{2r-2}(X_{2r-1}X_{2r}+X_{2r+1}(X_r+1))$
$2^{m-r+1}+2^{m-r-1}$ $-2^{m-2r+3}+2^{m-2r+1}$ $(10.01\underbrace{\cdots}_{r-4}101d)$	(26) $X_1\cdots X_r+X_{r+1}\cdots X_{2r-2}(X_{2r-1}X_{2r}+X_{r-1}X_r)$ $(r\geq 5)$
$2^{m-r+1}+2^{m-r-1}$ $-2^{m-2r+2}+2^{m-2r}$ $(10.01\underbrace{\cdots}_{r-3}101d)$	(27) $X_1\cdots X_r+X_{r+1}\cdots X_{2r-2}(X_{2r-1}X_{2r}+X_{2r+1}X_{2r+2})$

ここで、$X_1, X_2, \cdots$ はたがいに独立な一次式である。
重みの欄のカッコ内は、重みの2進数表現である。

表1の各代表多項式fに対し、その多項式の変数の個数を$\mu'(f)$とする．もし$\mu'(f)>\mu(f)$ならば，$f_{x_i=a}$の次数がfの次数に等しく、かつ

$$|f_{x_i=a}|_m = |f|_m, \quad a \in GF(2)$$

となる変数x_iが存在する．多項式 No.1, No.2, No.3, No.4, No.11 については、そのような変数x_iが存在しないことは明らかである．それ以外の多項式は

$$f = x_1 \cdots x_r + x_{r+1} \cdots x_{2r-l}(z_1 z_2 + \cdots + z_{2s-1} z_{2s} + c\, z_{2s+1}),$$
$$c \in GF(2), \quad s \geq 2, \quad l = 2$$

または

$$f = x_1 \cdots x_r + x_{r+1} \cdots x_{2r-l}(z_1 z_2 z_3 + z_4 z_5 z_6), \quad l = 3$$

という形をしている．そのとき、$r < i \leq 2r - l$に対して

$$|f_{x_i=0}|_m = |x_1 \cdots x_r|_m < |f|_m$$

となる．また$1 \leq i \leq r$に対して

$$|f_{x_i=0}|_m \leq 2^{m-r+1} < |f|_m$$

である．$i > 2r - l$に対しては、$f_{x_i=a}$はより小さいSを持つか、あるいは一般性を失うことなく

$$f_{x_i=0} = x_1 \cdots x_r + x_{r+1} \cdots x_{2r-3}(z_1 z_2 z_3)_{x_i=0}$$

となり、$|f_{x_i=0}|_m \neq |f|_m$である．したがって

$$\mu'(f) = \mu(f) \qquad (5)$$

である．

代表多項式を求める場合に、たとえば$f \in P_{r,2}$であれば3つの重み$|g|_{m-2}$, $|h|_{m-2}$, $|g+h+k|_{m-2}$で分類を行っているが、一般にどの一次式の組で展開するかにより重みの組が異なる．これは重みで分類すれば、いくつかの場合分けされた議論の中に互いにA等価な代表多項式が含まれる可能性があることを意味し、これらの多項式

は一つを除きいずれかの他の場合に帰着させれば良い訳である。しかし必ずしも一見してたいにA等価かどうかの判定ができるとは限らないので、求められた代表多項式が互いにA等価でないことを確認する必要がある。この確認については次章で行う。

第4章　多項式の数え上げ

この章では、表1の各代表多項式に対し、これとA等価な多項式の数を数え上げる。m次元ベクトル空間中で、$f \approx g$となる多項式gの数を$N(f)$とし、fを不変に保つA変換の数を$I(f)$とすると、A変換の総数は

$$2^m(2^m-1)(2^m-2)\cdots(2^m-2^{m-1})$$

であるから

$$N(f) = 2^{m(m+1)/2} \prod_{i=0}^{m-1} (2^{m-i}-1) / I(f) \quad (6)$$

である。したがって、$N(f)$の代りに$I(f)$も求めれば良い。そのためには、各代表多項式fに対して

$$\left.\begin{aligned} &f(y_1, y_2, \cdots, y_m) = f(x_1, x_2, \cdots, x_m) \\ &y_i = \sum_{j=1}^{m} a_{ij} x_j + a_{i0}, \quad a_{ij} \in GF(2) \\ &\qquad 1 \le i \le m, \quad 0 \le j \le m \\ &\#(y_1, y_2, \cdots, y_m) = \#(x_1, x_2, \cdots, x_m) = m \end{aligned}\right\} \quad (7)$$

を満たす係数行列$[a_{ij}]$の数を数え上げれば良い。（$[a_{ij}]$が決まれば、定数項a_{i0}は一意に決まる。また、$\mu(f) = m$ゆえ上式を満たす係数行列は正則である。）

多項式を重複して数えることのないように、表1の代表多項式のどの2つの組をとってもA等価でないことを保証する必要がある。2つの代表多項式f_1, f_2がA等価であるための必要条件として、1）f_1とf_2の次数が等しいこと、2）$|f_1|_m = |f_2|_m$、3）$\mu(f_1) = \mu(f_2)$、4）$I(f_1) = I(f_2)$が考えられる。そのほか、$f \in P_{r,2}$の多項式については

$f = xg + yh + xyk$, $g, h \in P_{r-1}$, $k \in P_{r-2}$,
g, h, kはx, yに独立

と展開したとき、一般性を失うことなく

$$|f|_m = |g|_{m-2} + |h|_{m-2} + |g+h+k|_{m-2},$$
$$|g|_m \leq |h|_{m-2} \leq |g+h+k|_{m-2}$$

とすることができて、fに対し3個の重みの組

$$W_f = (|g|_{m-2}, |h|_{m-2}, |g+h+k|_{m-2})$$

が定義できる。このとき、5) $W_{f_1} = W_{f_2}$ は $f_1 \approx f_2$ となることの一つの必要条件である。これらの必要条件のうち、条件4)はこれから求めようとするものであり、一般にこの条件を確めることは困難であるが、それ以外の条件1), 2), 3), 4)についての判定は容易である。これらにより判定した結果、表1のNo.8, No.9の組を除いて、すべての組がA等価でないことが判明した。このうち条件4)の判定には計算機(PDP11/20)を使用した。残りの一組についても、後述するようにA等価でないと言える。

次に多項式の数え上げに用いる2つの補題を示す。

[補題4] $r \geq 4$で

$$f = x_1 \cdots x_r + x_{r+1} \cdots x_{2r-\ell}\, p$$
$$= y_1 \cdots y_r + y_{r+1}\, g$$

とし、次の条件が成立すると仮定する。

1) もし$2 < \ell < r$ならば

$$p = z_1 \cdots z_\ell + z_{\ell+1} \cdots z_{2\ell}$$

で、もし$\ell = 2$ならば

$$p = z_1 z_2 + \cdots + z_{2s-1} z_{2s}, \quad s \geq 2.$$

2) gは独立な変数 $y_1, \cdots, y_r, y_{r+2}, \cdots, y_m$ ($m > r$)の$r-1$次の多項式で、$2^{m-r+1} < |g|_m < 2^{m-r+2}$かつ一次因数の数は$r-\ell-1$以上である。

3) $x_1, \cdots, x_{2r-\ell}, z_1, \cdots, z_{2\ell}$ は $y_1, \cdots, y_m$ の線形和であり

$$\#(x_1, \cdots, x_{2r-\ell}) = 2r - \ell,$$

$l > 2$ のとき

$$\#(x_{r+1}, \cdots, x_{2r-l}, z_1, \cdots, z_{2l}) = r + l$$

$l = 2$ のとき

$$\#(x_{r+1}, \cdots, x_{2r-l}, z_1, \cdots, z_{2s}) = r + 2(s-1)$$

ただし、$l > 2$ ならば $l' = l$, それ以外 $l' = s$.

4) もし $l > 3$ かまたは $l = s = 2$ のとき

$$\#(x_1, \cdots, x_{2r-l}, z_1, \cdots, z_l) \geq r + 3,$$

$$\#(x_1, \cdots, x_{2r-l}, z_{l+1}, \cdots, z_{2l}) \geq r + 3$$

かつ $l = 2$ ならば、p に関する任意の T 変換は上の関係を満足する.

5) $\mu(f) \geq 9$.

このとき、次式が成立する.

A) $x_1 \cdots x_r = y_1 \cdots y_r$,

$x_{r+1} \cdots x_{2r-l} p = y_{r+1} q$

または、$x_1 \cdots x_r$ と $x_{r+1} \cdots x_{2r-l}$ p に関する適当な R 変換と添字のつけかえにより

B) $x_1 = z_l = y_{r+1}$,

$x_{r+1} \cdots x_{2r-l} z_{l+1} \cdots z_{2l} = y_1 \cdots y_r$,

$x_1 \cdots x_r + x_{r+1} \cdots x_{2r-l} z_1 \cdots z_l = y_{r+1} q$

ただし、$l = 2$ のときは A) の場合のみである.

[補題5] 次式が成立すると仮定する.

$$f = x_1 x_2 x_3 + x_4 p$$
$$= y_1 y_2 y_3 + y_4 q$$

$$p = z_1 z_2 + \cdots + z_{2s-1} z_{2s} + k z_{2s+1},$$

$$q = u_1 u_2 + \cdots + u_{2t-1} u_{2t} + k' u_{2t+1}$$

ただし、1) $s \geq 3$, 2) $\#(x_4, z_1, \cdots, z_{2s+1}) = 2s + 2$, 3) $\#(x_1, x_2, x_3, x_4, z_{2i-1}, z_{2i}) \geq 5$ $(1 \leq i \leq s)$ かつこれらの関係は p に関する任意の T

変換のもとに保たれる，4) $x_1, \cdots, x_4, z_1, \cdots, z_{2s+1}, u_1, \cdots, u_{2t+1}$ は独立変数 $y_1, \cdots, y_m$ の線形和である．このとき

$$x_4 = y_4,$$
$$x_1 x_2 x_3 = (y_1 + a_1 y_4)(y_2 + a_2 y_4)(y_3 + a_3 y_4),\quad a_1, a_2, a_3 \in GF(2).$$

これらの補題の証明は省略する．（文献[20]参照．）

ここで，代表多項式 No.8，No.9 が A 等価でないことを証明する．もし A 等価であると仮定すると．

$$x_1 x_2 x_3 + x_4((x_3+1)x_5 + x_6 x_7 + \cdots + x_{2s+2} x_{2s+3})$$
$$= y_1 y_2 y_3 + y_4(y_1 y_5 + y_2 y_6 + y_3 y_7 + y_8 y_9 + \cdots + y_{2s+2} y_{2s+3})$$

補題5により．

$$x_1 x_2 x_3 = (y_1 + a_1 y_4)(y_2 + a_2 y_4)(y_3 + a_3 y_4)$$

$x_4 = y_4 = 1$ とおけば

$$\underbrace{(x_3+1)x_5 + x_6 x_7 + \cdots}_{s\text{項}}$$
$$\sim a_1 y_2 y_3 + a_2 y_1 y_3 + a_3 y_1 y_2 + y_1 y_5 + y_2 y_6 + y_3 y_7 + \cdots$$
$$= \underbrace{y_1(y_5 + a_2 y_3) + y_2(y_6 + a_3 y_1) + y_3(y_7 + a_1 y_2)}_{s+1\text{項}} + y_8 y_9 + \cdots$$

これは項数が異なり矛盾である．よって，No.8 と No.9 は A 等価ではない．

表1の各代表多項式 f について（7）式を考えて，補題4，5，1，2 などを利用し，手計算および機械計算（PDP 11/20）により，各 $E(f)$ したがい $N(f)$ が求められた．

I（ナ）の数え上げに用いられた機械計算のためのプログラムについて若干の説明を行う。入力は、多項式（各変数はその添字で表現する。）および各a_{ij}（$1 \leq i \leq m$, $0 \leq j \leq m$）に対し、定数0，1または可変であることの指定である。可変とした係数の個数の増加に伴い計算時間は指数的に増大するので、あまり多くの係数を可変にはできない。適当な時間内に結果を必要とするので実際には高々16個までの係数に対し可変の指定を行った。プログラムは多項式からその真理値表をデータ領域に生成し、それぞれの係数の組によるA変換で変換された変数の組による多項式の値と元の真理値表の値との比較を行い、両者がすべて等しいかどうかの判定をする。必要に応じ不変となる係数の組あるいはその数のみを出力する。ここで注意する必要があるのは、互いに関連して変化するすべての各係数を同時に可変であると指定しなければならないことである。

手計算では、一般にある変数に定数を代入することにする、次数，項数などの関係から変数の依存関係を限定てことにより場合の数を決定する。

以下に数え上げの3つの例を示す。他の場合については文献[20]を参照されたい。全体の結果は表2に示す。なお一部の結果は素因数形で表現されている。

（例1.）　No. 19

$$f(X) = x_1 \cdots x_r + x_{r+1} \cdots x_{2r-2}(x_{r-3}x_{r-2} + x_{r-1}(x_r + 1)) \quad (8)$$

