



Title	リードマラー符号の重み分布式及び最適な修正ハミング符号に関する研究
Author(s)	山村, 三朗
Citation	大阪大学, 1975, 博士論文
Version Type	VoR
URL	https://hdl.handle.net/11094/859
rights	
Note	

The University of Osaka Institutional Knowledge Archive : OUKA

<https://ir.library.osaka-u.ac.jp/>

The University of Osaka

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

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ー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ー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 ミ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
(リードミラー符号の重み $2.5d$ 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

山村三郎

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）に在学中嵩研究室において行つ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をまとめられている。

第1編第3章は、 $GF(2)$ の上の n 变数で t 次以下の多項式の集合に含まれる重み $2^{n-t+1} + 2^{n-t-1}$ 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 2^d 以上 2.5^d 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示している。

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	4
第1編 リードマラー符号の重み分布式	9
第1章 序言	9
第2章 準備	10
第3章 多項式の特性づけと代表多項式	14
第4章 多項式の教え上げ	20
第5章 重み分布式の導出	31
第6章 結論	49
文献	50
第2編 最適な修正ハミング符号	53
第1章 序言	53
第2章 準備	55
第3章 マスクパターンの発生	58
第4章 重み4の符号語数の計算	63
第5章 符号探索法	65
第6章 求められた符号	67
第7章 結論	71
文献	72
結論	73
謝辞	75

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求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)を中心にもとめられていく。

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) 穴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きた。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つ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2.5の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、計算機組織などによる複雑になりつ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より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、復号化に要する金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、いくつの符号長に

ついて最適あるの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, 守積
"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, 守積
"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, 守積
"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 $2.5 d_{\min}$ 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 $2.5 d$ of Reed-Muller Codes", Rept. of Faculty of Eng. Sci., Osaka Univ. (June 1974).

- (7) 宇積, 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) 宇積, 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。近年になって、リード マラー符号^{(1),(2)}(以下、RM符号といふ)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 5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たした^{(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 $RM(2^m, r)$ とおく。このとき情報点数 ℓ は

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

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、 $f(x_1, \dots, x_m) \in P_r$ に対して、 $f(a_1, \dots, a_m) = 1$ となるような $GF(2)$ の上の m 次元ベクトル (a_1, \dots, a_m) の個数を f の重みといい、 $|f|_m$ とおく。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

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

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

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 变換という）である。多項式 f を A 变換で多項式 g に変換できることを、 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 を不变に保つ A 变換で、独立な一次式を加え込む操作を R 变換という。たとえば、 $f = x_1 x_2$ に関して $x_2 \rightarrow x_1 + x_2 + 1$ という変換は f を不变に保つ R 变換である。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 ℓ 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

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

を不变に保つ A 変換

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

を T 変換といふ。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。 γ 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。 m 個の一次式 x_1, \dots, x_m に対し、このうちで一次独立な個数を $\#(x_1, \dots, x_m)$ と表わす。 $f \in P_r$ の中の独立な n 個の一次式 u_1, \dots, 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、 $f \in P_{r,z}$ の必要十分条件は

$$f = xg + yh + zy k, \quad x, y \in P_1,$$

$g, h \in P_{r-1}$, $k \in P_{r-2}$ 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、今までに知られてゐる主な性質で、以後の議論に必要なもの ^{(3), (4), (15)} をあげる。

[補題 1] $\gamma (\neq 0)$ が次の様に 2通りに表されたとする。

$$f = x_1 \cdots x_i g(x_{i+1}, \dots, x_m)$$

$$= y_1 \cdots y_j h(y_{j+1}, \dots, y_m)$$

ただし、 $\#(x_1, \dots, x_m) = \#(y_1, \dots, y_m) = m$ で。

y_1, \dots, y_m は x_1, \dots, 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

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

[補題2] $r \geq 3$ のとき

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

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

このとき

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

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

[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。

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

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

1.1) $|f|_m = 2^{m-1} - 2^{m-1-l}$ ($\text{または } 2^{m-1} + 2^{m-1-l}$)

となる必要十分条件は

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

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

となることである。ただし、 x_1, \dots, x_{2l} は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

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

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

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

$|f|_m$ は

$$2^{m-r+1} - 2^{m-r-l},$$

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

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

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

または

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

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え。

[定理1] $f \in P_r$ のつ $|f|_m < 2^{m-r+1} + 2^{m-r-1}$ 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、 $\#(x_1, \dots, x_7) = 7$ 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。

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

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

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

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

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

と仮定すると、補題3により、次の場合のみになる。

$$(i) |g|_{m-2} = 2^{m-r-1}, |h|_{m-2} = 2^{m-r} - 2^{m-r-s},$$

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

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

$$|g+h+k|_{m-2} < 2^{m-r}.$$

g と h 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 2 つ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 h 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らる必要がない。これらの条件の下で代表多項式を求めることができるので、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

