原始リード-ソロモン符号およびＪｕｓｔｅｓｅｎ符号の集合族内における2元重み分布多項式のクラス分け

遠藤, 寿之 / ENDO, Kazuyuki

(出版者 / Publisher)
法政大学
(発行年 / Year)
2009-03-24
(学位授与年月日 / Date of Granted)
2009-03-24
(学位名 / Degree Name)
修士(理学)
(学位授与機関 / Degree Grantor)
法政大学 (Hosei University)

2008年度修士論文

原始リード - ソロモン符号およびJustesen符号の集合族内における2元重み分布多項式のクラス分け

指導教員 西島利尚

法政大学大学院
情報科学研究科 情報科学専攻

遠藤寿之

Master thesis2008

Classification of the Binary Weight Enumerators of Primitive Reed-Solomon Codes and Justesen Codes

Supervisor Toshihisa NISHIJIMA

Graduate School of Computer and Information Sciences
Hosei University

Kazuyuki ENDO

概要

符号化パラメータである最小距離は誤り訂正能力を評価する上で重要な値である．一部を除いて，線形符号の 2 元重み分布が陽に求められていないので，最小距離の特定も全探索による方法のみというのが現状である．

本研究では，研究対象を原始リード-ソロモン符号と外部符号にリード-ソロモン符号を持つ連接符号の一クラスである Justesen 符号に限定する．特に前者はその生成多項式より，集合族を成すことがわかっている．集合族内の符号はそれぞれ異なる集合であるから，集合族内において 2 元重み分布がどのように与えられるかを明らかにすることは未解決問題への糸口となる．よって，符号の集合族内における 2 元重み分布多項式のクラス分けを行うことで，集合族内の代数的な性質を明らかにすることを目的とする．

キーワード リード-ソロモン符号，Justesen 符号，2 元重み分布多項式，完全重み分布多項式，生成多項式

Abstract

Since the generalized Reed-Solomon codes are Maximum Distance Separate codes, these Hamming Weight Distribution is already given explicitly. In addition to, for the ensemble of binary expanded of the generalized Reed-Solomon codes, average binary weight distribution is already given too. However, there is no progress in the research which values ability of the generalized Reed-Solomon codes. Therefore, it is necessary to find the beginning of the structure of the ensemble or binary weight enumerators of Reed-Solomon codes. Because it is very difficult to get explicitly binary weight enumerators of any linear block codes, the problem of analytically getting binary weight enumerators of primitive Reed-Solomon codes remains as the outstanding problem. In order to search for the beginning of this solution, we specify the ensemble of primitive Reed-Solomon codes with the same binary weight enumerators by using structure of the generator polynomial of these codes in this paper. In addition, we specify the ensemble of Justesen codes with the same binary weight enumerators by using these property of the primitive Reed-Solomon codes.

Key words Reed-Solomon Codes, Justesen Codes, The Binary Weight Enumerators, The Complete Weight Enumerators, Generator Polynomial

目 次

1　序論

この章では，符号理論において重要である概念や符号の諸性質について記す.

1.1　符号化

符号化とは情報伝送時に，ある目的を達成する為の技術である．情報伝送を行うときの送りたい情報を情報源と呼び，それをある規則に従って写像した集合を符号と呼ぶ．特に，その集合の要素を符号語と呼ぶ．そして，多種多様な通信路によりそれら符号語は伝送される．このときの通信路は ADSL や光ファイバ等の伝送路やメモリ，ハードディスク等の記憶媒体などが考えられる．このような通信路において，伝送効率あるいは信頼性向上を考慮して符号を構成することを符号化という.

通信路は物理的なものであるから，通信に時間的な限界が存在したり，送信した情報にひずみや雑音が付加されることも考えられる．それらの除去を目的として符号化が行われるので，伝送効率を目的とする場合と信頼性向上を目的とする場合では符号化の操作が異なる．前者は情報源符号化と呼ばれ，情報源から冗長性を除去することで実現される．後者は通信路符号化と呼ばれ，情報源に冗長性を付加することで実現される．これら符号化の逆操作として復号があり，符号から情報源への逆写像として定義されている.

しかし，伝送時の目的を実現する一方で，損失も発生している．情報源符号化の場合，復号による信頼性低下が考えられる．同様に，通信路符号化の場合は伝送効率の低下が考えられる．これらはトレードオフの関係となっており，状況に応じた符号化パラメータの設定が必要である.