補題4により

$$y_1 \cdots y_r = x_1 \cdots x_r, \quad (8\cdot1)$$

$$y_{r+1} \cdots y_{2r-2}(y_{r-3}y_{r-2} + y_{r-1}(y_r + 1)) = x_{r+1} \cdots x_{2r-2}(x_{r-3}x_{r-2} + x_{r-1}(x_r + 1)). \quad (8\cdot2)$$

補題1により

$$y_{r+1}\cdots y_{2r-2}=x_{r+1}\cdots x_{2r-2}. \qquad (8\cdot3)$$

(8·1), (8·3)により

$$a_{ij}=0 \quad (1\le i\le r,\ r<j\le 2r-2),$$
$$a_{ij}=0 \quad (r<i\le 2r-2,\ 1\le j\le r),$$
$$\begin{vmatrix} a_{11} & \cdots & a_{1r} \\ \vdots & & \vdots \\ a_{r1} & \cdots & a_{rr} \end{vmatrix}=1, \quad \begin{vmatrix} a_{r+1,r+1} & \cdots & a_{r+1,2r-2} \\ \vdots & & \vdots \\ a_{2r-2,r+1} & \cdots & a_{2r-2,2r-1} \end{vmatrix}=1.$$

もし $1\le i\le r$ に対し $x_i=1$ ならば $y_i=1$ $(1\le i\le r)$ となるので、

$$\sum_{j=1}^{r} a_{ij}=1+a_{i0} \quad (1\le i\le r).$$

同様に

$$\sum_{j=r+1}^{2r-2} a_{ij}=1+a_{i0} \quad (r<i\le 2r-2).$$

逆にこれらの条件が満たされておれば、(8·1), (8·3)は成立する. よって、a_{ij} $(r<i\le 2r-2,\ 0\le j\le 2r-2)$ の数は

$$(2^{r-2}-1)(2^{r-2}-2)\cdots(2^{r-2}-2^{r-3}).$$

(8·2)式の右辺の一次因数のすべてに1を代入することにより

$$a_{ij}=0 \quad (r-3\le i\le r,\ 1\le j<r-3) \qquad (8\cdot6)$$

が得られる. よって

$$\begin{vmatrix} a_{11} & \cdots & a_{1,r-4} \\ \vdots & & \vdots \\ a_{r-4,1} & \cdots & a_{r-4,r-4} \end{vmatrix}=1, \quad \begin{vmatrix} a_{r-3,r-3} & \cdots & a_{r-3,r} \\ \vdots & & \vdots \\ a_{r,r-3} & \cdots & a_{r,r} \end{vmatrix}=1.$$

また

$$y_{r-3}y_{r-2}+y_{r-1}(y_r+1)=x_{r-3}x_{r-2}+x_{r-1}(x_r+1).$$

上式を満たす a_{ij} $(r-3\le i\le r,\ 0\le j\le 2r-2)$ の数は

120である．これは機械計算により求められた．a_{ij}（$1 \leq i < r-3$，$0 \leq j \leq 2r-2$）の数は

$$2^{4(r-4)} \prod_{i=0}^{r-5} (2^{r-4} - 2^i)$$

である．したがって

$$I(f) = 2^{4(r-4)} \cdot 120 \cdot \prod_{i=0}^{r-5} (2^{r-4} - 2^i) \prod_{i=0}^{r-3} (2^{r-2} - 2^i)$$

である．ここで係数行列の0でない各部分の場合の数を図1に示す．ただし，a_{i0}は省略する．

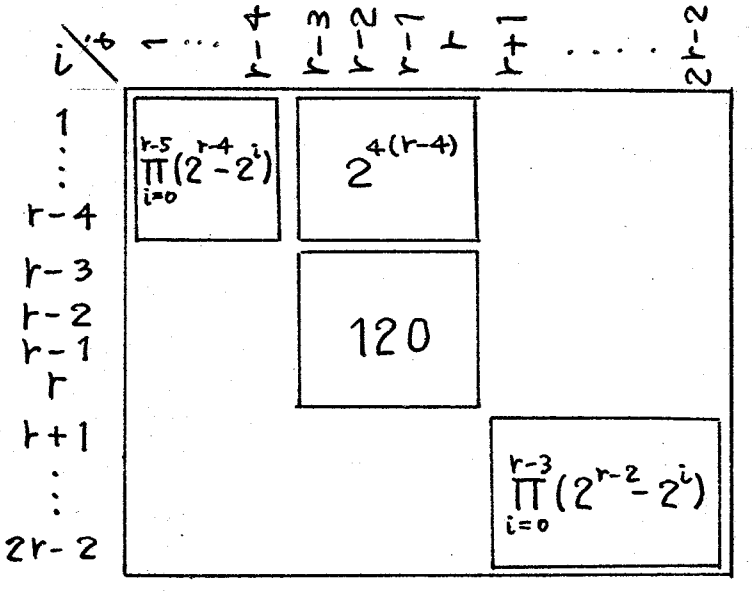


図1．No.19の係数行列の数

（例2．）No.6

$$f(X) = x_1 x_2 x_3 + x_4 (x_3 x_5 + x_6 x_7 + \cdots + x_{2s+2} x_{2s+3}) \quad (9)$$

補題5により

$$y_4 = x_4,$$

$$y_1 y_2 y_3 = (x_1 + b_1 x_4)(x_2 + b_2 x_4)(x_3 + b_3 x_4),$$

$$b_1, b_2, b_3 \in GF(2) \quad (9\cdot1)$$

である．これより

$$(y_3y_5+y_6y_7+\cdots+y_{2s+2}y_{2s+3})_{x_4=1}$$
$$=b_3(x_1x_2+b_1x_2+b_2x_1+b_1b_2)+(b_1x_2+b_1x_1+x_5+b_1b_2)x_3+x_6x_7+\cdots+x_{2s+2}x_{2s+3}. \quad (9\cdot2)$$

両辺の項数の関係から $b_3=0$. また

$$a_{ij}=0 \quad (1\le i\le 3,\ j>4),$$

$$\sum_{j=1}^{3} a_{ij}=1 \quad (1\le i\le 3),$$

$$\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix}=1.$$

$$\therefore\ y_3=1+a_{33}+a_{33}x_3+a_{34}x_4.$$

$(9\cdot1)$式において、$x_1=\overline{b_1}$, $x_2=\overline{b_2}$, $x_3=x_4=1$ とすると、$a_{34}=0$. よって

$$y_3=x_3.$$

$y_i'=(y_i)_{y_3=0,\ y_4=1}$ $(6\le i\le 2s+3)$ とおくと

$$y_6'y_7'+y_8'y_9'+\cdots+y_{2s+2}'y_{2s+3}'$$
$$=x_6x_7+x_8x_9+\cdots+x_{2s+2}x_{2s+3} \quad (9\cdot3)$$

となり、これより

$$a_{ij}=0 \quad (6\le i\le 2s+3,\ j=1,2,5).$$

また

$$(y_{2i}y_{2i+1})_{x_4=1}=y_{2i}'y_{2i+1}'$$
$$+(a_{2i,3}y_{2i+1}'+a_{2i+1,3}y_{2i}'+a_{2i,3}a_{2i+1,3})x_3$$

であるから、$(9\cdot2)$式と$(9\cdot3)$式により

$$(y_5)_{x_3=1,\ x_4=1}=b_2x_1+b_1x_2+b_1b_2+x_5$$
$$+\sum_{i=3}^{s+1}(a_{2i,3}y_{2i+1}'+a_{2i+1,3}y_{2i}'+a_{2i,3}a_{2i+1,3}).$$

a_{i3}, a_{i4} $(5\le i\le 2s+3)$ は任意に選択できるので、a_{ij} $(5\le i\le 2s+3,\ 0\le j\le 2s+3)$ の数は

$$2^{4s-2}B_{s-1}.$$

ただし、B_{s-1} は $s-1$ 項の2次の多項式が A 変換で不変

に保たれる数である。B_{s-1}は次の様に求まる。Sloane-Berlekampの公式により、2次の符号語数

$$N_{m,2,w} = 2^{(s-1)s} \prod_{i=0}^{s-2} (2^{m-2i}-1)(2^{m-2i-1}-1)/(4^{i+1}-1)$$

$$(m = 2s-2,\ w = 2^{m-1} - 2^{m-s})$$

が知られており、m変数のA変換の数$A^{(m)}$は

$$2^m(2^m-1)(2^m-2)\cdots(2^m-2^{m-1})$$

であるから、$y_6 y_7 + \cdots + y_{2s+2} y_{2s+3}$を不変に保つA変換の数は

$$B_{s-1} = A^{(2s-2)} / N_{2s-2,2,2^{2s-3}-2^{s-2}}$$

$$= 2^{(s-1)^2} \prod_{i=0}^{s-2} (4^{i+1}-1)$$

である。またy_1, y_2については

$$\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = 1$$

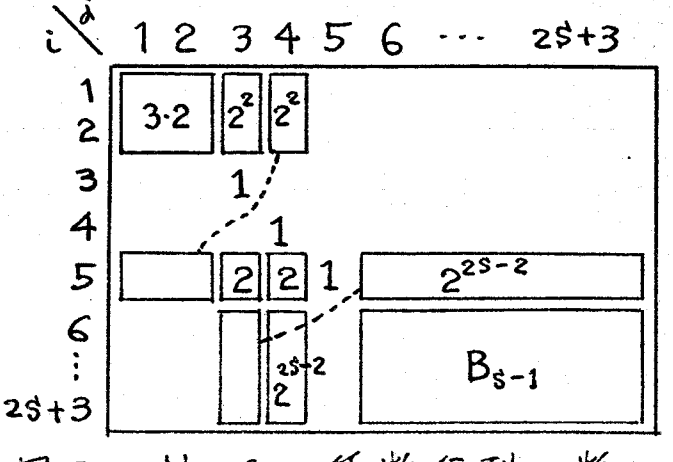
で、b_1, b_2は任意に選択できる。よってa_{ij} ($1 \le i \le 2$, $0 \le j \le 2s+3$)の数は

$$2^4 \cdot (2^2-1)(2^2-2)$$

となり、全体では

$$\Sigma(f) = 2^{4s+3} \cdot 3 \cdot B_{s-1}$$

となる。



図中の破線は互いに関連する部分を示す。

図2. No.6の係数行列の数

（例3）　No. 11

$$f(X) = x_1 x_2 \cdots x_r + (x_1+1)x_{r+1}\cdots x_{2r-1} \quad (10)$$

$y_i' = (y_i)_{x_1=0}$ $(1 \le i \le 2r-1)$ とおくと

$$\#(y_1', y_2', \cdots, y_{2r-1}') = 2r-2,$$

$$y_1' y_2' \cdots y_r' + (y_1'+1) y_{r+1}' \cdots y_{2r-1}' = x_{r+1}\cdots x_{2r-1}.$$

$y_1' = \sum_{j=1} b_j x_j + b_0$ であれば、$y_1, y_2, \cdots, y_{2r-1}$ の一次独立性から上式左辺のいずれかの項は r 次となり矛盾する．よって y_1' は定数である．

$$\therefore y_1 = x_1 + a_{10}.$$

$a_{10} = 0$ とすると、このとき

$$(y_2 y_3 \cdots y_r)_{x_1=1} = x_2 x_3 \cdots x_r,$$

$$(y_{r+1} y_{r+2} \cdots y_{2r-1})_{x_1=0} = x_{r+1} x_{r+2} \cdots x_{2r-1}.$$

したがって

$$a_{ij} = 0 \quad (2 \le i \le r,\ r < j \le 2r-1),$$

$$a_{ij} = 0 \quad (r < i \le 2r-1,\ 2 \le j \le r),$$

$$\sum_{j=2}^{r} a_{ij} = a_{i0} + a_{i1} \quad (2 \le i \le r),$$

$$\sum_{j=r+1}^{2r-1} a_{ij} = a_{i0} \quad (r < i \le 2r-1),$$

$$\begin{vmatrix} a_{22} & \cdots & a_{2r} \\ \vdots & & \vdots \\ a_{r2} & \cdots & a_{rr} \end{vmatrix} = 1, \qquad \begin{vmatrix} a_{r+1,r+1} & \cdots & a_{r+1,2r-1} \\ \vdots & & \vdots \\ a_{2r-1,r+1} & \cdots & a_{2r-1,2r-1} \end{vmatrix} = 1.$$