$$|f|_m = 2^{m-2} + 2^{m-6} \text{ かつ}$$

$$f \approx x_1 x_2 x_3 + x_4 (x_5 x_6 + x_7 x_8)$$

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かめる。

* 証明は文献(20)に詳しく述べられていく。

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} (10.010ld)	(1) $x_1 x_2 x_3 + x_4 x_5 x_6 + x_7 x_8 x_9$
$2^{m-r+1} + 2^{m-r-2}$ + 2^{m-r-3} (10.011d)	(2) $x_1 (x_2 x_3 + x_4 x_5) + x_6 (x_7 x_8 + x_9 x_2)$
$2^{m-r+1} + 2^{m-r-2}$ + $2^{m-r-3} + 2^{m-r-4}$ (10.0111d)	(3) $x_1 x_2 x_3 + x_4 x_5 x_6 + x_7 (x_8 x_9 + x_1 x_4)$ (4) $x_1 (x_2 x_3 + x_4 x_5) + x_6 (x_7 x_8 + x_9 x_{10})$
$2^{m-r+1} + 2^{m-r-1}$ - $2^{m-r-s+3}$ (10.01...ld) $\underbrace{s-2}_{s-2}$	(5) $x_1 x_2 x_3 + x_4 (x_2 x_5 + x_3 x_6 + x_7 x_8 + \dots + x_{2s+1} x_{2s+2})$ ($s \geq 4$) (6) $x_1 x_2 x_3 + x_4 (x_3 x_5 + x_6 x_7 + \dots + x_{2s+2} x_{2s+3})$ ($s \geq 3$)
$2^{m-r+1} + 2^{m-r-1}$ - $2^{m-r-s+1} + 2^{m-r-s-1}$ (10.01...ld) $\underbrace{s-2}_{s-2}$	(7) $x_1 x_2 x_3 + x_4 (x_5 x_6 + \dots + x_{2s+3} x_{2s+4})$ ($s \geq 3$)
$2^{m-r+1} + 2^{m-r-1}$ - 2^{m-r-s} (10.01...ld) $\underbrace{s-1}_{s-1}$	(8) $x_1 x_2 x_3 + x_4 ((x_3+1)x_5 + x_6 x_7 + \dots + x_{2s+2} x_{2s+3})$ ($s \geq 3$) (9) $x_1 x_2 x_3 + x_4 (x_1 x_5 + x_2 x_6 + x_3 x_7 + x_8 x_9 + \dots + x_{2s+2} x_{2s+3})$ ($s \geq 3$)
$2^{m-r+1} + 2^{m-r-1}$ - $2^{m-r-s-1}$ (10.01...ld) \underbrace{s}_{s}	(10) $x_1 x_2 x_3 + x_4 (x_5 x_6 + \dots + x_{2s+3} x_{2s+4} + x_1)$ ($s \geq 3$)
2^{m-r+1} (10d)	(11) $x_1 x_2 \dots x_r + (x_1+1)x_{r+1} \dots x_{2r-1}$
$2^{m-r+1} + 2^{m-r-2}$ + 2^{m-r-3} (10.011d)	(12) $x_1 x_2 x_3 x_4 + x_5 (x_3 x_6 x_7 + x_4 x_8 x_9)$ (13) $x_1 x_2 x_3 x_4 + x_5 x_6 (x_3 x_4 + (x_2+1)x_7 + x_8 x_9)$ (14) $x_1 x_2 x_3 x_4 + x_5 (x_3 x_6 x_7 + (x_4+x_7)x_8 x_9)$ (15) $x_1 x_2 x_3 x_4 x_5 + x_6 x_7 (x_3 x_4 x_8 + x_2 (x_5+x_8)x_9)$
$2^{m-r+1} + 2^{m-r-2}$ + $2^{m-r-3} + 2^{m-r-4}$ (10.0111d)	(16) $x_1 x_2 x_3 x_4 + x_5 (x_4 x_6 x_7 + x_8 x_9 x_{10})$ (17) $x_1 x_2 x_3 x_4 + x_5 x_6 (x_3 x_4 + x_7 x_8 + x_9 x_{10})$ (18) $x_1 x_2 x_3 x_4 x_5 + x_6 x_7 (x_3 x_4 x_8 + (x_5+x_8)x_9 x_{10})$
$2^{m-r+1} + 2^{m-r-1}$ - 2^{m-2r+3} (10.01...ld) $\underbrace{r-4}_{r-4}$	(19) $x_1 \dots x_r + x_{r+1} \dots x_{2r-2} (x_{r-3} x_{r-2} + x_{r-1} (x_r+1))$ ($r \geq 6$) (20) $x_1 \dots x_r + x_{r+1} \dots x_{2r-2} (x_{2r-1} (x_r+1) + x_{r-2} x_{r-1})$ ($r \geq 5$)

表1 つづき

$2^{m-r+1} + 2^{m-r-1}$ -2^{m-2r+2} $(10.\underbrace{01\cdots 1}_{r-3}d)$	(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} $(10.\underbrace{01\cdots 1}_{r-2}d)$	(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) $x_1 \cdots x_r + x_{r+1} \cdots x_{2r-2} (x_{2r-1} x_{2r} + x_{2r+1} (x_r + 1))$
$2^{m-r+1} + 2^{m-r-1}$ $-2^{m-2r+3} + 2^{m-2r+1}$ $(10.\underbrace{01\cdots 1}_{r-4}01d)$	(26) $x_1 \cdots x_r + x_{r+1} \cdots x_{2r-2} (x_{2r-1} x_{2r} + x_{r-1} x_r)$ ($r \geq 5$)
$2^{m-r+1} + 2^{m-r-1}$ $-2^{m-2r+2} + 2^{m-2r}$ $(10.\underbrace{01\cdots 1}_{r-3}01d)$	(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, \dots は互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

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

となる变数 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、そのような变数 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

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

または

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

という形をしています。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、 $f_{x_i=a}$ はより小さな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

$$\mu'(f) = \mu(f) \tag{5}$$

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、いくつも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試である。しかし必ずしも一見して互いに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を不变に保つ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)を求れば良い。そのためには、各代表多項式fに対して

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

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、2つとも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2つは

$$f = xg + yh + xyk, \quad g, h \in P_{r-1}, k \in P_{r-2},$$

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、すなはち 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認す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 (PDP 11/20) 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ひる 2 つの補題を示す。

[補題 4] $r \geq 4$ で

$$\begin{aligned} f &= x_1 \cdots x_r + x_{r+1} \cdots x_{2r-l} p \\ &= y_1 \cdots y_r + y_{r+1} g \end{aligned}$$

とし、次の条件が成立すると仮定する。

1) もし $2 < l < r$ ならば

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

で、もし $l = 2$ 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 $y_1, \dots, y_r, y_{r+2}, \dots, y_m$ ($m > r$) 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 $r-l-1$ 以上である。

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

$$\#(x_1, \dots, x_{2r-l}) = 2r-l,$$

$\ell > 2$ のとき

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

$\ell = 2$ のとき

$$\begin{aligned} \#(x_{r+1}, \dots, x_{2r-\ell}, z_1, \dots, z_{2s}) \\ = r + 2(s - 1) \end{aligned}$$