1.2　誤り訂正符号

情報源に対して冗長性を付加することで，通信路において付加される誤りの訂正を行うことができる．この操作により，情報伝送時の信頼性向上に繋がることから，この用途で構成される符

号を特別に誤り訂正符号とよぶ．また情報源を情報記号と呼び，そのベクトル長を k とする．次にそれら情報記号を誤り訂正符号に写像したベクトルの長さを n とおくと，$n > k$ であり，$n-k$ を検査記号数という．この検査記号数が冗長性となり，この値を大きく取ることによって非常に信頼性の高い符号を構成できる．一方で伝送効率が悪くなってしまうことから，誤り訂正個数と検査記号数の適当な組合せを見つける問題は非常に重要なテーマとなっている．

1.3 線形符号

数学的な取り扱いの良さから誤り訂正符号は線形符号であることが多い．すなわち，情報記号系列を線形部分空間のベクトルと捉え，線形写像により符号を構成する．ただし，符号語ベクトルは有限体 $GF(q)$ 上のシンボルであるとする．有限体上のベクトルにおいて注意しなければならない点は，加算演算の結果であるシンボルを陽に特定できないことである．実際，この性質により解析の進まない未解決問題が存在している．

1.4 ハミング距離

線形符号は線形部分空間を成すから，距離の定義が可能である．特に，符号語間の距離は符号の誤り訂正能力を解析する上で非常に重要なパラメータとなる．2 つのベクトル v_m と $v_{m'}$ のハミング距離は,

$$D_H(v_m, v_m^{'}) = \sum_{i=1}^{n} d_H(v_{mi}, v_{m'i}), \tag{1}$$

$$d_H(a,b) = \begin{cases} 0 & , a_i = b_i \\ 1 & , a_i \neq b_i \end{cases} \tag{2}$$

で定義される．すなわち，任意の符号語間のハミング距離はその符号語間の異なる要素の総数で定義される．次に，ハミング距離と同様の概念であるハミング重みを以下のように与える．長さ n の系列 $\boldsymbol{u} = (u_1, u_2, \cdots, u_n)$ に対して,

$$w_H(\boldsymbol{u}) = d_H(\boldsymbol{u}, \boldsymbol{0}), \tag{3}$$

と与えられる値をハミング重みとよぶ．式 (3) より，ハミング重みは線形部分空間の零元を基準とした距離であるということがわかる．

1.5　誤り訂正符号による訂正個数

符号 C において，任意の異なる符号語間のハミング距離の最小値 $d_{\min}$ を考える．この値は線形部分空間に存在するベクトル間において最も近い距離であるから，

$$d_{\min} = \min_{\boldsymbol{v_i},\boldsymbol{v_j}\in C,\boldsymbol{v_i}\neq\boldsymbol{v_j}} d_H(v_i, v_j), \tag{4}$$

で定義され，最小ハミング距離あるいは最小距離と呼ばれる．すなわち，最小距離は線形部分空間内の最小重みを有するベクトルの存在を示している．よって，最小重みが $d_{\min}$ であるから $t = \lfloor \frac{d_{min}-1}{2} \rfloor$ 個の誤りを訂正することができる．符号の訂正個数に関する最小距離あるいは最小重みは能力の評価において重要な役割を果たすことがわかる．

2　リード-ソロモン符号

本研究の対象となる符号の 1 つである原始リード-ソロモン符号に関する諸性質を以下に記す. この符号は代数的に整った生成多項式を持つので，良く研究されている符号の 1 つである．研究対象だけではなく，CD や記憶装置などの実用製品にも適用され，幅広く利用されている.

2.1　巡回符号と最大距離分離符号

線形符号でかつその符号語のシンボルを巡回置換した系列もまた符号語であるような符号を巡回符号と呼ぶ．巡回符号はその代数的な性質より良く研究された符号である．次に巡回符号の一クラスである最大距離分離符号を以下のように定義する．(n, k, d)[1]線形符号 C において,

$$d = n - k + 1, \tag{5}$$

を満たす符号を最大距離分離符号とする.

2.2　符号化パラメータ

$GF(2^m)$ 上の (n, k, d) リード-ソロモン符号は,

$$n = 2^m - 1, \tag{6}$$

$$0 < k \leq 2^m - 1, \tag{7}$$

$$d = n - k + 1 \tag{8}$$

を満足する符号長 n，情報記号数 k，最小距離 d を持つ [**?**].