これらの式を満たす a_{ij} $(2 \le i \le 2r-1)$ の数は

$$2^{2r-2}\left\{\prod_{i=1}^{r-2}(2^{r-1}-2^i)\right\}^2$$

また $a_{10} = 1$ の場合は添字のつけかえで上記の場合に帰着される．よって

$$E(f) = 2^{2r-1}\left\{\prod_{i=1}^{r-2}(2^{r-1}-2^i)\right\}^2$$

である．

表2.　表1の代表多項式のN(f)

重み	(No.)	2	3	5	7	11	17	31	73	127
10.0101d	(1)	35	1	2	-	-	1	1	1	1
10.011d	(2)	29	3	2	3	-	1	1	1	1
	(12)	29	1	2	3	-	1	1	1	1
	(13)	28	2	2	3	-	1	1	1	1
	(14)	29	3	2	3	-	1	1	1	1
	(15)	29	3	2	3	-	1	1	1	1
10.0111d	(3)	35	1	2	3	-	1	1	1	1
	(4)	38	2	-	3	1	1	2	1	1
	(16)	37	3	2	1	1	1	2	1	1
	(17)	36	1	1	3	1	1	2	1	1
	(18)	34	2	2	3	1	1	2	1	1
$10.0\underbrace{1\ldots1}_{s-2}d$	(5)	$2^{s^2+3s+2}\cdot\beta_{2s+2} / 3\cdot\gamma_{s-2}$								
	(6)	$2^{s^2+5s+2}\cdot\beta_{2s+3} / 3\cdot\gamma_{s-1}$								
$10.0\underbrace{1\ldots1}_{s-1}d$	(8)	$2^{s^2+5s+4}\cdot\beta_{2s+3} / 3\cdot\gamma_{s-1}$								
	(9)	$2^{s^2+3s+6}\cdot\beta_{2s+3} / 3\cdot7\cdot\gamma_{s-2}$								
$10.0\underbrace{1\ldots1}_{s}d$	(10)	$2^{s^2+7s+7}\cdot\beta_{2s+4} / 3\cdot\gamma_{s}$								
$10.0\underbrace{1\ldots101}_{s-2}d$	(7)	$2^{s^2+7s+7}\cdot\beta_{2s+4} / 3\cdot7\cdot\gamma_{s}$								
10d	(11)	$2^{r^2-1}\cdot\beta_{2r-1} / \beta_{r-1}^2$								
$10.0\underbrace{1\ldots1}_{r-4}d$	(19)	$2^{r^2+1}\cdot\beta_{2r-2} / 3\cdot5\cdot\beta_{r-4}\cdot\beta_{r-2}$								
	(20)	$2^{r^2+r-2}\cdot\beta_{2r-1} / 3\cdot\beta_{r-3}\cdot\beta_{r-2}$								
$10.0\underbrace{1\ldots1}_{r-3}d$	(21)	$2^{r^2+r}\cdot\beta_{2r-1} / 3\cdot\beta_{r-3}\cdot\beta_{r-2}$								
	(22)	$2^{r^2+2r-2}\cdot\beta_{2r} / \beta_{r-2}^2$								
	(23)	$2^{r^2+3r}\cdot\beta_{2r+1} / 3\cdot\beta_{r-2}\cdot\beta_{r-1}$								
$10.0\underbrace{1\ldots1}_{r-2}d$	(24)	$2^{r^2+2r}\cdot\beta_{2r} / 3\cdot\beta_{r-2}^2$								
	(25)	$2^{r^2+3r}\cdot\beta_{2r+1} / 3\cdot\beta_{r-2}\cdot\beta_{r-1}$								
$10.0\underbrace{1\ldots101}_{r-4}d$	(26)	$2^{r^2+2r}\cdot\beta_{2r} / 3^2\cdot\beta_{r-2}^2$								
$10.0\underbrace{1\ldots101}_{r-3}d$	(27)	$2^{r^2+4r+4}\cdot\beta_{2r+2} / 3^2\cdot5\cdot\beta_{r-2}\cdot\beta_{r}$								

ただし、$\beta_m = \prod_{i=0}^{m-1}(2^{m-i}-1)$, $\gamma_s = \prod_{i=0}^{s-1}(4^{i+1}-1)$

第5章　重み分布式

$RM(2^m, r)$ の重み w の符号語数を $N_{m,r,w}$ とする．$r \geq 2$ に対し，$f \in P_r - P_{r,1}$ かつ $|f|_m = w$ の多項式の数を $N'_{m,r,w}$ とし，$r < 2$ に対しては $N'_{m,r,w} = N_{m,r,w}$ とする．また $r \geq 2$ に対し，$f \in P_r - P_{r-1} - P_{r,1}$，$|f|_m = w$ かつ $\mu(f) = m$ となる多項式の数を $M_{m,r,w}$ とする．

$N_{m,r,w}$，$N'_{m,r,w}$，$M_{m,r,w}$ の間には次の関係式が成立することが知られている[4]．

$$N_{m,r,w} = \sum_{j=0}^{r} N'_{m-r+j,j,w}\, 2^{r-j}\, \alpha_{m,r-j} \quad (11)$$

$$N'_{m,r,w} - N'_{m,r-1,w} = \sum_{j=r}^{m} M_{j,r,2^{j-m}w}\, \alpha_{m,j} \quad (12)$$

$(r \geq 2)$

ただし，$\alpha_{m,j} = \prod_{i=0}^{j-1} (2^{m-i} - 1) / (2^{j-i} - 1)$ * $(0 < j \leq m)$，$\alpha_{m,0} = 1$，$\alpha_{m,j} = 0$ $(j > m)$．

$f \in P_r$, $|f|_m = w$ $(N_{m,r,w})$

- $f \in P_{r,1}$
- $f \notin P_{r,1}$ $(N'_{m,r,w})$
  - $f \in P_{r-1}$
  - $f \in P_r - P_{r-1}$
    - $\mu(f) < m$
    - $\mu(f) = m$ $(M_{m,r,w})$

図 3.　f の分類

---

*　$\alpha_{m,j}$ は m 次元ベクトル空間中の j 次元部分空間の数である．

重み $2^{m-r+1} \leq w < 2^{m-r+1} + 2^{m-r-1}$ について、$N_{m,r,w}$ を求めることを考える。まず定義から

$$N'_{m-r,0,w} = 0$$

$$N'_{m-r+1,1,2^{m-r+1}} = 1$$

であり、$w > 2^{m-r+1}$ の場合には、明らかに

$$N'_{m-r+1,1,w} = 0$$

となる。次に $f \in P_2$ の場合、表1に表れている重みのうちで、$w = 2^{m-r+1}$, $2^{m-r+1} + 2^{m-r-2}$, $2^{m-r+1} + 2^{m-r-3}$ を除いては、補題3-1）により

$$N'_{m-r+2,2,w} = 0$$

で、非零ならば $N'_{m-r+2,2,w}$ が Sloane - Berlekamp の重み分布式[3]から計算できる。

$$N'_{m-r+2,2,2^{m-r+1}} = N_{m-r+2,2,2^{m-r+1}} - (\text{1次式の数})$$

$$= 2\{ 2^{(m-r+2)(m-r+3)/2} - 2^{m-r+2}$$

$$- \sum_{l=1}^{[m-r+2/2]} 2^{l(l+1)} \prod_{i=1}^{l} (2^{m-r+4-2i} - 1)(2^{m-r+3-2i} - 1)$$

$$/ (4^i - 1) \}$$

また $w = 2^{m-r+1} + 2^{m-r-2}$, $2^{m-r+1} + 2^{m-r-3}$ の重みのときには一次因数を含まないから

$$N'_{m-r+2,2,w} = N_{m-r+2,2,w} \quad (w = 2^{m-r+1} + 2^{m-r-2},\ 2^{m-r+1} + 2^{m-r-3}).$$

補題3-1）により

$$N'_{m-r+i,i-1,w} = 0$$

ただし、$3 \leq i \leq r$ かつ $2^{m-r+1} < w < 2^{m-r+1} + 2^{m-r-1}$.

$i \geq 3$, $|f|_{m-r+i} = 2^{m-r+1}$ で $f \in P_{i-1}$ となる多項式は、補題3-2.1）により一次因数を持つから

$$N'_{m-r+i,i-1,2^{m-r+1}} = 0$$

となる。よって、(11)式は(12)式を使い、次の様に書きかえられる。

$$N_{m,r,w} = 2^{r-1}\ \alpha_{m,r-1} + 2^{r-2}\ N'_{m-r+2,2,w}\ \alpha_{m,r-2} + \sum_{i=3}^{r}\left(\sum_{j=i}^{m-r+i} M_{j,i,2^{j-m+r-i}w}\ \alpha_{m-r+i,j}\right) 2^{r-i}\ \alpha_{m,r-i} \qquad (13)$$

ただし、第1項は $w = 2^{m-r+1}$ 以外零で、第2項は $w = 2^{m-r+1}$, $2^{m-r+1}+2^{m-r-2}$, $2^{m-r+1}+2^{m-r-3}$ 以外零である。そして非零のときは既知である。ゆえに、$N_{m,r,w}$ を求めるには、$M_{m,r,w}$ $(r \geq 3)$ を求めれば良い。

逆に、$N_{m',r',w'}$ $(m' \leq m,\ r' \leq r,\ w' \leq w)$ が既知であれば、$M_{m,r,w}$ は (11) 式, (12) 式を使い次の様に計算できる。

$$M_{m,r,w} = N'_{m,r,w} - N'_{m,r-1,w} - \sum_{j=1}^{m-r} M_{m-j,r,w/2^j}\ \alpha_{m,m-j} \quad (r \geq 2) \qquad (14)$$

$$N'_{m,r,w} = N_{m,r,w} - \sum_{j=1}^{r} N'_{m-j,r-j,w}\ 2^j\ \alpha_{m,j} \qquad (15)$$

符号長 n, 情報点数 k, 重み i の符号語数を a_i, 双対符号の重み j の符号語数を b_j とする二元線形符号について、Pless が MacWilliams の恒等式[(18)*]から導出した Pless の恒等式[(17)]が成立する。

$$\sum_{j=0}^{n} j^l a_j = \sum_{j=0}^{n} (-1)^j b_j \left(\sum_{\nu=0}^{l} \nu!\ G_l^{\nu}\ 2^{k-\nu} \binom{n-j}{n-\nu}\right)$$

$$l = 0, 1, 2, \cdots$$

ここで、G_l^{ν} は第2種のスターリング数である。

重み分布を求めるここは、この恒等式を使うことにより、連立一次方程式を解くことに帰着される。RM(256, 3) の場合の方程式を解くには、既知の $w < 2^6$ の符号語数のほか、未知の $N_{2^8,3,2^6}$ が必要である。ところが、$w = 2^{m-r+1}$ のとき、系1により

---

* MacWilliams の恒等式は第2編第4章で言及している。

$M_{i,3,2^{i-2}} = 0$ ($i \leq 4$, $i \geq 8$)

であり、また $N_{5,3,2^3}$, $N_{6,3,2^4}$, $N_{7,3,2^5}$ はもとめられている[16],[3],[5]ので、$M_{i,3,2^{i-2}}$ ($5 \leq i \leq 7$) が (14), (15) 式より計算できる。(ここでは、系1で示された代表多項式を前章のように数え上げる必要はない。) ゆえに、(13) 式から $N_{8,3,2^6}$ がもとまる。よって連立一次方程式が一意に解けて、重み分布がもとまる。あわせて、この重み分布から双対符号 RM (256, 4) の重み分布が、MacWilliams の恒等式を使いもとめられる。この結果を、表3, 4に示す。

これらの結果および既知の RM 符号の重み分布[3],[5],[7]と (14), (15) 式により、$M_{m,r,w}$ ($m \leq 8$, $2 \leq r \leq 5$, $w \leq 2^{m-1}$) がもとまる。この結果を表5に示す。

次に、$r \geq 6$ または $m \geq 9$ の $M_{m,r,w}$ について考える。McEliece の定理[19]により、非零の $N_{m,r,w}$ の重みに対して

$$w \equiv 0 \mod 2^{\lceil m/r \rceil - 1} \quad *$$

したがって、補題3-1) により

$$w = 0 \mod 2^{m-r-1}$$

すなわち

$$M_{m,r,w} = 0$$

ただし、$6 \leq r \leq m \leq 8$, $2^{m-r+1} < w < 2^{m-r+1} + 2^{m-r-1}$.