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

4) もし $\ell > 3$ かまたは $r = s = 2$ のとき

$$\#(x_1, \dots, x_{2r-\ell}, z_1, \dots, z_\ell) \geq r + 3,$$

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

かつ $\ell = 2$ 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) $x_1 \cdots x_r = y_1 \cdots y_r,$

$$x_{r+1} \cdots x_{2r-\ell} p = y_{r+1} g$$

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

B) $x_1 = z_\ell = y_{r+1},$

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

$$x_1 \cdots x_r + x_{r+1} \cdots x_{2r-\ell} z_1 \cdots z_\ell = y_{r+1} g$$

ただし、 $\ell = 2$ 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。

$$f = x_1 x_2 x_3 + x_4 p$$

$$= y_1 y_2 y_3 + y_4 g$$

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

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

ただし、1) $s \geq 3$, 2) $\#(x_4, z_1, \dots, z_{2s+1}) =$

$2s + 2$, 3) $\#(x_1, x_2, x_3, x_4, z_{2i-1}, z_{2i}) \geq 5$

($1 \leq i \leq s$) かつこれらは p に関する任意の T

変換のもとに保たれる, 4) $x_1, \dots, x_4, z_1, \dots, z_{2s+1}, u_1, \dots, u_{2t+1}$ は独立変数 y_1, \dots, 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。

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

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

$$\underbrace{(x_3 + 1) x_5 + x_6 x_7 + \dots}_{S \text{ 項}}$$

$$\sim a_1 y_2 y_3 + a_2 y_1 y_3 + a_3 y_1 y_2 + y_1 y_5 + y_2 y_6 \\ + y_3 y_7 + \dots$$

$$\begin{aligned} &= y_1 (y_5 + a_2 y_3) + y_2 (y_6 + a_3 y_1) \\ &\quad \underbrace{+ y_3 (y_7 + a_1 y_2)}_{S+1 \text{ 項}} + y_8 y_9 + \dots \end{aligned}$$

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 $\Gamma(f)$ したがい $N(f)$ を求められた。

I(子)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} ($1 \leq i \leq m$, $0 \leq j \leq r$) 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、それからの係数の組による 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。必要に応じ不变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し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

$$y_1 \cdots y_r = x_1 \cdots x_r, \quad (8.1)$$

$$\begin{aligned} y_{r+1} \cdots y_{2r-2} (y_{r-3} y_{r-2} + y_{r-1} (y_r + 1)) \\ = x_{r+1} \cdots x_{2r-2} (x_{r-3} x_{r-2} + x_{r-1} (x_r + 1)). \end{aligned} \quad (8.2)$$

補題1により

$$y_{r+1} \cdots y_{2r-2} = x_{r+1} \cdots x_{2r-2}. \quad (8.3)$$

(8.1), (8.3) により

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

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

$$\begin{vmatrix} a_{11} & \cdots & a_{1r} \\ \vdots & & \vdots \\ a_{ri} & \cdots & a_{rr} \end{vmatrix} = 1, \quad \begin{vmatrix} a_{r+1,r+1} & \cdots & a_{r+1,2r-2} \\ \vdots & & \vdots \\ a_{2r-2,r+1} & \cdots & a_{2r-2,2r-1} \end{vmatrix} = 1.$$

もし $1 \leq i \leq r$ に付し $x_i = 1$ ならば $y_i = 1$ ($1 \leq i \leq r$) となるので、

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

同様に

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

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} ($r < i \leq 2r-2, 0 \leq j \leq 2r-2$) 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

$$a_{ij} = 0 \quad (r-3 \leq i \leq r, 1 \leq j \leq r-3) \quad (8.6)$$

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} ($r-3 \leq i \leq r, 0 \leq j \leq 2r-2$) 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

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

である。したがって

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

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_{10} は省略する。

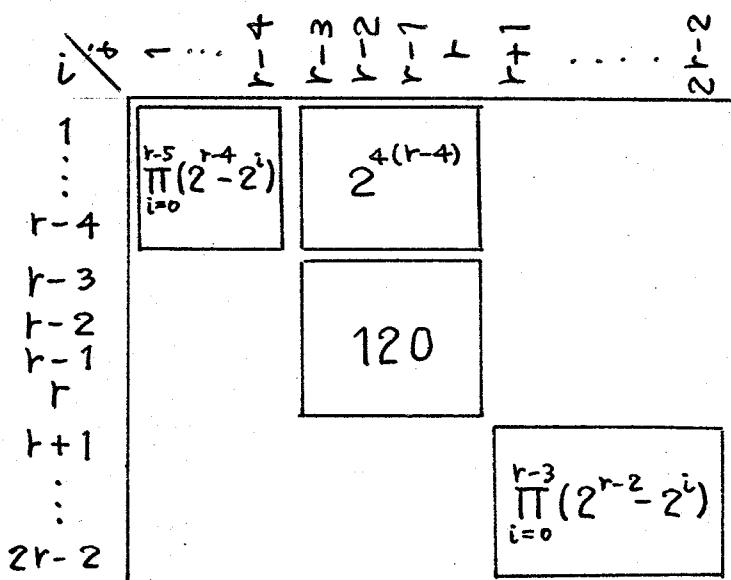


図1. No.19の係数行列の数

(例2.) No. 6

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

補題5により

$$y_4 = x_4,$$

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

$$b_1, b_2, b_3 \in GF(2) \quad (9.1)$$

である。これより

$$\begin{aligned}
 & (y_3 y_5 + y_6 y_7 + \cdots + y_{2s+2} y_{2s+3})_{x_4=1} \\
 & = b_3 (x_1 x_2 + b_1 x_2 + b_2 x_1 + b_1 b_2) + (b_1 x_2 + b_1 x_1 + x_5 \\
 & + b_1 b_2) x_3 + x_6 x_7 + \cdots + x_{2s+2} x_{2s+3}. \quad (9.2)
 \end{aligned}$$

両辺の項数の関係から $b_3 = 0$. また

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

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

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

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

(9.1) 式において $x_1 = \bar{b}_1, x_2 = \bar{b}_2, x_3 = x_4 = 1$ とする

と $a_{34} = 0$. したがって

$$y_3 = x_3.$$

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

$$\begin{aligned}
 & y'_6 y'_7 + y'_8 y'_9 + \cdots + y'_{2s+2} y'_{2s+3} \\
 & = x_6 x_7 + x_8 x_9 + \cdots + x_{2s+2} x_{2s+3} \quad (9.3)
 \end{aligned}$$