2.3　原始リード-ソロモン符号の定義

巡回符号かつ最大距離分離符号である $GF(q)$ 上の (n, k, d) 原始リード - ソロモン符号 C を次のように定義する [1]．ただし，$q = 2^m$, m は 2 以上の整数とし，$n = q - 1$ とする．原始元 $\alpha \in$

[1]符号長 n，情報記号数 k，最小距離 d の線形ブロック符号を (n, k, d) 符号 C と記す.

$GF(q)$，d_0，d を任意の自然数とするとき，生成多項式 $G_{d_0}(x)$ が，

$$G_{d_0}(x) = (x - \alpha^{d_0})(x - \alpha^{d_0+1}) \cdots (x - \alpha^{d_0+d-2}), \tag{9}$$

で与えられる符号を原始リード - ソロモン符号と定義する．式 (9) より，原始リード-ソロモン符号を構成する生成多項式は自然数の数だけ存在していることになり，この原始リード-ソロモン符号は集合族を成すことがわかる．この集合族を成すという性質に本研究では着目している．

2.4 符号の等価性

2 つの異なる原始リード-ソロモン符号 C_1，C_2 において，以下の 2 つの操作により C_1 から C_2 あるいは C_2 から C_1 が構成できるとき，それらの符号は等価であるという．

1. 符号語のシンボルを巡回置換

2. 符号語全体の拡大縮小

3 Justesen 符号

この章では，リード-ソロモン符号を基に構成される Justesen 符号に関する諸性質を記す.

3.1 連接符号

2 つの異なる符号を用いて，符号化を 2 段階に分けることで構成される符号である．本研究で対象とする連接符号は外部符号に原始リード-ソロモン符号を持ち，内部符号に Wozencraft のランダムシフト符号を持つ可変内部符号化された連接符号の一クラスである Justesen 符号である．この符号は外部符号の各符号語シンボルに対して，すべて異なる内部符号器により符号化されるので，符号の最小距離を比較的簡単な処理で大きくすることができるという性質を持つ.

3.2 Wozencraft のランダムシフト符号

$GF(2^m)$ 上の生成行列 $G^{(i)} = [1|\alpha^i]$ で与えられる線形ブロック符号を $(2,1)$ ランダムシフト符号 $C^{(i)}$[1] と定義する．ただし，α，$1 \in GF(2^m)$ は，それぞれ原始元と乗法に関する単位元，そして m は任意の自然数を表す．また，$\mathcal{C} = \{C^{(i)} | i = 0, 1, \ldots, 2^m - 2\}$ で与えられる集合族をランダムシフト符号の集合族 $\mathcal{C}$ と定義する．ただし，$GF(2^m)$ 上の $(2,1)$ 符号 $C^{(i)}$ を 2 元に展開した符号は，$(2m, m)$ 符号 $C_b^{(i)}$ と記す.

3.3 Justesen 符号の構成法

kK ビットの 2 元情報記号を k 個の連続する K ビットに分割する．それぞれの K ビットを $GF(2^K)$ 上の元とみなし，$GF(2^K)$ 上の (n, k, d) リードソロモン符号 C の符号語として外部符号化する．このリードソロモン符号の符号語を長さ K のシンボルと捉え，ランダムシフト符号 C^i の符号語として内部符号化する．これらの符号語を連接して得られる符号を Justesen 符号と定義する [6].

[1] 符号長 n，情報シンボル数 k の線形符号を (n, k) 符号 C と記す.

4　重み分布

この章では，2 つの重み分布の定義を与える．そして，第 2 章 5 節で記した最小距離への議論を通じて未解決問題を紹介する．

4.1　2 元重み重み分布

式 (9) より構成される $GF(q)$ 上の (n, k, d) 原始リード - ソロモン符号 C を 2 元に展開して得られる $(nm, km, d^{'})$ 線形符号 C_b の 2 元重み分布および 2 元重み分布多項式を以下に定義する．$GF(q)$ 上の (n, k, d) 原始リード - ソロモン符号を 2 元に展開して得られる $(nm, km, d^{'})$ 線形符号 C_b において，重みが i の符号語の総数を A_i で表す．ただし，$i = 0, 1, \cdots, nm$ である．このとき，