また、$M_{m,r,w}$ ($m \geq 9$, $r \geq 3$) は表5で同じ m, r, w を持つ多項式の $N(f)$ の和としてもとまる。

このようにして、再び (13) 式を利用して、$2^{m-r+1} \leq w < 2^{m-r+1} + 2^{m-r-1}$ について、任意の次数の $N_{m,r,w}$ の重み分布式が導びかれる。非零の $N_{m,r,w}$ に対する重み分布式を表6に示す。

なお、重み分布の計算や $M_{m,r,w}$ をもとめる計算では総符

---

* 「x」は x 以上の最小の整数である。

号語数に相当する程度の非常に大きい整数を取扱う必要があるので、剰余計算を利用している。プログラムは、FORTRAN で書かれ、NEAC 2200-500 の上で実行された。

表3.　RM(256, 3)の重み分布

重み	符号語数
0 256	1
32 224	777240
48 208	2698577280
56 200	30429671 4240
64 192	7498480471 8940
68 188	707415842488320
72 184	2805501 3884190720
76 180	7642449151 68215040
80 176	20661827603503720320
84 172	41 4411510493363568640
88 168	626613151720190164 9920
92 164	71773299826457585909760
96 160	627671543662325464743336
100 156	420899766531 6969256058880
104 152	217299456742774363427 63520
108 148	866662543611024442078 00320
112 144	267788217345284850768843520
116 140	642477460725187489919139840
120 136	11989598333926588917910896 64
124 132	17424528988794890853600460 80
128	19735408045135544268709626 30

表4. RM(256, 4) の重み分布

重み	符号語数
0 256	1
16 240	3212592
24 232	12593360640
28 228	1518742159360
30 226	168432343 4496
32 224	233496616617720
34 222	2063296207257600
36 220	542807099651 03104
38 218	1024338139923087360
40 216	252719937867046612 48
42 214	6033794958074943897 60
44 212	1399854347244465389 5680
46 210	2987759818922058936 48384
48 208	5792904737745505583537040
50 206	1017252286096269112875417 60
52 204	1619655103361553447861288960
54 202	2343565322961309273295945 7280
56 200	3089417926604160449287795246 08
58 198	3719273524902445073837200506880
60 196	4098137264836771002114121521561 6
62 194	4141480619173867171367168979763 20
64 192	3845865740985098084153656733970460
66 190	3287542793242282666562965426772377 6
68 188	2591212947932701536114666878823628 80
70 186	1886059681929059537272710259084886016
72 184	1269548390171068174996778641485615 3600
74 182	7913408623447625764176899279740207 1040
76 180	4573394856970386006185433693839608381 44
78 178	2453459578418327749200576673639248691 200
80 176	1223080656390056298170784545624868128 1072
82 174	5671617617441057539069326146551035199 4880
84 172	2448752632384909803467471116137640175 20640
86 170	9852628237934713697460734745456908571 77088
88 168	3697309421267214103563968278797989344922880
90 166	1295027629426966103287245094737779792176 7424
92 164	4236837884863832319120204476264041117016 0640
94 162	1295574815048980598319704329861942067855 3600
96 160	3705173500884647486774705211318003305544419 28
98 158	9915802004735909143925198963656039689564979 20
100 156	2484559439836444906990396066029287139548184576
102 154	5831551859032115012912215228214655135598510080
104 152	1282701875564882424375653155536496318431175 2960
106 150	2645154846922844952447010773023487027466941 2352
108 148	5115888787830317886778650235887997152639778816 0
110 146	9282842073524476093207800076996706146784064 3072
112 144	1580741366698452193516048522050804339170247908 00
114 142	2526830167765851924716193074277275819898725990 40
116 140	3792518262515199423076814339875331966357412 24960
118 138	5345676183126909356768139385292824180335365324 80
120 136	7077405736980403869746916592502341954334414 67392
122 134	8802409519265438099288023569683620514970048921 60
124 132	1028563745485706295956669509417284523312047390720
126 130	1129265034025624245213546787421529408984443781120
128	1164971371906499969599368781577141376282748620870

表 5·1. 素因数形による $M_{m,2,w}$

m	w	2	7	31	127
3	4	3	1		
4	6	6	1		
5	16	7	1	1	
6	28	12	1	1	
7	64	13	1	1	1
8	120	20	1	1	1

表 5·2. 素因数形による $M_{m,3,w}$

m	w	2	3	5	7	17	31	127	
4	6	6	1	1	1				
	8	5	1	3					
5	8	8		1	1		1		
	10	9		3			1		
	12	8	1		1		1		41
	14	8		1	1		1		53
	16	8			1		1		331
6	14	14	2	1			1		
	16	10	3	1	2		1		
	18	14	1		2		1		23
	20	12	3	1	2		1		11
	22	16	2		1		1		13·23
	24	10	2	1	2		1		13·131
	26	16	2		1		1		2239
	28	14	5		1		1		617
	30	15	2		2		1		1723
	32	9	2		1		1		873619

表5.2 つづき (r=3)

m	w	2	3	5	7	17	31	127	
7	32	15	2	1	2		1	1	
	36	16	1	1	1		1	1	661
	40	14	1		1		1	1	406907
	44	15	1		1		1	1	61·137·419
	48	14	1		2		1	1	293·33871
	52	15	1		1		1	1	37·5484767
	56	14	1		1	2	1	1	4905917
	60	14	1		2		1	1	*
	64	13	5	1			1	1	113·1172867
8	68	25	2	1	1	1	1	1	
	72	20	1	2	3	1	1	1	13
	76	25	1	1	2	1	1	1	463
	80	17	2	1	1	1	1	1	67·271·409
	84	25	1	1	1	1	1	1	13^2·10399
	88	20	2	1	1	1	1	1	*
	92	25	2	1		1	1	1	5569·127529
	96	16	3	1	2	1	1	1	2671·8098747
	100	25	1	1	1	1	1	1	359·49719953
	104	20	2	1	1	1	1	1	*
	108	25	3	1	1	1	1	1	71 *
	112	17	2	2	1	1	1	1	19·101·6491·1555963
	116	25	2	1	1	2	1	1	263·911·222977
	120	22	2	1	1	1	1	1	13 *
	124	25	2	1	2	1	1	1	*
	128	15	1	1	2	1	1	1	*

*のついた行は、14533 以上の因数を省略している。

表5·3. 素因数形による $M_{m,4,w}$

m	w	2	3	5	7	17	31	127	
4	5	7	1		1				
	7	6		2	1				
5	6	11			1		1		
	8	9		1	1	1	1		
	10	9	1				1		1301
	12	7			1	1	1		463
	14	8		1	1		2		53
	16	7	3	1			1		1087
6	8	14	2		1		1		
	10	14		1	2	1	1		
	12	12	1		1		1		41·461
	14	12	2		1		1		93239
	16	12	1		3		1		23·2539
	18	13	1		1		1		53·263·757
	20	11	2	1	2		1		2189741
	22	10	3		1		1		209245097
	24	10	1		1		1		*
	26	10	2		1		1		367·647·19793
	28	10			1		1		13 *
	30	10	1		1		1		29 *
	32	10	2		1		1		389·36806779
7	16	16	2	3			1	1	
	18	19	3	1	2		1	1	
	20	16	1		2		1	1	11689
	22	18	1			1	1	1	13·73·223
	24	14	1		2		1	1	29·817433
	26	18	1		2		1	1	4457·5479
	28	21	1		4		1	1	29·73·401
	30	17	1		2		1	1	13 *
	32	13	1		1		1	1	23 *
	34	17	3		1		1	1	19·89·2357·115117
	36	15	1		1		1	1	61 *

表5·3 つづき (r=4)

m	w	2	3	5	7	17	31	127	
7	38	18			1		1	1	11 *
	40	13	3	1	1		1	1	*
	42	18	1	1	1		1	1	13·23
	44	17	2		1		1	1	*
	46	16			1		1	1	11·547·677·1439·51874159
	48	11	1		1		1	1	59·71·191·1553 *
	50	16	1		1		1	1	73·103·311 *
	52	14	2		1		1	1	89 *
	54	18	1	1	1		1	1	*
	56	12	3		1		1	1	167·433 *
	58	18	2				1	1	13 *
	60	15	2		1		1	1	*
	62	17	1		1		1	1	*
	64	11					1	1	13 *
8	30	23	1			1	1	1	
	34	23	1	2	2	1	1	1	
	36	22	1		2	1	1	1	19·53
	38	28	2	1	1	1	1	1	181
	40	18	1		2	1	1	1	41·7589
	42	27	1	1	1	1	1	1	639701
	44	20	6	1	1	1	1	1	7813303
	46	25	3		1	1	1	1	*
	48	19	3	1	1	1	1	1	*
	50	25	2	1	1	2	1	1	*
	52	21	1	1	1		1	1	13 *
	54	27	2	1	1	1	1	1	*
	56	19	2		1	2	1	1	13·19·151 *
	58	31		1	1	1	1	1	*
	60	18	1		1	1	1	1	29·47·2539·8863 *
	62	24	2	1	1	1	1	2	1877 *
	64	18	1	1	1	1	1	1	$13\cdot41^2\cdot269\cdot571\cdot821\cdot9833\cdot77041$
	66	24				1	1	1	*
	68	18	3	1	1		1	1	*

表5.3 つづき (r=4)

m	w	2	3	5	7	17	31	127	
8	70	30	1		1	1	1	1	47·53·1231 *
	72	17	3	2	1	1	1	1	1187 *
	74	27	2	1	1	1	1	1	13·41·61 *
	76	18	1		1	1	1	1	37 *
	78	25	1	2		1	1	1	4013 *
	80	19	3			1	1	1	13·41·47·71 *
	82	25	2	1	1	1	1	1	1951 *
	84	18		1	1	1	1	2	19 *
	86	27	2		1		1	1	2791 *
	88	17	1	1	2	1	1	1	4871 *
	90	28	1		1	1	1	1	59·193·1579 *
	92	16	1	1		1	1	1	*
	94	23		2		1	1	1	*
	96	16	1		1	1	2	1	11 *
	98	23	2	1	1	1	1	1	11·23 *
	100	16	2		1	1	1	1	487 *
	102	29	1	1	1		1	1	29 *
	104	16	2	1	1	1	1	1	*
	106	28	2		1	1	1	1	401 *
	108	17		1	1	1	1	1	37 *
	110	26	1		1	1	1	1	239 *
	112	16	1	1	1	1	1	1	*
	114	26	2	1		1	1	1	*
	116	17	2	2	1	1	1	1	13·347 *
	118	28		1	1	1	1	1	2161 *
	120	16			1		2	1	311·457 *
	122	30	5	1	1	1	1	1	41·2347 *
	124	16	2	1	1	1	1	1	*
	126	25	1	1		1	1	1	1579·8369 *
	128	15	1	1		1	1	1	*

*のついた行は、14533 以上の因数を省略している。

表5.4. 素因数形による $M_{m,5,w}$

m	w	2	3	5	7	17	31	127	
5	7	12	1		1		1		
	9	8		1			1		$13 \cdot 53$
	11	13	1				1		13^2
	13	7		1	1		1		$41 \cdot 61$
	15	7					1		$11 \cdot 13 \cdot 997$
6	8	15	2		3		1		
	10	14	2	1	1		1		883
	12	13	2		2		1		28621
	14	12	2		1		1		*
	16	11	5	2	1		1		178093
	18	13	2	1	2		1		*
	20	16	2		1		1		*
	22	10	3		1		1		653 *
	24	9	2	1	1		1		11 *
	26	10	2	1	2		1		*
	28	8	4		1		1		11^2 *
	30	10	3		2		1		19 *
	32	9	8		1	2			19 *
7	10	21	1		2		1	1	
	12	19	1		1		1	1	$23 \cdot 173$
	14	19	1		1		1	1	309059
	16	18	1		1		1	1	$439 \cdot 76441$
	18	17	1		1		1	1	$89 \cdot 163 \cdot 188369$
	20	16	2		1		1	1	11 *
	22	16	1		1		1	1	*
	24	14	1		2		1	1	*
	26	15	1		1		1	1	*
	28	14	1		1		1	1	*
	30	14	1		1		1	1	11 *
	32	14	1		1		1	1	*
	34	14	1		1			1	$19 \cdot 89$ *
	36	15	1	1	2	1	1	1	$29 \cdot 179$

表 5·4　つづき　($r=5$)

m	w	2	3	5	7	17	31	127	
7	38	17		1	1		1	1	*
	40	12	1		1		1	1	29 *
	42	13	1	1	1		1	1	11·23·41·269 *
	44	12	1		1		1	1	*
	46	12			1		1	1	*
	48	12	1	2	1		2	1	*
	50	12	1		1		1	1	*
	52	12	2	1	1		1	1	*
	54	11	2		1		1	1	*
	56	19			1		1	1	*
	58	11	1	2	1		1	1	*
	60	12	2		1		1	1	*
	62	12	2	1	1		1	1	421 *
	64	12		2	1		1	1	*
8	18	28	1	1	1	1	1	1	11
	20	22	2	1	1	1	1	1	43627
	22	24	1	1	2	1	1	1	37·101·157
	24	21	2	1		1	1	1	19·193 *
	26	25	2	1	1	1	1	1	*
	28	21	2	1	1	1	1	1	223 *
	30	22	1	1		1	1	1	*
	32	18	2	1		1	1	1	103 *
	34	22	2	1	2	1	1	1	683 *
	36	22	3	1		1	1	1	23·53 *
	38	22	2	1		1		1	271 *
	40	18	2	1	1	1	1	1	19·257·313 *
	42	22	2	1		1	2	1	13·179·641 *
	44	25	2	1		1	1	1	*
	46	20	3	1	1	1	1	1	*
	48	16	1	1	1	1	1	1	*
	50	20	2	1		1	1	1	*
	52	18	2	1	1	1	1	1	*
	54	21	2	1	1	1	1	1	263 *
	56	16	1	2	1	1	1	1	109 *
	58	21	2	3	1	1	1	1	173 *
	60	21	2	1	1	1	1	1	151 *