となり、これが式(9.1)

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

また

$$\begin{aligned}
 (y_{2i} y_{2i+1})_{x_4=1} & = y'_{2i} y'_{2i+1} \\
 & + (a_{2i,3} y'_{2i+1} + a_{2i+1,3} y'_{2i} + a_{2i,3} a_{2i+1,3}) x_3
 \end{aligned}$$

であるが、(9.2) 式と (9.3) 式により

$$\begin{aligned}
 (y_5)_{x_3=1, x_4=1} & = b_2 x_1 + b_1 x_2 + b_1 b_2 + x_5 \\
 & + \sum_{i=3}^{s+1} (a_{2i,3} y'_{2i+1} + a_{2i+1,3} y'_{2i} + a_{2i,3} a_{2i+1,3}).
 \end{aligned}$$

a_{i3}, a_{i4} ($5 \leq i \leq 2s+3$) は任意に選択できるので、

a_{ij} ($5 \leq i \leq 2s+3, 0 \leq j \leq 2s+3$) 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 変換で不变

に係たれる数である。 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

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

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

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、 $y_6 y_7 + \cdots + y_{2s+2} y_{2s+3}$ を不变に保つ 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 につけては

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

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

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

となり、全体では

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

となる。

$i \setminus j$	1	2	3	4	5	6	\cdots	$2s+3$
1	$3 \cdot 2$	2^2	2^2					
2				1				
3								
4				1				
5			2	2	1		2^{2s-2}	
6								
\vdots								
$2s+3$								B_{s-1}

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

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

$$y'_i = (y_i)_{x_1=0} \quad (1 \leq i \leq 2r-1) \text{ とおくと}$$

$$\#(y'_1, y'_2, \dots, y'_{2r-1}) = 2r-2,$$

$$\begin{aligned} & y'_1 y'_2 \cdots y'_r + (y'_1 + 1) y'_{r+1} \cdots y'_{2r-1} \\ & = x_{r+1} \cdots x_{2r-1}. \end{aligned}$$

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

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

$a_{10} = 0$ とするとき

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

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

したがって

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

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

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

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

$$\left| \begin{array}{ccc} a_{22} & \cdots & a_{2r} \\ \vdots & \ddots & \vdots \\ a_{rr} & \cdots & a_{rr} \end{array} \right| = 1, \quad \left| \begin{array}{ccc} a_{r+1,r+1} & \cdots & a_{r+1,2r-1} \\ \vdots & \ddots & \vdots \\ a_{2r-1,r+1} & \cdots & a_{2r-1,2r-1} \end{array} \right| = 1.$$

これらの方を満たす a_{ij} ($2 \leq i \leq 2r-1$) 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

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

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
10.010ld	(1)	35	1	2	-	-	1	1	1	1
10.011ld	(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
10.01...1d s-2	(5)	$2^{s^2+3s+2} \cdot \beta_{2s+2}$	/	$3 \cdot \gamma_{s-2}$						
	(6)	$2^{s^2+5s+2} \cdot \beta_{2s+3}$	/	$3 \cdot \gamma_{s-1}$						
10.01...1d s-1	(8)	$2^{s^2+5s+4} \cdot \beta_{2s+3}$	/	$3 \cdot \gamma_{s-1}$						
	(9)	$2^{s^2+3s+6} \cdot \beta_{2s+3}$	/	$3 \cdot 7 \cdot \gamma_{s-2}$						
10.01...1d s	(10)	$2^{s^2+7s+7} \cdot \beta_{2s+4}$	/	$3 \cdot \gamma_s$						
10.01...10ld s-2	(7)	$2^{s^2+7s+7} \cdot \beta_{2s+4}$	/	$3 \cdot 7 \cdot \gamma_s$						
10d	(11)	$2^{r^2-1} \cdot \beta_{2r-1}$	/	β_{r-1}^2						
10.01...1d r-4	(19)	$2^{r^2+1} \cdot \beta_{2r-2}$	/	$3 \cdot 5 \cdot \beta_{r-4} \cdot \beta_{r-2}$						
	(20)	$2^{r^2+r-2} \cdot \beta_{2r-1}$	/	$3 \cdot \beta_{r-3} \cdot \beta_{r-2}$						
10.01...1d r-3	(21)	$2^{r^2+r} \cdot \beta_{2r-1}$	/	$3 \cdot \beta_{r-3} \cdot \beta_{r-2}$						
	(22)	$2^{r^2+2r-2} \cdot \beta_{2r}$	/	β_{r-2}^2						
	(23)	$2^{r^2+3r} \cdot \beta_{2r+1}$	/	$3 \cdot \beta_{r-2} \cdot \beta_{r-1}$						
10.01...1d r-2	(24)	$2^{r^2+2r} \cdot \beta_{2r}$	/	$3 \cdot \beta_{r-2}^2$						
	(25)	$2^{r^2+3r} \cdot \beta_{2r+1}$	/	$3 \cdot \beta_{r-2} \cdot \beta_{r-1}$						
10.01...10ld r-4	(26)	$2^{r^2+2r} \cdot \beta_{2r}$	/	$3^2 \cdot \beta_{r-2}^2$						
10.01...10ld r-3	(27)	$2^{r^2+4r+4} \cdot \beta_{2r+2}$	/	$3^2 \cdot 5 \cdot \beta_{r-2} \cdot \beta_r$						

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

$$\begin{aligned} f \in P_{r,1} \\ f \in P_r \\ |f|_m = w \\ (N_{m,r,w}) \end{aligned} \left\{ \begin{array}{l} f \in P_{r-1} \\ f \notin P_{r,1} \\ (N'_{m,r,w}) \end{array} \right\} \left\{ \begin{array}{l} \mu(f) < m \\ \mu(f) = m \\ (M_{m,r,w}) \end{array} \right\}$$