$$\{A_0,\ A_1,\ A_2,\ \cdots,\ A_{nm}\},$$

が 2 元に展開された $(nm, km, d^{'})$ 原始リード - ソロモン符号 C_b の 2 元重み分布である．また，

$$A_{d_0}(z) = \sum_{i=0}^{nm} A_i z^i, \tag{10}$$

を 2 元重み分布多項式とする．この 2 元重み分布多項式が与えられればその符号の最小距離が陽にわかるため，符号の訂正能力を明らかにできる．

4.2　完全重み分布

集合 $I = *, 0, 1, \cdots, q-2$ とする．ただし, 記号 " $*$ " は, $\alpha^* = 0$ と定義する．このとき $GF(q)$ の原始元を α とすると, $\alpha^i \in GF(q), i \in I$ と表される．$GF(q)$ 上の (n, k, d) 一般化リードソロモン符号 c の完全重み分布多項式を $W_c[z]$ とすると,

$$W_c[z] = \sum_{v \in c} w_v[z], \tag{11}$$

である．ただし, $w_c[z]$ は符号語 $v \in c$ の完全重み分布多項式を示し, 符号語 v の s_i 個の成分が α^i

であるとき,

$$w_c[z] = \prod_{i \in I} z_i^{s_i}, \tag{12}$$

$$\sum_{i \in I} s_i = n \tag{13}$$

のように定義される.

4.3 未解決問題の整理と本研究のアプローチ

リード - ソロモン符号は最大距離分離符号の一クラスとして定義され，そのハミング重み分布はすでに解析的に与えられている [1]．更に，2 元に展開されたリード - ソロモン符号の集合族上に与えられる平均 2 元重み分布も解析的に求められている [2]．ところが，リード - ソロモン符号の能力を解析的に与える極めて重要でかつ本質的な完全重み分布，あるいは 2 元重み分布の研究には進展がない．依然として符号理論の中で，最も本質的な未解決問題として残されているのが現状である．特に，2 元重み分布多項式を求める問題は有限体のシンボル同士の加算結果をそのシンボルで陽に与えられないことに起因している．

ここで，符号を原始リード-ソロモン符号に限定する．この符号の場合は，式 (9) より集合族を成すことがわかっている．よって，この集合族内には訂正能力の異なる符号が線形部分空間として存在していることになる．すなわち，集合族内において 2 元重み分布多項式が等しくなるような部分集合族に分類できれば，誤り訂正能力を評価する最小距離の議論へ繋げることができる．将来的には，2 元重み分布多項式を直接求めずとも最小距離を陽に与えることができ，集合族内での訂正能力の順序付けが可能になる．

次章からは，原始リード-ソロモン符号と Justesen 符号に限定し，2 元重み分布多項式が等しくなるようなクラス分けを行う．

5　2元重み分布多項式のクラス分け1

この章では，原始リード-ソロモン符号 C の集合族すべてにおいて成り立つクラス分けを行う．符号を構成する生成多項式 $G_{d_0}(x)$ とその根に着目し，それらに関する3つの補題を示したあとに定理を導く．

5.1　クラス分けに関する補題1

補題 1 d_0 を任意の自然数とするとき，

$$G_{d_0}(x) = G_{d_0 \pmod n}(x), \tag{14}$$

である．

(証明)

$$\begin{aligned} G_{d_0 \pmod n}(x) &= (x - \alpha^{d_0 \pmod n})(x - \alpha^{d_0 \pmod n+1}) \cdots (x - \alpha^{d_0 \pmod n+d-2}), \\ &= (x + \alpha^{d_0 \pmod n})(x + \alpha^{d_0+1 \pmod n}) \cdots (x + \alpha^{d_0+d-2 \pmod n}), \\ &= (x - \alpha^{d_0})(x - \alpha^{d_0+1}) \cdots (x - \alpha^{d_0+d-2}) \end{aligned}$$

(証明終)

補題1は，n を法として合同な自然数により生成多項式が定義されるとき，それらの多項式は同一のものであるということを示している．

次に，原始リード-ソロモン符号の集合族内において2元重み分布多項式が等しくなるような部分集合族の特定に必要な補題を証明する．

5.2　クラス分けに関する補題2

補題 2 $GF(q)$ 上の生成多項式が式 (9) で与えられるとする．そして，この多項式 $G_{d_0}(x)$ の相反多項式 $G_{d_0'}(x)$ を考える．ただし，連続根そのものは変わらないものとする．このとき，$G_{d_0}(x)$

と $G_{d_0{}'}(x)$ が構成する原始リード-ソロモン符号は等価である．

(証明) 任意の生成多項式を式 (9) より，以下のように与える．

$$\begin{aligned} G_{d_0}(x) &= (x-\alpha^{d_0})(x-\alpha^{d_0+1})\cdots(x-\alpha^{d_0+d-2}), \\ &= \prod_{i=d_0}^{d_0+d-2}(x-\alpha^i) \end{aligned} \tag{15}$$