表 5·4　つづき　(r=5)

m	w	2	3	5	7	17	31	127	
8	62	20	3	1	2	1	1	1	*
	64	15	2	2	1	1	1	1	43 *
	66	20	1	1		1	1	1	*
	68	18	2	2	1	1	1	1	179
	70	21	2	1	1	1	1	1	223
	72	17	1	1		1	1	1	*
	74	21	1	1		1	1	1	29 *
	76	18	1	3	2	1	2	1	67·73·463·941*
	78	18	3	1		2	1	1	*
	80	14	5	1		1	1	1	673 *
	82	18	1	1	2	1	1	1	*
	84	16	1	2		1	1	1	13 *
	86	22	2	1	1	1	1	1	167 *
	88	14	2	1		1	1	1	*
	90	22	2	2	1	1	1	1	29·37·53·443 *
	92	20	1	1		1	1	1	103·109 *
	94	21	1	1		1	1	1	199 *
	96	13	3	1	3	1	1	1	*
	98	21	2	1		1		1	71 *
	100	17	1	1		1	1	1	*
	102	21	1	1	1	1	1	1	*
	104	14	2	2	1	1	1	1	101 *
	106	21	3	1		1	1	1	*
	108	16	1	1		1	1	1	11·23·797 *
	110	19	1	1	2	1	1	1	83·691 *
	112	12	1	2	1	1	1	1	*
	114	19	3	1		1	2	1	293 *
	116	16	4	1		1	1	1	*
	118	20	1	1	1	1	2	1	11 *
	120	14	1	1		1	1	1	*
	122	20	3	1	2	1	1	1	59 *
	124	17	2	1	1	1	1	1	*
	126	19	1	1		1	1	1	*
	128	13	1	1		1		1	*

＊のついた行は、1009 以上の因数を省略している。

表6. $2^{m-r+1} \le w < 2^{m-r+1} + 2^{m-r-1}$ の重み分布式

(a) $N_{m,r,2^{m-r+1}}$ (w = 10d)

$$= 2^{r-1} \cdot \alpha_{m,r-1}$$

$$+ 2^{r-1} \cdot (2^{(m-r+2)(m-r+3)/2} - 2^{m-r+2} - \sum_{\ell=1}^{[m-r+2/2]} 2^{\ell(\ell+1)} \prod_{i=1}^{\ell} (2^{m-r+4-2i} - 1)$$

$$(2^{m-r+3-2i} - 1)/(4^i - 1)) \cdot \alpha_{m,r-2}$$

$$+ 2^{r+5} \cdot 5 \cdot 7 \cdot 31 \cdot (\alpha_{m-r+3,5} + 2^2 \cdot 3^3 \cdot 7 \cdot \alpha_{m-r+3,6} + 2^7 \cdot 3^2 \cdot 7 \cdot 127 \cdot \alpha_{m-r+3,7}) \cdot \alpha_{m,r-3}$$

$$+ 2^{r+10} \cdot 3^2 \cdot 7 \cdot 31 \cdot (\alpha_{m-r+4,6} + 2 \cdot 5 \cdot 7 \cdot 127 \cdot \alpha_{m-r+4,7}) \cdot \alpha_{m,r-4}$$

$$+ \sum_{k=4}^{r} 2^{r+k^2-k-1} \cdot \beta_{m-r+k} \cdot \alpha_{m,r-k} / \beta_{k-1}^2$$

(b) $N_{m,r,2^{m-r+1}+2^{m-r-3}}$ (w = 10.001d)

$$= 2^{r-2} \cdot N_{m-r+2,2,2^{m-r+1}+2^{m-r-3}} \cdot \alpha_{m,r-2}$$

$$+ 2^{r+22} \cdot 3^2 \cdot 5 \cdot 7 \cdot 17 \cdot 31 \cdot 127 \cdot \alpha_{m-r+3,8} \cdot \alpha_{m,r-3}$$

$$+ 2^{r+19} \cdot 3 \cdot 5^2 \cdot 7^2 \cdot 17 \cdot 31 \cdot 127 \cdot \alpha_{m-r+4,8} \cdot \alpha_{m,r-4}$$

(c) $N_{m,r,2^{m-r+1}+2^{m-r-2}}$ (w = 10.01d)

$$= 2^{r-2} \cdot N_{m-r+2,2,2^{m-r+1}+2^{m-r-2}} \cdot \alpha_{m,r-2}$$

$$+ 2^{r+11} \cdot 3 \cdot 7 \cdot 31 \cdot (7 \cdot 23 \cdot \alpha_{m-r+3,6} + 2^2 \cdot 5 \cdot 127 \cdot 661 \cdot \alpha_{m-r+3,7}$$

$$+ 2^6 \cdot 5^2 \cdot 7^2 \cdot 13 \cdot 17 \cdot 127 \cdot \alpha_{m-r+3,8} + 2^{12} \cdot 3 \cdot 5 \cdot 7^2 \cdot 17 \cdot 73 \cdot 127 \cdot \alpha_{m-r+3,9}) \cdot \alpha_{m,r-3}$$

$$+ 2^{r+15} \cdot 3 \cdot 7^2 \cdot 31 \cdot 127 \cdot (3^2 \cdot 5 \cdot \alpha_{m-r+4,7} + 2^3 \cdot 17 \cdot 19 \cdot 53 \cdot \alpha_{m-r+4,8}$$

$$+ 2^9 \cdot 3 \cdot 5^2 \cdot 17 \cdot 73 \cdot \alpha_{m-r+4,9}) \cdot \alpha_{m,r-4}$$

$$+ 2^{r+23} \cdot 3 \cdot 5 \cdot 7 \cdot 17 \cdot 31 \cdot 127 \cdot (11 \cdot \alpha_{m-r+5,8} + 3 \cdot 5 \cdot 7 \cdot 73 \cdot \alpha_{m-r+5,9}) \cdot \alpha_{m,r-5}$$

表6 つづき

(d) $N_{m,r,2^{m-r+1}+2^{m-r-2}+2^{m-r-4}}$ (w = 10.0101d)

$$= 2^{r+32}\cdot 3\cdot 5\cdot 17\cdot 31\cdot 73\cdot 127\cdot(5\cdot\alpha_{m-r+3,9} + 2^2\cdot 7\cdot 11\cdot 31\cdot\alpha_{m-r+3,10})\cdot\alpha_{m,r-3}$$

$$+ 2^{r+32}\cdot 3\cdot 7^2\cdot 11\cdot 17\cdot 31^2\cdot 73\cdot 127\cdot\alpha_{m-r+4,10}\cdot\alpha_{m,r-4}$$

$$+ 2^{r+30}\cdot 3^2\cdot 5^2\cdot 7\cdot 11\cdot 17\cdot 31^2\cdot 73\cdot 127\cdot\alpha_{m-r+5,10}\cdot\alpha_{m,r-5}$$

(e) $N_{m,r,2^{m-r+1}+2^{m-r-2}+2^{m-r-3}}$ (w = 10.011d)

$$= 2^{r+21}\cdot 3\cdot 5\cdot 7^2\cdot 17\cdot 31\cdot 127\cdot(2\cdot 463\cdot\alpha_{m-r+3,8} + 3\cdot 11\cdot 73\cdot 317\cdot\alpha_{m-r+3,9}$$

$$+ 2^6\cdot 3^2\cdot 7\cdot 11\cdot 31\cdot 73\cdot\alpha_{m-r+3,10} + 2^{14}\cdot 11\cdot 23\cdot 31\cdot 73\cdot 89\cdot\alpha_{m-r+3,11})\cdot\alpha_{m,r-3}$$

$$+ 2^{r+24}\cdot 3\cdot 5\cdot 7\cdot 17\cdot 31\cdot 127\cdot(3\cdot 181\cdot\alpha_{m-r+4,8} + 2^2\cdot 5\cdot 7\cdot 41\cdot 73\cdot\alpha_{m-r+4,9})\cdot\alpha_{m,r-4}$$

$$+ 2^{r+24}\cdot 3^2\cdot 5\cdot 7\cdot 17\cdot 31\cdot 73\cdot 127\cdot(5\cdot 7\cdot 23\cdot\alpha_{m-r+5,9} + 2^4\cdot 3^2\cdot 5\cdot 11\cdot 31\cdot\alpha_{m-r+5,10}$$

$$+ 2^{11}\cdot 11\cdot 23\cdot 31\cdot 89\cdot\alpha_{m-r+5,11})\cdot\alpha_{m,r-5}$$

$$+ 2^{r+31}\cdot 3^2\cdot 7\cdot 11\cdot 17\cdot 31^2\cdot 73\cdot 127\cdot(7\cdot\alpha_{m-r+6,10} + 2^3\cdot 5\cdot 23\cdot 89\cdot\alpha_{m-r+6,11})\cdot\alpha_{m,r-6}$$

(f) $N_{m,r,2^{m-r+1}+2^{m-r-2}+2^{m-r-3}+2^{m-r-4}}$ (w = 10.0111d)

$$= 2^{r+31}\cdot 3\cdot 7^2\cdot 31\cdot 73\cdot 127\cdot(2\cdot 5^2\cdot 7\cdot 17\cdot\alpha_{m-r+3,9} + 2^3\cdot 11\cdot 17\cdot 31\cdot 47\cdot\alpha_{m-r+3,10}$$

$$+ 5\cdot 11\cdot 17\cdot 23\cdot 31\cdot 73\cdot 89\cdot\alpha_{m-r+3,11} + 2^8\cdot 3^2\cdot 5^2\cdot 7\cdot 11\cdot 13\cdot 17\cdot 23\cdot 31\cdot 89$$

$$\cdot\alpha_{m-r+3,12} + 2^{18}\cdot 3\cdot 5\cdot 7\cdot 11\cdot 13\cdot 23\cdot 31\cdot 89\cdot 8191\cdot\alpha_{m-r+3,13})\alpha_{m,r-3}$$

$$+ 2^{r+32}\cdot 3\cdot 5\cdot 7\cdot 11\cdot 17\cdot 31^2\cdot 73\cdot 127\cdot 139\cdot\alpha_{m-r+4,10}\cdot\alpha_{m,r-4}$$

$$+ 2^{r+29}\cdot 3^2\cdot 5\cdot 7\cdot 11\cdot 17\cdot 31^2\cdot 73\cdot 127\cdot(5^2\cdot 11\cdot\alpha_{m-r+5,10}$$

$$+ 2^6\cdot 23\cdot 89\cdot\alpha_{m-r+5,11})\cdot\alpha_{m,r-5}$$

表6 つづき

$$+ 2^{r+36}\cdot 3^2\cdot 5\cdot 7\cdot 11\cdot 17\cdot 23\cdot 31\cdot 73\cdot 89\cdot 127\cdot (31\cdot \alpha_{m-r+6,11}$$

$$+ 2^4\cdot 3^2\cdot 7\cdot 13\cdot 31\cdot \alpha_{m-r+6,12} + 2^{12}\cdot 3\cdot 7\cdot 13\cdot 8191\cdot \alpha_{m-r+6,13})\cdot \alpha_{m,r-6}$$

$$+ 2^{r+43}\cdot 3^3\cdot 5\cdot 7^2\cdot 11\cdot 13\cdot 17\cdot 23\cdot 31\cdot 73\cdot 89\cdot 127\cdot (3\cdot \alpha_{m-r+7,12}$$

$$+ 2^4\cdot 8191\cdot \alpha_{m-r+7,13})\cdot \alpha_{m,r-7}$$

(g) $N_{m,r,2^{m-r+1}+2^{m-r-1}-2^{m-r-k-1}}$ ($w = 10.0\underbrace{1\ldots1}_{k}d$, $m-r-\lceil m/r\rceil \geq k \geq 4$)

$$= 2^{r+k^2+5k+7}\cdot \beta_{m-r+3}\cdot (1/3\cdot 7\cdot \gamma_{k-1} + 2^{2k-3}\cdot 41/3\cdot \gamma_k + 2^{4k+6}/3\cdot \gamma_{k+1})\cdot \alpha_{m,r-3}$$

$$+ 2^{r+k^2+5k+6}\cdot \beta_{m-r+k+2}\cdot (1/3\cdot \beta_k^2 + 2^{k+2}/3\cdot \beta_k\cdot \beta_{k+1})\cdot \alpha_{m,r-k-2}$$

$$+ 2^{r+k^2+6k+9}\cdot \beta_{m-r+k+3}\cdot (1/3\cdot \beta_k\cdot \beta_{k+1} + 2^{k+1}/\beta_{k+1}^2 + 2^{2k+6}/3\cdot \beta_{k+1}\cdot \beta_{k+2})$$

$$\cdot \alpha_{m,r-k-3}$$

$$+ 2^{r+k^2+7k+13}\cdot \beta_{m-r+k+4}\cdot (1/3\cdot 5\cdot \beta_k\cdot \beta_{k+2} + 2^{k+1}/3\cdot \beta_{k+1}\cdot \beta_{k+2})\cdot \alpha_{m,r-k-4}$$