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113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。

$$\begin{aligned} N'_{m-r+2, 2, 2^{m-r+1}} &= N_{m-r+2, 2, 2^{m-r+1}} - (1\text{次式の数}) \\ &= 2 \left\{ 2^{\frac{(m-r+2)(m-r+3)}{2}} - 2^{m-r+2} \right. \\ &\quad \left. - \sum_{l=1}^{\lfloor \frac{m-r+2}{2} \rfloor} 2^{l(l+1)} \prod_{i=1}^l (2^{m-r+4-2i} - 1) (2^{m-r+3-2i} - 1) \right. \\ &\quad \left. / (4^i - 1) \right\} \end{aligned}$$

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、次のように書きかえられる。

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

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) 式を使ひ次のように計算できる。

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

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

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 とする二元統形符号について、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。

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

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

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 $N_{2,3,2^6}$ 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。

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

であり、また $N_{5,3,2^3}, N_{6,3,2^4}, N_{7,3,2^6}$ は求められて
 いる^{(16), (3), (5)}ので、 $M_{i,3,2^{i-2}} \quad (5 \leq i \leq 7)$ 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 $N_{8,3,2^6}$ が求まる。よって連立一次
 方程式を一意に解けて、重み分布が求まる。あわせて、
 ニの重み分布から双対符号 RM (256, 4) の重み分布
 が、MacWilliams の恒等式を用い求められる。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
 と (14), (15) 式により、 $M_{m,r,w} \quad (m \leq 8, 2 \leq r \leq 5, w \leq 2^{m-1})$ が求まる。この結果を表 5 に示す。^{(3), (5), (7)}

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

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

したがって、補題 3-1) により

$$w \equiv 0 \pmod{2^{m-r-1}}$$

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、 $M_{m,r,w} \quad (m \geq 9, r \geq 3)$ は表 5 で同じ $m, r,$
 w を持つ多項式の $N(\chi)$ の和として求まる。

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
 み分布式が導びられる。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 $M_{m,r,w}$ を求める計算では總符

* 「 $\lceil x \rceil$ 」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るので、剰余計算を利用していふ。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	304296714240
64 192	74984804718940
68 188	707415842488320
72 184	28055013884190720
76 180	764244915168215040
80 176	20661827603503720320
84 172	414411510493363568640
88 168	6266131517201901649920
92 164	71773299826457585909760
96 160	627671543662325464743336
100 156	4208997665316969256058880
104 152	21729945674277436342763520
108 148	86666254361102444207800320
112 144	267788217345284850768843520
116 140	642477460725187489919139840
120 136	1198959833392658891791089664
124 132	1742452898879489085360046080
128	1973540804513554426870962630

表4. RM(256, 4) の重み分布

重み	符号語数
0	256
16	240
24	232
28	228
30	226
32	224
34	222
36	220
38	218
40	216
42	214
44	212
46	210
48	208
50	206
52	204
54	202
56	200
58	198
60	196
62	194
64	192
66	190
68	188
70	186
72	184
74	182
76	180
78	178
80	176
82	174
84	172
86	170
88	168
90	166
92	164
94	162
96	160
98	158
100	156
102	154
104	152
106	150
108	148
110	146
112	144
114	142
116	140
118	138
120	136
122	134
124	132
126	130
128	128

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	$13^2 \cdot 10399$
	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	13·41 ² ·269·571·821·9833·77041
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・53
	11	13	1			1		13^2
	13	7		1	1			41・61
	15	7				1		11・13・997
6 8	15	2		3		1		
	10	14	2	1	1			883
	12	13	2		2			28621
	14	12	2		1			*
	16	11	5	2	1			178093
	18	13	2	1	2			*
	20	16	2		1			*
	22	10	3		1			653 *
	24	9	2	1	1			11 *
	26	10	2	1	2			*
	28	8	4		1			11^2 *
	30	10	3		2			19 *
	32	9	8		1	2		19 *
7 10	21	1		2		1	1	
	12	19	1		1		1	23・173
	14	19	1		1		1	309059
	16	18	1		1		1	439・76441
	18	17	1		1		1	89・163・188369
	20	16	2		1		1	11 *
	22	16	1		1		1	*
	24	14	1		2		1	*
	26	15	1		1		1	*
	28	14	1		1		1	*
	30	14	1		1		1	11 *
	32	14	1		1		1	*
	34	14	1		1		1	19・89 *
	36	15	1	1	2	1	1	29・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. $2^{m-r+1} \leq w < 2^{m-r+1} + 2^{m-r-1}$ の重み分布式

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

$$\begin{aligned}
 &= 2^{r-1} \cdot \alpha_{m,r-1} \\
 &+ 2^{r-1} \cdot (2^{(m-r+2)(m-r+3)/2} - 2^{m-r+2} - \sum_{\ell=1}^{\lfloor m-r+2/2 \rfloor} 2^{\ell(\ell+1)} \prod_{i=1}^{\ell} (2^{m-r+4-2i} - 1) \\
 &\quad (2^{m-r+3-2i} - 1)/(4^i - 1)) \cdot \alpha_{m,r-2} \\
 &+ 2^{r+5} \cdot 5 \cdot 7 \cdot 31 \cdot (\alpha_{m-r+3,5} + 2^2 \cdot 3^3 \cdot 7 \cdot \alpha_{m-r+3,6} + 2^7 \cdot 3^2 \cdot 7 \cdot 127 \cdot \alpha_{m-r+3,7}) \cdot \alpha_{m,r-3} \\
 &+ 2^{r+10} \cdot 3^2 \cdot 7 \cdot 31 \cdot (\alpha_{m-r+4,6} + 2 \cdot 5 \cdot 7 \cdot 127 \cdot \alpha_{m-r+4,7}) \cdot \alpha_{m,r-4} \\
 &+ \sum_{k=4}^r 2^{r+k^2-k-1} \cdot \beta_{m-r+k} \cdot \alpha_{m,r-k} / \beta_{k-1}^2
 \end{aligned}$$