(h) $N_{m,r,2^{m-r+1}+2^{m-r-1}-2^{m-r-k-1}+2^{m-r-k-3}}$ ($w = 10.0\underbrace{1\ldots1}_{k}01d$,

$m-r-\lceil m/r\rceil-2 \geq k \geq 2$)

$$= 2^{r+k^2+11k+22}\cdot \beta_{m-r+3}\cdot \alpha_{m,r-3}/3\cdot 7\cdot \gamma_{k+2}$$

$$+ 2^{r+k^2+9k+22}\cdot \beta_{m-r+k+3}\cdot \alpha_{m,r-k-3}/3^2\cdot 5\cdot \beta_{k+1}\cdot \beta_{k+3}$$

$$+ 2^{r+k^2+9k+20}\cdot \beta_{m-r+k+4}\cdot \alpha_{m,r-k-4}/3^2\cdot \beta_{k+2}^2$$

ただし、$\alpha_{m,j} = \prod_{i=0}^{j-1} (2^{m-i} - 1)/(2^{j-i} - 1)$ $(0 < j \leq m)$, $\alpha_{m,0} = 1$,

$\alpha_{m,j} = 0$ $(j < 0$, $j > m)$,

$\beta_m = \prod_{i=0}^{m-1} (2^{m-i} - 1)$, $\gamma_s = \prod_{i=0}^{s-1} (4^{i+1} - 1)$.

$[x]$ は x の整数部分，$\lceil x\rceil$ は x 以上の最小の整数を表す.

第6章　結論

任意の次数で、重み $2d \leq w < 2.5d$ についての重み分布式が導出された。これらは既知の重み分布式の重みに関する拡張になっている。また導出の課程において、この重みの範囲の代表多項式が示されている。そして符号長256で3次および4次のすべての重み分布が求められている。さらに素因数形で表現された $M_{m,r,w}$ ($m \leq 8$, $2 \leq r \leq 5$, $w \leq 2^{m-1}$) も示されている。ここで示された分布式および $M_{m,r,w}$ などの結果は、RM符号あるいは関連する符号の構造を知る手がかりになるものと思われる。

文献

(1) D. E. Muller : "Application of Boolean algebra to switching circuit design and to error detection", IRE Trans. Electron. Comput., vol. EC-3, p. 6 (Sept. 1954).

(2) I. S. Reed : "A Class of multiple-error-correcting codes and the decoding scheme", IRE Trans. Inform. Theory, vol. IT-4, p. 38 (Sept. 1954).

(3) N. J. Sloane and E.R. Berlekamp : "Weight Enumerator for Second-Order Reed-Muller Codes", IEEE Trans. Inform. Theory, vol. IT-16, p. 745 (1970).

(4) T. Kasami and N. Tokura : "On the Weight Structure of Reed-Muller Codes", op. cit. p. 752.

(5) M. Sugino, Y. Lenaga, N. Tokura and T. Kasami: "Weight Distribution of (128, 64) Reed-Muller Code", ibid., vol. IT-17 (Sept. 1971).

(6) 笠, 都倉, 安積 : "Reed-Muller 符号の重み分布について", 信学会インホナ理研資, IT71-14 (1971-04).

(7) 安積 : "Reed-Muller 符号の重み分布と構造", 阪大・基工・制御・修士論文 (昭47).

(8) D. V. Sarwate and E.R. Berlekamp : "On the Weight Enumeration of Reed-Muller Codes and their Cosets", Abstracts of Papers, 1972 IEEE International Symposium on Information Theory.

(9) E.R. Berlekamp : 私信

(10) H.C.A. van Tilborg : "On Weights in Codes", Rept. of Mathematics, Technological Univ. Eindhoven,

Netherlands (Dec. 1971).
(11) 嵩, 都倉, 安積: "Reed-Muller符号の重み分布構造", 信学会インホメ理研資, IT71-75 (1972-01).
(12) 嵩, 都倉, 安積: "Reed-Muller符号の重み分布公式 ($2d \leq w < 2.5d$)", ibid., (Jan. 1973).
(13) T. Kasami, N. Tokura and S. Azumi: "Weight Enumerator Formulas of Reed-Muller Codes for $2d \leq w < 2.5d$", Proc. of the 3rd International Symposium on Information Theory, Tallinn, USSR (June 1973).
(14) T. Kasami, N. Tokura and S. Azumi: "On the Weight Enumeration of Weights less than $2.5d_{min}$ of Reed-Muller Codes", IEEE International Symposium on Information Theory, Ashkelon, ISRAEL (June 1973).
(15) E. R. Berlekamp: "Algebraic Coding Theory", MacGraw-Hill, New York (1968).
(16) W. W. Peterson and E. J. Weldon Jr.: "Error Correcting Codes", 2nd Edition, MIT Press, Cambridge, Mass. (1972).
(17) V. Pless: "Power moment identities on weight distributions in error correcting codes", Information and Control, vol. 6, p. 147 (1963).
(18) F. J. MacWilliams: "A theorem on the distribution of weights in a systematic code", Bell Syst. Tech. J., vol. 42, p. 79 (1963).
(19) R. J. McEliece: "Linear recurring sequences over finite fields", Ph. D. dissertation, Calif. Inst. of Technology, Pasadena (1967).

(20) T. Kasami, N. Tokura and S. Azumi : " On the Weight Enumeration of Weights less than 2.5 d of Reed-Muller Codes ", 阪大・基礎工・報告 (June 1974).

第2編　最適な修正ハミング符号

第1章　序言

能率が良く、機構化も比較的容易である単一誤り訂正二重誤り検出可能な符号として、修正ハミング符号（以下、MH符号という）がある。このMH符号は二元ハミング符号[1]の拡大符号から、実際に必要なだけの情報点数を持つ符号になるように、ベクトル成分の適当な部分を取り除いた符号で、最近では主記憶装置の信頼性をあげる目的等で使われている[2],[3]。

拡大ハミング符号の符号長を2^m，検査点数を$m+1$とし、その拡大ハミング符号から導出されたMH符号の符号長をn（$2^{m-1}<n\leq 2^m$），パリティ検査行列の列ベクトルの集合をSとする。三重以上の多重誤りとして、たとえばSのなかの列C_1, C_2, C_3に対応する成分でビット誤りが起きたとすると、シンドロームは$C_1+C_2+C_3$となり、この列ベクトルがSに含まれていなければ誤り訂正不能と判定して、誤り検出ができる。Sに含まれていれば、その列ベクトルに対応する成分にビット誤りが起きたものとして誤って訂正する。特にこのような多重誤りを誤って復号することは好ましくないので、誤って復号する確率P_eが最小になるようにSを選択することが問題となる。

集合Sとして、拡大ハミング符号のパリティ検査行列の奇数の重みを持つ列から、その重みの小さい順にn個選択してMH符号のパリティ検査行列とする方法が提案されている[2]。これは復号器のある種の費用を最小にすることを主目的としており、本論とは立場が異なる。また、いくつかの与えられたMH符号について、多重誤り

に対する能力が計算されている[4]が、その計算手続きは能率的ではない。本論文では、Sとしてあらゆる組合せを考慮に入れて、できるだけ小さいP_eを持つMH符号を組織的に能率良くさがす方法について考察している。

長さ2^mのベクトルの成分位置に、GF(2)の上のm次元ベクトル空間V_mの各ベクトルを1対1に対応させると、V_mの一つの可逆アフィン変換に対応して、ベクトル成分の置換が一つ定まる。拡大ハミング符号は任意の可逆アフィン変換によって不変に保たれている。したがって、拡大ハミング符号のパリティ検査行列のなかで、取り除くべき列ベクトルの集合$\bar{S}$を考えたとき、この$\bar{S}$から可逆アフィン変換により変換される任意の集合$\bar{S}'$を考えても、得られるMH符号の重み分布はもとの符号の重み分布に等しいことが示される。この結果を利用すると、考えるべき集合Sの場合の数は大幅に減少する。

さらに各MH符号の重み分布を能率良く求めるために、MH符号の双対符号を利用する。$m \geq 5$なら、もとのMH符号の総符号語数と比較して、双対符号の総符号語数の方がはるかに少ない。したがって、双対符号の各符号語を生成することにより、双対符号の重み分布が能率良く求められる。そして互いに双対な線形符号間の重み分布に関するMacWilliamsの恒等式により、もとのMH符号の重み分布を求めることができる。

このようにして、(22, 16)(符号長22, 情報点数16の符号、以下同様), (55, 48)について本論の意味で最適な符号を、(18, 12), (39, 32), (43, 36), (72, 64)について、すぐれた符号を計算機により求めた。またこれらの符号長について、原始多項式を生成多項式とする短縮化巡回符号の拡大符号のなかで最適なものを求めた。

第2章　準備

MH符号の符号長をn（$2^{m-1} < n \leq 2^m$），重みiの符号語数をN_i，各ビットの誤り確率をp，正しく復号する確率をP_c，誤って復号する確率をP_e そして誤りを検出しても復号できない確率をP_f とすると、P_c，P_e，P_f は次式で与えられる[5]。

$$\left.\begin{aligned} &P_c + P_e + P_f = 1 \\ &P_c = (1-p)^{n-1}(1-p+np) \\ &P_c + P_e = \sum_{i=0}^{n} N_i p^{i-1}(1-p)^{n-i-1} \\ &\quad \{i(1-p)^2 + (n-i)p^2 + p(1-p)\} \end{aligned}\right\} \quad (1)$$

一般に$p \ll 1$だから、P_e を小さくするためにはMH符号の最小重みの符号語数を最小にすれば良い。よく知られているようにハミング符号の最小重みは3であり、拡大ハミング符号は偶パリティになるように1ビット加えて最小重み4にし、二重誤りも検出可能にしている。この性質を保って作ったMH符号の最小重みも4だから、最小のN_4 を持つMH符号を見つけることを考える。同じ符号長のMH符号のクラスのなかで最小のN_4 を持つ符号を最適な符号とよぶことにする。N_4 が求まれば、三重誤りを誤って訂正する割合P_{e3}，四重誤りを見逃す割合P_{e4}は次式の様になる。

$$P_{e3} = \frac{4N_4}{\binom{n}{3}}, \quad P_{e4} = \frac{N_4}{\binom{n}{4}} \qquad (2)$$

符号長2^m の拡大ハミング符号は、よく知られているように、$m-2$次のリード マラー符号と等価である。GF(2)の上のm変数で次数r次以下の多項式全体の集合をP_r とかく。αをGF(2^m)の任意の原始元とし、

$$\alpha^i = \sum_{j=1}^{m} a_{ij}\,\alpha^{j-1}, \quad 0 \le i < 2^m - 1$$

とおく。ここで a_{ij} は GF(2) の元である。各 i ($0 \le i < 2^m - 1$) について

$$A_i^T = (a_{i1}, a_{i2}, \cdots, a_{im}) \quad *$$

とおく。P_r の元 f について、$f(a_{i1}, a_{i2}, \cdots, a_{im})$ を $f(A_i)$, $f(0, 0, \cdots, 0)$ を $f(0)$ とかき、$f \in P_r$ に対して

$$\psi(f) = (f(0), f(A_0), f(A_1), \cdots, f(A_{2^m-2}))$$

と定義すると、良く知られているように、拡大ハミング符号は $m-2$ 次のリード・マラー符号

$$RM(2^m, m-2) = \{\psi(f) \mid f \in P_{m-2}\}$$

であり、その双対符号は1次のリード・マラー符号で

$$RM(2^m, 1) = \{\psi(f) \mid f \in P_1\}$$

で与えられる(5)。

最小重みを4以上に自動的に保証するため、以下MH符号としては、全パリティチェックを持ったものを考えることにする。(したがって、符号語の重みはすべて偶数である。) $RM(2^m, m-2)$ から最初の成分を落したものがハミング符号であるから、ここで考えているMH符号はハミング符号から任意の $2^m - 1 - n$ 成分を除去した符号の拡大符号にほかならない。

1から $2^m - 2$ までの自然数から、任意に重複なく $n-1$ 個選んで、$i_1 < i_2 < \cdots < i_{n-1}$ とし

$$S = \{A_{i_1}, A_{i_2}, \cdots, A_{i_{n-1}}\}$$

$$\bar{S} = V_m - \{\text{零ベクトル}\} - S$$

とおき、$\bar{S}$ をマスクパターンとよぶ。定義から S は零ベクトルでない $n-1$ 個の相異なる V_m のベクトルよりな

* A_i^T は A_i の転置ベクトルを示す。

る．また$\overline{S}$の要素の数をlとかくことにすると

$$l = 2^m - n$$

である．

$$H(S) = \{ (f(A_{i_1}), f(A_{i_2}), \cdots, f(A_{i_{n-1}})) \mid f \in P_{m-2} \}$$

とおくと、これはハミング符号から、第i_1+1成分，第i_2+1成分，$\cdots$，第$i_{n-1}+1$成分以外を除去して得られる符号である．$H(S)$の拡大符号

$$\{ (\sum_{j=1}^{n-1} f(A_{i_j}), f(A_{i_1}), f(A_{i_2}), \cdots, f(A_{i_{n-1}})) \mid f \in P_{m-2} \}$$

を$EH(S)$とかく．本論の問題は、$EH(S)$の重み4の符号語数が最小となるようなSを見い出すことである．

第3章　マスクパターンの発生

m個の一次式

$$y_i = \sum_{j=1}^{m} t_{ij} x_j, \quad t_{ij} \in GF(2), \quad 1 \leq i \leq m$$

による線形変換において、係数行列 $T = [t_{ij}]$ のランクがmのとき、この変換をユークリッド変換（以下、E変換と略す）* とよび、上式をベクトル表示で

$$Y = TX$$

とおく。前章の $S = \{A_{i_1}, A_{i_2}, \cdots, A_{i_{n-1}}\}$ に対して

$$g(S, X) = \sum_{j=1}^{n-1} \prod_{k=1}^{m} (x_k + 1 + a_{i_j k}), \quad a_{ik} \in GF(2)$$

を考えると、$g(S, A_{i_j}) = 1$ $(1 \leq j < n)$、そして $A_i \notin S$ なら、$g(S, A_i) = 0$ である。またXに対する任意のE変換Tについて

$$TS = \{TA_i \mid A_i \in S\}$$

とおく。定義から

$$g(TS, X) = g(S, T^{-1}X) \qquad (3)$$

となり、次の補題が成立する。

［補題1］　任意の $GF(2)$ の上の m行 m列の正則行列Tについて、$EH(S)$ の重み分布と $EH(TS)$ の重み分布は等しい。

（証明）　定義から、$\{w(f(X)g(S, X)) \mid f \in P_{m-2}\}$, $\{w(f(X)g(TS, X)) \mid f \in P_{m-2}\}$ の重み分布**は、$H(S)$, $H(TS)$ の重み分布にそれぞれ等しい。一方式(3)より

$$\{w(f(X)g(TS, X)) \mid f \in P_{m-2}\}$$

---

*　可逆アフィン変換で定数項が0の場合である。

**　上の集合で同じベクトルの重みは重複して数えない。

$= \{ v(f(TX)g(S,X)) \mid f \in P_{m-2} \}$

である。さらに、$\{ f(TX) \mid f \in P_{m-2} \} = P_{m-2}$ により、$H(S)$ と $H(TS)$ は同じ重み分布を持ち、それらの拡大符号の重み分布も等しい。　（証明終）

$l < 2^{m-1} < n$ ゆえ、S より $\bar{S}$ を考える方が便利である。補題1により、互いに E 変換で移り得るような $\bar{S}$ について、その代表を一つ選んで考えれば十分である。しかし、正確に代表のみを選択する良い方法は知られていないので、以下の様に、一般性を失うことなく、$\bar{S}$ として〝標準的〟なものに限定する。

$\bar{S}$ に含まれるベクトルのなかで一次独立なものの数を $\#(\bar{S})$ とかく。第 i 成分が1で他のすべての成分が0の V_m の列ベクトルを e_i とし、$e_1, e_2, \cdots, e_i$ で張られる V_m の部分空間を $V_m^{(i)}$ とかく。補題1から、次の補題が得られる。

［補題2］　$\#(\bar{S}) = t$ ならば、$\bar{S}$ として $e_1, e_2, \cdots, e_t$ を含み、残りが $V_m^{(t)}$ の重み2以上の列ベクトルよりなるもののみ選択すれば十分である。

これにより、考えるべき $\bar{S}$ の場合の数は、$\binom{2^m-1}{l}$ から $\sum_{t=1}^{m} \binom{2^t-1-t}{l-t}$ に減少する。

$\bar{S} = \{ v_1, v_2, \cdots, v_l \}$

ただし、$v_i = e_i$ $(1 \le i \le t)$

とする。ベクトル v の第1成分を下位の桁とみた2進数の値を $b(v)$ とし、ベクトルの重みを $w(v)$ とかく。また $v = (a_1, a_2, \cdots, a_m)^T$ の部分ベクトル $(a_i, a_{i+1}, \cdots, a_k)^T$ を $v(i, k)$ とかく。$\bar{S}$ を選択する場合の重複をさけるために、$v_{t+1}, v_{t+2}, \cdots, v_l$ に対して、一般性を失うことなく次の条件1，2に従って順序づけを行う。

条件1：　$w(v_{t+1}) \leq w(v_{t+2}) \leq \cdots \leq w(v_\ell)$.

条件2：　$w(v_j) = w(v_{j+1}) = \cdots = w(v_{j'})$ を満たすベクトルに対しては $b(v_j) < b(v_{j+1}) < \cdots < b(v_{j'})$ であること.

すなわち、いくつかの列ベクトルを選択したとして、次に選択する列ベクトルは条件1，2を満たすもののなかから順次選択する．もしも $\ell - t$ 個の適合する列ベクトルが選択できなくなれば、バックトラックすることにより、他の新しい組合せを調べる．さらに、$V_m^{(t)}$ のベクトル成分の置換およびそれに伴う $v_1, v_2, \cdots, v_\ell$ の並びかえを考えることにより、一般性を失うことなく、v_{t+1} は $v_{t+1}(1, t)$ が次の条件を満たすように選び得る．

条件3：　2成分以上のベクトルに対し、その成分が、すべて1であるか、すべて0であるか、最初のいくつかの連続する成分が1で残りの成分が0であること.

$V_m^{(t)}$ のベクトル成分は v_{t+1} の成分が1であるものと0であるものとの2組に分割され、各組に属する成分間の置換の自由度が残る．以下、次々に分割された2成分以上の各部分ベクトルについて、いずれも条件3を満足するものを選択すれば十分である．置換できる自由度が残っている際に、条件3を満足するベクトルを選択することは、先の条件2に矛盾しない．したがって、条件1，2を満たし、置換できる自由度が残っている場合に限り、条件3を満足するベクトルを $V_m^{(t)}$ から順に選択する．図1に、$m=7$，$\#(S)=6$ の場合の列ベクトルの選択を例示する．図の中で、⌋ は次に選択するベクトルに対して置換できる自由度のある部分を示す．この性質によ

	v_1	v_2	・・・	v_6	v_7	v_8	v_9	v_{10} ・・・
1	1	0		0	1	0	1	1
2	0	1		0	1	0	1	0
3	0	0		0	0	1	1	1
4	0	0		0	0	1	0	1
5	0	0		0	0	1	0	0
6	0	0		1	0	0	1	1
7	0	0		0	0	0	0	0

図1　列ベクトルの選択例

り、$\overline{S}$の場合の数は近似的に

$$\frac{\sum_{t=1}^{m} \binom{2^t-1-t}{l-t}}{m!}$$

にまで減少する。

次にMH符号のクラスを既約な生成多項式を持つ短縮化巡回符号に限って、そのなかで最適な符号を求めることを考える。m次の原始多項式$f_m(X)$を任意に選び、その根の一つをαとする。パリティ検査行列$[A_0, A_1, \cdots, A_{2^m-2}]$の最後の連続する$l$個の列ベクトルを選んで、

$$\overline{S} = \{A_{2^m-l-1}, A_{2^m-l}, \cdots, A_{2^m-2}\}$$

として、一つの符号が決まる。他のm次既約多項式で周期が2^{m-1}より大きいものは原始多項式に限る。$\{s_1, s_2, \cdots, s_L\}$を$2^m-1$と素な$2^m-2$以下の正整数で、かつどの2つの$s_i, s_j$（$i \neq j$）についても

$$s_i \equiv s_j 2^{\mu} \bmod (2^m-1), \quad 0 \leq \mu < m$$

の関係が成り立たないような最大集合とすると、α^{s_1},

$\alpha^{s_2}, \cdots, \alpha^{s_L}$ の最小多項式は互いに異なる原始多項式で、これ以外に m 次の原始多項式はない。異なる原始多項式を一つ一つとる代りに、$f_m(X)$ を一つ固定しておき、これに対する $\overline{S}$ から次の L 個

$$\{A_{s_l}(2^m-l-1), A_{s_l}(2^m-l), \cdots, A_{s_l}(2^m-2)\}, \quad 1 \leq l \leq L$$

をとればよい。ただし添字は $\bmod(2^m-1)$ で考える。

第4章　重み t の符号語数の計算

一つのマスクパターン $\bar{S}$ が与えられたとき、$EH(S)$ の重み分布を求めることを考える。$EH(S)$, $H(S)$ の重み i の符号語数をそれぞれ N_i, N_i' とすると、前者は後者の拡大符号だから、$0 \le i \le n$ に対して

$$\left.\begin{array}{ll} N_i = N_{i-1}' + N_i' & i: \text{偶数} \\ N_i = 0 & i: \text{奇数} \end{array}\right\} \quad (4)$$

ただし、$N_{-1}' = N_n' = 0$. したがって $H(S)$ の重み分布を求めれば良い。$H(S)$ の総符号語数は 2^{n-m-1}, その双対符号 $H^d(S)$ の総符号語数は 2^m であり、$2^{m-1} < n \le 2^m$ により、$m \ge 5$ では $2^{n-m-1} >> 2^m$. したがって、まず $H^d(S)$ の重み分布を求め、次に MacWilliams の恒等式で $H(S)$ の重み分布を求める方が、$H(S)$ の重み分布を直接求めるよりもはるかに能率が良い。

与えられた $\bar{S} = \{A_{j_1}, A_{j_2}, \cdots, A_{j_\ell}\}$ に対して、第 j_1+1 成分, 第 j_2+1 成分, $\cdots$, 第 $j_\ell+1$ 成分が1, 他の成分が0の V_{2^m-1} のベクトルを $u(\bar{S})$ とかく。

$$[A_0, A_1, \cdots, A_{2^m-2}] \quad (5)$$

は、ハミング符号のパリティ検査行列の一つであり、行の任意の線形和は、第1行目の行ベクトルを何ビットか巡回シフトしたものに1対1に対応する[6]。ここで、(5) の各行はいわゆる長さ 2^m-1 の最大長系列である。(5) の行列から第 j_1+1 列, 第 j_2+1 列, $\cdots$, 第 $j_\ell+1$ 列を除去した行列は $H(S)$ のパリティ検査行列であり、$H^d(S)$ の生成行列である。$\ell < 2^{m-1}$ ゆえに、$H(S)$ の各行はさいに一次独立である。

以上から、$H^d(S)$ の重み i の符号語数を M_i とすると、M_i は次の様に求まる。(5) の第1行目の行ベクトル g_1 をよビット巡回シフトして得られるベクトルを

$c^j g_1$ とする。

［補題3］ $c^j g_1 \cdot u(S)$ のなかで、重み i (>0) である j の個数は M_i に等しい。ただし、$0 \le j < 2^m - 1$ で、$\cdot$ はビット毎の AND 操作を表わす。

補題3により、g_1 を巡回シフトして求めた重み分布と、$M_0 = 1$ により、$H^d(S)$ 全体の重み分布が求まる。

一般に、符号長 n、情報点数 k、重み i の符号語数を a_i，双対符号の重み j の符号語数を b_j とする二元線形符号について、次の MacWilliams の恒等式*が成立する(7)。

$$\sum_{i=0}^{n} a_i \binom{i}{r} = 2^{k-r} \sum_{j=0}^{r} (-1)^j b_j \binom{n-j}{n-r},$$

$$r = 0, 1, \cdots, n$$

上式は一方の符号の重み分布が完全に知られているとき、双対符号の重み分布を求めるのに便利である。上式から、$H(S)$ と $H^d(S)$ の場合の重み分布の関係式が次のように導びかれる。

$$N_i' = \frac{1}{2^m} \sum_{j=0}^{n-1} M_j h(i, j), \quad 0 \le i < n$$

$$h(0, j) = 1, \quad h(i, 0) = \binom{n-1}{i}$$

$$h(i, j) = (-1)^i h(i, n-1-j)$$

$$h(i, j) = \{(n-i-j) h(i-1, j) - j h(i-1, j-1)\} / i$$

上式と式(4)により $EH(S)$ の重み分布が決まるが、符号の評価を重み 4 の符号語数をもとに行うので、上式から N_3', N_4' を求めれば良い。

---

* MacWilliams の恒等式は多様に表現できる(たとえば5)。

第5章　符号探索法

マスクパターンを発生するために実際に使用した手続においては、効果とプログラムの簡単さを考慮して、上で述べたベクトル成分の置換のうちの一部のみを利用した。すなわち、v_{i+2} 以降の選択で置換の自由度があるとき、置換する範囲を、各列ベクトルのうち第 t 成分を含む一箇所の部分ベクトルに限った。