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

$$\begin{aligned}
 &= 2^{r-2} \cdot N_{m-r+2,2,2^{m-r+1}+2^{m-r-3}} \cdot \alpha_{m,r-2} \\
 &+ 2^{r+22} \cdot 3^2 \cdot 5 \cdot 7 \cdot 17 \cdot 31 \cdot 127 \cdot \alpha_{m-r+3,8} \cdot \alpha_{m,r-3} \\
 &+ 2^{r+19} \cdot 3 \cdot 5^2 \cdot 7^2 \cdot 17 \cdot 31 \cdot 127 \cdot \alpha_{m-r+4,8} \cdot \alpha_{m,r-4}
 \end{aligned}$$

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

$$\begin{aligned}
 &= 2^{r-2} \cdot N_{m-r+2,2,2^{m-r+1}+2^{m-r-2}} \cdot \alpha_{m,r-2} \\
 &+ 2^{r+11} \cdot 3 \cdot 7 \cdot 31 \cdot (7 \cdot 23 \cdot \alpha_{m-r+3,6} + 2^2 \cdot 5 \cdot 127 \cdot 661 \cdot \alpha_{m-r+3,7} \\
 &\quad + 2^6 \cdot 5^2 \cdot 7^2 \cdot 13 \cdot 17 \cdot 127 \cdot \alpha_{m-r+3,8} + 2^{12} \cdot 3 \cdot 5 \cdot 7^2 \cdot 17 \cdot 73 \cdot 127 \cdot \alpha_{m-r+3,9}) \cdot \alpha_{m,r-3} \\
 &+ 2^{r+15} \cdot 3 \cdot 7^2 \cdot 31 \cdot 127 \cdot (3^2 \cdot 5 \cdot \alpha_{m-r+4,7} + 2^3 \cdot 17 \cdot 19 \cdot 53 \cdot \alpha_{m-r+4,8} \\
 &\quad + 2^9 \cdot 3 \cdot 5^2 \cdot 17 \cdot 73 \cdot \alpha_{m-r+4,9}) \cdot \alpha_{m,r-4} \\
 &+ 2^{r+23} \cdot 3 \cdot 5 \cdot 7 \cdot 17 \cdot 31 \cdot 127 \cdot (11 \cdot \alpha_{m-r+5,8} + 3 \cdot 5 \cdot 7 \cdot 73 \cdot \alpha_{m-r+5,9}) \cdot \alpha_{m,r-5}
 \end{aligned}$$

表6 つづき

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

$$\begin{aligned}
 &= 2^{r+32} \cdot 3 \cdot 5 \cdot 17 \cdot 31 \cdot 73 \cdot 127 \cdot (5 \cdot \alpha_{m-r+3,9} + 2^2 \cdot 7 \cdot 11 \cdot 31 \cdot \alpha_{m-r+3,10}) \cdot \alpha_{m,r-3} \\
 &+ 2^{r+32} \cdot 3 \cdot 7^2 \cdot 11 \cdot 17 \cdot 31^2 \cdot 73 \cdot 127 \cdot \alpha_{m-r+4,10} \cdot \alpha_{m,r-4} \\
 &+ 2^{r+30} \cdot 3^2 \cdot 5^2 \cdot 7 \cdot 11 \cdot 17 \cdot 31^2 \cdot 73 \cdot 127 \cdot \alpha_{m-r+5,10} \cdot \alpha_{m,r-5}
 \end{aligned}$$

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

$$\begin{aligned}
 &= 2^{r+21} \cdot 3 \cdot 5 \cdot 7^2 \cdot 17 \cdot 31 \cdot 127 \cdot (2 \cdot 463 \cdot \alpha_{m-r+3,8} + 3 \cdot 11 \cdot 73 \cdot 317 \cdot \alpha_{m-r+3,9} \\
 &+ 2^6 \cdot 3^2 \cdot 7 \cdot 11 \cdot 31 \cdot 73 \cdot \alpha_{m-r+3,10} + 2^{14} \cdot 11 \cdot 23 \cdot 31 \cdot 73 \cdot 89 \cdot \alpha_{m-r+3,11}) \cdot \alpha_{m,r-3} \\
 &+ 2^{r+24} \cdot 3 \cdot 5 \cdot 7 \cdot 17 \cdot 31 \cdot 127 \cdot (3 \cdot 181 \cdot \alpha_{m-r+4,8} + 2^2 \cdot 5 \cdot 7 \cdot 41 \cdot 73 \cdot \alpha_{m-r+4,9}) \cdot \alpha_{m,r-4} \\
 &- + 2^{r+24} \cdot 3^2 \cdot 5 \cdot 7 \cdot 17 \cdot 31 \cdot 73 \cdot 127 \cdot (5 \cdot 7 \cdot 23 \cdot \alpha_{m-r+5,9} + 2^4 \cdot 3^2 \cdot 5 \cdot 11 \cdot 31 \cdot \alpha_{m-r+5,10} \\
 &+ 2^{11} \cdot 11 \cdot 23 \cdot 31 \cdot 89 \cdot \alpha_{m-r+5,11}) \cdot \alpha_{m,r-5} \\
 &+ 2^{r+31} \cdot 3^2 \cdot 7 \cdot 11 \cdot 17 \cdot 31^2 \cdot 73 \cdot 127 \cdot (7 \cdot \alpha_{m-r+6,10} + 2^3 \cdot 5 \cdot 23 \cdot 89 \cdot \alpha_{m-r+6,11}) \cdot \alpha_{m,r-6}
 \end{aligned}$$

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

$$\begin{aligned}
 &= 2^{r+31} \cdot 3 \cdot 7^2 \cdot 31 \cdot 73 \cdot 127 \cdot (2 \cdot 5^2 \cdot 7 \cdot 17 \cdot \alpha_{m-r+3,9} + 2^3 \cdot 11 \cdot 17 \cdot 31 \cdot 47 \cdot \alpha_{m-r+3,10} \\
 &+ 5 \cdot 11 \cdot 17 \cdot 23 \cdot 31 \cdot 73 \cdot 89 \cdot \alpha_{m-r+3,11} + 2^8 \cdot 3^2 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 23 \cdot 31 \cdot 89 \\
 &\cdot \alpha_{m-r+3,12} + 2^{18} \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 23 \cdot 31 \cdot 89 \cdot 8191 \cdot \alpha_{m-r+3,13}) \cdot \alpha_{m,r-3} \\
 &+ 2^{r+32} \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 17 \cdot 31^2 \cdot 73 \cdot 127 \cdot 139 \cdot \alpha_{m-r+4,10} \cdot \alpha_{m,r-4} \\
 &+ 2^{r+29} \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 17 \cdot 31^2 \cdot 73 \cdot 127 \cdot (5^2 \cdot 11 \cdot \alpha_{m-r+5,10} \\
 &+ 2^6 \cdot 23 \cdot 89 \cdot \alpha_{m-r+5,11}) \cdot \alpha_{m,r-5}
 \end{aligned}$$

表 6 つづき

$$\begin{aligned}
 & + 2^{r+36} \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 17 \cdot 23 \cdot 31 \cdot 73 \cdot 89 \cdot 127 \cdot (31 \cdot \alpha_{m-r+6, 11} \\
 & + 2^4 \cdot 3^2 \cdot 7 \cdot 13 \cdot 31 \cdot \alpha_{m-r+6, 12} + 2^{12} \cdot 3 \cdot 7 \cdot 13 \cdot 8191 \cdot \alpha_{m-r+6, 13}) \cdot \alpha_{m, r-6} \\
 & + 2^{r+43} \cdot 3^3 \cdot 5 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 23 \cdot 31 \cdot 73 \cdot 89 \cdot 127 \cdot (3 \cdot \alpha_{m-r+7, 12} \\
 & + 2^4 \cdot 8191 \cdot \alpha_{m-r+7, 13}) \cdot \alpha_{m, r-7}
 \end{aligned}$$

(g) $N_{m, r, 2}^{m-r+1} + 2^{m-r-1} - 2^{m-r-k-1}$ ($w = 10.01 \dots ld$, $m-r-\lceil m/r \rceil \geq k > 4$)

$$\begin{aligned}
 & = 2^{r+k^2+5k+7} \cdot \beta_{m-r+3} \cdot (1/3 \cdot 7 \cdot \gamma_{k-1} + 2^{2k-3} \cdot 41/3 \cdot \gamma_k + 2^{4k+6}/3 \cdot \gamma_{k+1}) \cdot \alpha_{m, r-3} \\
 & + 2^{r+k^2+5k+6} \cdot \beta_{m-r+k+2} \cdot (1/3 \cdot \beta_k^2 + 2^{k+2}/3 \cdot \beta_k \cdot \beta_{k+1}) \cdot \alpha_{m, r-k-2} \\
 & + 2^{r+k^2+6k+9} \cdot \beta_{m-r+k+3} \cdot (1/3 \cdot \beta_k \cdot \beta_{k+1} + 2^{k+1}/\beta_{k+1}^2 + 2^{2k+6}/3 \cdot \beta_{k+1} \cdot \beta_{k+2}) \\
 & \cdot \alpha_{m, r-k-3} \\
 & + 2^{r+k^2+7k+13} \cdot \beta_{m-r+k+4} \cdot (1/3 \cdot 5 \cdot \beta_k \cdot \beta_{k+2} + 2^{k+1}/3 \cdot \beta_{k+1} \cdot \beta_{k+2}) \cdot \alpha_{m, r-k-4}
 \end{aligned}$$

(h) $N_{m, r, 2}^{m-r+1} + 2^{m-r-1} - 2^{m-r-k-1} + 2^{m-r-k-3}$ ($w = 10.01 \dots ld$, $m-r-\lceil m/r \rceil - 2 \geq k \geq 2$)

$$\begin{aligned}
 & = 2^{r+k^2+11k+22} \cdot \beta_{m-r+3} \cdot \alpha_{m, r-3} / 3 \cdot 7 \cdot \gamma_{k+2} \\
 & + 2^{r+k^2+9k+22} \cdot \beta_{m-r+k+3} \cdot \alpha_{m, r-k-3} / 3^2 \cdot 5 \cdot \beta_{k+1} \cdot \beta_{k+3} \\
 & + 2^{r+k^2+9k+20} \cdot \beta_{m-r+k+4} \cdot \alpha_{m, r-k-4} / 3^2 \cdot \beta_{k+2}^2
 \end{aligned}$$

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

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

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

$[x]$ 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おり、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 $M_{m,r,w}$ ($m \leq 8$, $2 \leq r \leq 5$, $w \leq 2^{m-1}$) も示されており、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. Ienaga, N. Tokura and T. Kasami : "Weight Distribution of (128, 64) Reed-Muller Code", ibid., vol. IT-17 (Sept. 1971).
- (6) 尚, 都倉, 安積 : "Reed-Muller 符号の重み分布について", 信学会イシホナ理研資, 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 $2.5d$ 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單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符号といふ）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、ベクトル成分の適當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 のなみの列 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、できるだけトヨリ P_e を持つ MH 符号を組織的に能率良くさぐす方法について考察していく。

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变に保たれていく。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 \bar{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 と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。よく知られてるようない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 符号のクラスの中で最小の N_4 を持つ符号を最適な符号とよぶことにする。 N_4 が求めれば、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。

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

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、 $m-2$ 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 \leq 次以下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、

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

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

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

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

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

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

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

であり、その双対符号は 1 次のリード・マラー符号で

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

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ことする。（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と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 個成分を除去した符号の拡大符号にはならない。

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、 $i_1 < i_2 < \dots < i_{n-1}$ とし

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

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

とかき、 \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 S の要素の数を l とおくことにすると

$$l = 2^m - n$$

である。

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

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、 \dots 、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

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

を $EH(S)$ とおく。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 $S = \{A_{i_1}, A_{i_2}, \dots, A_{i_{n-1}}\}$ に対して

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

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

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

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

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

* 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)

$l < 2^{m-1}$ くれゆえ、 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1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, \dots, e_i で張られる V_m の部分空間を $V_m^{(i)}$ とおく。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, \dots, e_t を含み、残りが $V_m^{(t)}$ の重み ≥ 1 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 $\sum_{t=1}^m \binom{2^t - 1 - l}{t-1}$ に減少する。

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

$$\text{ただし、 } v_i = e_i \quad (1 \leq i \leq t)$$

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 $v = (a_1, a_2, \dots, a_m)^T$ の部分ベクトル $(a_i, a_{i+1}, \dots, a_k)^T$ 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、 $v_{t+1}, v_{t+2}, \dots, v_l$ 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: $w(v_{t+1}) \leq w(v_{t+2}) \leq \dots \leq w(v_\ell)$.