列ベクトル v について、$v(i, j)$ の成分がすべて1で、かつ $v(j, t)$ がすべて0である最小の i, および j をそれぞれ $O(v)$, $z(v)$ とする。$V_m^{(l)}$ のベクトルは一定の順序に並んでおり、S の要素のうち今 v_i まで選択されたとする。次に条件に適合するベクトル v_{i+1} を $V_m^{(l)}$ から選ぶ場合、$w(v_i) \leq w(v)$, かつ $w(v_i) = w(v)$ なら $b(v_i) < b(v)$, かつ $z(v_i) + 1 \geq O(v)$ を満足する最初のベクトル v を v_{i+1} とし、第 $i+1$ 番目の列ベクトルとしてこの v を選択したことを記憶して、バックトラックできるようにしておく。

一つのマスクパターンが決定されると、補題3により、あらかじめ用意しておいた最大長系列を、巡回シフトしそれにマスクをして $H^d(S)$ の重み分布を求める。これからもとのMH符号の N_4 の値を求める。

双対符号間の重み分布計算では、総符号語数に相当する程度の大きさの整数計算を伴うため、剰余計算による方法を利用した。結果の N_4 の値は整数型一語長（16ビット）に納まる大きさであるので、N_4 をこえかつ整数型一語に納まる一つの素数を法とする剰余計算を行った。

計算時間は、m と l に依存して大きく変動し、すべて

の必要なマスクパターンを調べつくすことができない場合がある。これらの符号のクラスに対しては、次に示す方法で小さいN_4の値を求めた。

最初はいくつかの適当なマスクパターン（たとえば、短縮化巡回符号に対するマスクパターン）を初期値として与え、前記のアルゴリズムに従い、$\bar{S}$の場合の数を適当に限ってN_4の値を求める。次にこのうちで小さいN_4^*を与える$\bar{S}$の一つから、$U(\bar{S})$を作り$\mathrm{mod}(2^m-1)$で巡回シフトしたベクトルに対応するマスクパターンを考えると、各マスクパターンを使い導出された符号は、いずれも同じ重み分布を持つ。これらのマスクパターンを新しい初期値として、くり返し探索することにより、最適という保証はないが、すぐれた符号が求められた。

プログラムはFORTRANで書かれ、マスクパターン発生とN_4を計算するルーチンは約400ステートメントである。計算機はFACOM230-45Sを使用し、すべての必要なマスクパターンを調べるのに要した処理時間は、符号長55の場合で約15分である。一つのマスクパターンからN_4の値を求めるのに要した時間は、符号長72の場合で1秒弱であった。

---

* 本稿では、最小のN_4のうち最初に出現したものを使用した。

第6章　求められた符号の表

実際の計算機システムで使用されている語長[8]を情報点数とする符号として、本稿では次の6種類の符号のクラスをとりあげ、計算を行っている。

(18, 12), (22, 16), (39, 32),
(43, 36), (55, 48), (72, 64)

表1に、各符号長に対する符号のクラスについての最小のN_4の値とそのときの一つのマスクパターンを示す。このうちで符号長22および55に関するものは、必要なすべてのマスクパターンを調べつくすことにより、最適であることが保証されている。マスクパターンは、Sの各要素β_iの値$b(\beta_i)$を10進数で表現したものの組で表わされている。

ここで求められたMH符号を比較評価するため、次のような他の構成法によるMH符号についてもN_4の値を求めた。

(i)　拡大ハミング符号のパリティ検査行列の列ベクトルのうち、$b(\beta)$の小さいものからn列使う場合
(ii)　(i)で値の大きいものからn列使う場合
(iii)　HSIAOが例示したMH符号[2]
(iv)　短縮化巡回符号

表1に示したように、(i), (ii)のMH符号は、ここでとりあげたどの符号長の場合も良くない符号である。これらの符号は、$\#(\bar{S})$がmより小さい。本稿の結果では一般にSのランクが低い場合には良い符号が見つけられていない。(iv)については、既約多項式を生成多項式とする短縮化巡回符号のなかで、最適な符号に対するN_4の値とその生成多項式の係数の8進数表現したものを表に示した。その結果によると、最適またはこれに近い良

好な符号が得られている。一般に短縮化巡回符号については、どの生成多項式を使うかによりいくつかのMH符号が考えられるが、いずれの生成多項式を使う場合も比較的良好なMH符号が求められた。

また(1)のMH符号と本稿で求めた最良のMH符号について、それらに対する P_{e3} と P_{e4} を、式(2)から求めて表2に示した。特に符号長72については、両者のMH符号の重み分布と式(1)により、p に対する P_e の確率を計算し表3に示した。

表1　最良のMH符号および他の構成法によるMH符号との比較

符号長	情報点数	次数	マスク数	マスクパターン	N_4	他の構成法による N_4			
						(i)	(ii)	(iii)	(iv)
18	12	5	14	1,2,3,4,5,8,10,13,16,20,26,28,30,31	102	148	148	—	(75) 102
22	16	5	10	1,2,3,4,5,8,10,16,20,26	250	263	261	252	(45) 250
39	32	6	25	1,2,3,4,6,8,12,15,16,19,24,27,28,29,32, 33,38,46,50,52,54,55,56,59,61	1335	1583	1579	1363	(155) 1338
43	36	6	21	1,2,3,4,6,8,12,15,16,24,30,31,32,34,35, 38,47,53,54,55,61	2009	2146	2138	—	(147) 2017
55	48	6	9	1,2,3,4,8,12,16,32,48	5589	5603	5599	—	(155) 5589
72	64	7	56	1,3,7,9,11,12,14,19,22,23,29,32,33,34,35, 37,38,44,47,49,51,52,55,58,59,62,64,65,66, 68,69,77,79,85,86,93,94,95,96,99,100,101,102, 104,106,107,110,111,113,115,117,118,122, 123,124,125	8175	11326	11319	8392 8404	(271) 8179

(注)　( )内は生成多項式の係数の8進数表現である.

表2　P_{e3}, P_{e4} についての比較

符号長	P_{e3} (%)		P_{e4} (%)	
	(a)	(b)	(a)	(b)
18	50.00	72.55	3.33	4.84
22	64.94	68.31	3.42	3.60
39	58.43	69.29	1.62	1.92
43	65.12	69.56	1.63	1.74
55	85.21	85.43	1.64	1.64
72	54.83	75.96	0.79	1.10

(a)　表1のマスクパターンのMH符号

(b)　(i)のMH符号

表3　符号長72の符号の誤って復号する確率

誤り確率	すぐれた符号のPe	(i)の Pe
10^{-2}	$.168 \times 10^{-1}$	$.232 \times 10^{-1}$
10^{-3}	$.305 \times 10^{-4}$	$.423 \times 10^{-4}$
10^{-4}	$.325 \times 10^{-7}$	$.450 \times 10^{-7}$
10^{-5}	$.327 \times 10^{-10}$	$.453 \times 10^{-10}$
10^{-6}	$.327 \times 10^{-13}$	$.453 \times 10^{-13}$

第7章　結論

本稿に示した方法により、適当な計算時間内で最適なMH符号を探索した結果、符号長22および55のクラスについては最適なMH符号、符号長18，39，43および72のクラスについては最適であるという保証はないがすぐれた符号が求められた。またこれらの実際に求められたMH符号の評価のため、他のいくつかの構成法により得られたMH符号についてのN_4の値が示されている。

Sの要素の個数からmを減じた数があまり大きくなければ、適当な時間内ですべての必要なマスクパターンをつくすことができるが、この数が増加すると、第3章で示したように所要時間が急激に大きくなり、最適なMH符号を求めることが困難となる。しかし本稿で示した方法により、すぐれた符号が比較的能率良く求められたことから、本方法は、たとえば文献(2)のようにSとして適当な条件を持つ良いMH符号を求める問題にも有効であろう。

文　献

(1) R. W. Hamming : "Error detecting and error correcting codes", Bell Syst. Tech. J., vol. 29, pp. 147-160 (1950).

(2) M. Y. Hsiao : "A Class of Optimal Minimum Odd-Weight-column SEC-DED Codes", IBM J., 14, p. 395 (1970).

(3) 岩垂 : "誤り制御符号 [I]", 信学誌, 55, 12, p. 1608 (昭47-201).

(4) 三瀬, 山本, 岡本, 都築 : "ハミング符号の誤り検出の一評価法", 昭48 信学全大, 1410.

(5) E. R. Berlekamp : "Algebraic coding theory", MacGraw Hill, New York (1968).

(6) W. W. Peterson and E. J. Weldon, Jr., : "Error-correcting Codes", edition 2, M.I.T. Press, Cambridge, Mass. (1972).

(7) F. J. MacWilliams : "A theorem on the distribution of weights in a systematic code", Bell Syst. Tech. J., vol. 42, pp. 79-94 (1963).

(8) C. G. Bell and A. Newell : "Computer Structures : Readings and Examples", p. 44, MacGraw Hill, New York (1971).

結　　論

各編の新しい諸結果はそれぞれの結論ですでにまとめられているので繰り返さず、ここでは今後に残された問題について若干ふれる。

今後さらに大きい符号長のRM符号の重み分布を求める問題がある。当面の目標となるものとして、自己双対符号であるRM(512, 4)と、互いに双対な符号であるRM(512, 3), RM(512, 5)があり、本論文と同様のPlessの恒等式を使う方法で重み分布を求めるとすれば、前者ではあと4次で重み2.5dおよび2.625dの符号語数が必要となる。後者では3次および5次で重み2.5d, 2.5625d, 2.625dの符号語数を求めるか、あるいは3次の重み構造がかなり複雑になると予想されるため、5次の分布式を大きく拡張して方程式の未知数を減少させ、3次の重み分布式の範囲を補う方法が考えられる。

重み2.5d以上の代表多項式については、現在ほとんど未知である。まず重み2.5dの代表多項式が必要となるが、$M_{m,r,2^{m-r+1}+2^{m-r-1}}$の値は大部分素因数2の数が他の重みのものより小さい。これはおのおののm, rについて複数個の代表多項式が存在することを予想させることから、今後必要となる代表多項式を求めることは必ずしも容易ではないと思われる。

アフィン同値類の数え上げや第2編の探索の問題は、いわゆる組合せ的な問題で、これを機械計算で行う場合には場合の数が指数的に増大することが問題である。本研究の場合では、理論的な手段を効果的に使い、場合の数を比較的小さい数におさえた後機械計算によりいくつかの結果を得ているが、この種の問題のかぎは、良いア

ルゴリズムにより場合の数を大きく減少させることが第1であり、次に言語およびデータ構造の工夫が必要である。第2編において、Sの数が大きい場合には、場合の数がかなり多くなり今後に問題を残している。短縮化巡回符号から良好な結果を得ているが、この理論的な解明などいくらかこの問題の手がかりになるのではないだろうか。また最適の保証が得られなかった符号のクラスについても、今後プログラムや言語などの工夫により最適性の確認の可能性がある。

謝　辞

本研究の全過程を通じて、直接理解ある御指導を賜わり、常に励ましていただいた嵩忠雄教授に心から深謝する。

大学院過程において、御指導御教示いただいた情報工学科の藤沢俊男教授、田中幸吉教授、木澤誠教授、ならびに制御工学科の桜井良文教授、坂和愛幸教授、辻三郎教授に対し厚く御礼申し上げる。

本研究において直接御指導いただいた都倉信樹助教授に深く感謝する。

講義などにおいて御教示いただいた的場裕司助教授、豊田順一助教授、志村正道助教授に厚く感謝する。

また筆者の所属する嵩研究室の藤井護講師、谷口健一助手、細見輝政助手、ならびに神戸商船大学中村圭二郎助教授、当情報工学科吉田信夫助手の御助言、御鞭撻に対し厚く感謝する。

学友の奥井順氏、菊野亨氏とは、日頃より議論し励ましあってきた。また本研究において、菊川（小畠）和子氏、藤枝公子氏，曽貝清美氏、西原明子氏をはじめ嵩研究室の諸氏には種々の面で御援助いただいた。ここに記して感謝の意を表する次第である。