条件2: $w(v_j) = w(v_{j+1}) = \dots = w(v_{j'})$
を満たすベクトルに対しては

$b(v_j) < b(v_{j+1}) < \dots < b(v_{j'})$ であると.

すなわち、11くつから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, \dots, v_ℓ の並び替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11くつの連続する成分が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、11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、 $m=7$, $\#(\bar{S})=6$ 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	\dots	v_6	v_7	v_8	v_9	v_{10}	\dots
1	1	0		0	1	0	1	1	
2	0	1		0	1	0	1	0	
3	0	0	\ddots	0	0	1	1	1	
4	0	0	\ddots	0	0	1	0	1	
5	0	0	\ddots	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、 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 $[A_0, A_1, \dots, A_{2^m-2}]$ の最後の連続する l 個の列ベクトルを選んで、

$$\bar{S} = \{A_{2^m-l-1}, A_{2^m-l}, \dots, A_{2^m-2}\}$$

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。 $\{p_1, p_2, \dots, p_L\}$ を 2^m-1 と素な 2^m-2 以下の正整数で、かつどの2つの p_i, p_j ($i \neq j$)についても

$$p_i \equiv p_j \pmod{2^m-1}, \quad 0 \leq i < m$$

の関係が成り立たないような最大集合とすると、 $\alpha^{p_1},$

$\alpha^{p_2}, \dots, \alpha^{p_L}$ 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 S から次の L 個

$$\{ A_{f_i}(2^m - l - 1), A_{f_i}(2^m - l), \dots, A_{f_i}(2^m - 2) \}, \\ 1 \leq i \leq L$$

をとればよい。ただし添字は $\text{mod } (2^m - 1)$ で考える。

第4章 重みの符号語数の計算

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ことを考える。 $EH(S)$, $H(S)$ の重み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、 $0 \leq i \leq n$ に対して

$$\begin{aligned} N_i &= N'_{i-1} + N'_i & i: \text{偶数} \\ N_i &= 0 & i: \text{奇数} \end{aligned} \quad \} \quad (4)$$

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、 $2^{m-1} < n \leq 2^m$ により、 $m \geq 5$ では $2^{n-m-1} \gg 2^m$ 。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 $\bar{S} = \{A_{j_1}, A_{j_2}, \dots, A_{j_e}\}$ に対して、第 j_1+1 成分、第 j_2+1 成分、…、第 j_e+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。

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

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、…、第 j_e+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。 $l < 2^{m-1}$ ゆえに、 $H(S)$ の各行は互いに一次独立である。

以上から、 $H^d(S)$ の重みの符号語数を 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 l ビット巡回シフトして得られるベクトルを

$C^d g_1$ とする。

[補題3] $C^d g_1 \cdot h(S)$ のなみで、重み $i (> 0)$ である μ の個数は M_i に等しい。ただし、 $0 \leq \mu < 2^m - 1$ で、 \cdot はビット毎の AND 操作を表す。

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)

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

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

上式は一オ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。

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

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

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

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

上式と式(4)により $EH(S)$ の重み分布が決まる。符号の評価を重み μ の符号語数をもとにを行うので、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。すなむち、 v_{t+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七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_i について、 $v_i(j, \rho)$ の成分がすべて 1 で、かつ $v_i(\rho, t)$ がすべて 0 である最小の j 、および ρ をそれぞれ $0(v_i)$ 、 $\epsilon(v_i)$ とする。 $V_m^{(t)}$ 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 $V_m^{(t)}$ 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 $\epsilon(v_i) + 1 \geq 0(v)$ を満足する最初のベクトル v を v_{i+1} とし、第 $j+1$ 番目の列ベクトルとしてこの v を選択したこと記憶して、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りた最大長系列を、巡回シフトしそれをマスクをして $H^d(S)$ 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、剩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剩余計算を行った。

計算時間は、 m ととも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な 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。次にこのうちでトータル N_4^* を与える \bar{S} の一つから、 $U(\bar{S})$ を作り $\text{mod}(2^m - 1)$ 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 FACOM 230-45S 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々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、 b_i の各要素 b_i の値 b_i を10進数で表現したもののが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_i の小さいものから順列使う場合
- (ii) (i) で値の大きいものから順列使う場合
- (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、井(5)よりも小さく、本稿の結果では一般によるランクが低い場合には良い符号が見つからない。(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用う場合も比較的良好的なMH符号が求められた。

また(i) 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、 ρ 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

件数 長 点数	情報 次 数	2スラ 数	2スラ ハ ⁰ 9 - ノ	N ₄	他の構成法による N ₄		
					(i)	(ii)	(iii)
18	12	5	14	1, 2, 3, 4, 5, 8, 10, 13, 16, 20, 26, 28, 30, 31	102	148	148
							(75)
22	16	5	10	1, 2, 3, 4, 5, 8, 10, 16, 20, 26	250	263	261
							(45)
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
							(15)
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	209	2146	2138
							(147)
55	48	6	9	1, 2, 3, 4, 8, 12, 16, 32, 48	5589	5603	5599
							(155)
72	64	7	56	1, 3, 7, 9, 11, 12, 14, 19, 22, 23, 29, 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
							(271)
							8404
							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 P_e	(i) の P_e
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らの結論ですでにまとめられてるので繰り返さず、ここでは今後残された問題について若干ふれる。

今後さらに大きめ符号長の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いえば、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を考えられる。

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。これはおののののの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ところから、今後必要となる代表多項式を求めるに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か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、良りア

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、 λ の数が大きい場合には、場合の数が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かどうか。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梅井良文教授、坂和慶幸教授、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教授、当情報工学科吉岡信夫助手の御助言、御鞭撻に對し厚く感謝する。

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（小島）和子氏、藤枝公子氏、曾貝清美氏、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。