次に式 (15) の不定元と根をそれらの逆元に置き換えると，

$$(x^{-1}-\alpha^{-i}) = x^{-1}\cdot\alpha^{-i}\cdot(\alpha^i - x),$$

であることを用いて，

$$\begin{aligned} G_{d_0{}'}(x) &= \prod_{i=d_0}^{d_0+d-2}(x^{-1}-\alpha^{-i}), \\ &= \alpha^{-T}\cdot x^{-(d-1)}\cdot G_{d_0}(x) \pmod{x^n-1}, \\ G_{d_0}(x) &= \alpha^{T}\cdot x^{(d-1)}\cdot G_{d_0{}'}(x) \pmod{x^n-1} \end{aligned} \tag{16}$$

と変形できる．ただし，$T = \sum_{i=d_0}^{d+d_0-2} i$ である．したがって，$G_{d_0}(x)$ と $G_{d_0{}'}(x)$ が構成する原始リード-ソロモン符号は等価である．

(証明終)

補題 2 より集合族内の任意の生成多項式において，その不定元と根をそれらの逆元に置き換えた別の生成多項式が存在していることがわかる．またこの補題は，原始リード-ソロモン符号の集合族に関して $\frac{n}{2}$ 個の異なる 2 元重み分布多項式を持つ集合族であるということを示している．最後に，原始リード-ソロモン符号が等価となるための d_0' の条件を導く．

5.3 クラス分けに関する補題 3

補題 3 $d_0' = n+k-d_0+1 \pmod{n}$ のとき，$G_{d_0}(x)$ が構成する原始リード-ソロモン符号 C_{d_0} と $G_{d_0{}'}(x)$ が構成する原始リード-ソロモン符号 $C_{d_0'}$ は等価である．

(証明) 補題 2 より，原始リード-ソロモン符号 C_{d_0}，$C_{d_0'}$ が等価を満足するには，各々の生成多項式 G_{d_0}，$G_{d_0{}'}(x)$ が適当な重みを持つ相反多項式の関係を満たしている必要がある．よって，生成多項式の連続根に関して逆元を取った範囲から d_0' を求めることができる．$G_{d_0}(x)$ の連続根は，

$$d_0 \leq i \leq d_0 + d - 2 \pmod{n},$$

の範囲に存在しているので，$G_{d_0{}'}(x)$ の連続根は

$$(d_0 + d - 2)^{-1} \leq \quad i^{-1} \quad \leq {d_0}^{-1},$$

$$n + k - d_0 + 1 \leq \quad i^{-1} \quad \leq n - d_0 \pmod{n}$$

に存在している．自然数 d_0 は生成多項式の連続根の始まり位置であるから，

$$d_0' = n + k - d_0 + 1 \pmod{n}, \tag{17}$$

となる．

(証明終)

これらの補題より，以下の定理を得る．

5.4 クラス分けに関する定理 1

定理 1 自然数 d_0，d_0' により与えられる生成多項式 G_{d_0}，$G_{d_0{}'}(x)$ において，それらが構成する原始リード-ソロモン符号 C_{d_0}，$C_{d_0'}$ の 2 元重み分布多項式 $A_{d_0}(z)$，$A_{d_0{}'}(z)$ は以下を満たす．

$$A_{d_0}(z) \quad = \quad A_{d_0{}'}(z), \tag{18}$$

$$d_0{}' \quad = \quad n + k - d_0 + 1 \pmod{n} \tag{19}$$

また，それらの完全重み分布多項式も等しくなり，集合族内には異なる重み分布を持つ符号が高々 $\frac{n}{2}$ 個存在している．

□

(証明) 完全重み分布はその定義より，巡回による影響を受けない．すなわち，2 つの原始リード-ソロモン符号が等価であれば，定義 4 の 2 と式 (10) より各々の符号語シンボルは適当な重みにより拡大縮小された別のシンボル系列に写像されたものといえる．この写像において，完全重み分布に変更は生じないから 各々の原始リード-ソロモン符号の完全重み分布多項式は一致する．完全重み分布が一致すれば，2 元重み分布多項式も一致するので定理は成り立つ.

(証明終)

$GF(2^3)$ 上の $(7,3,5)$ 原始リード - ソロモン符号に対して，この定理 1 を適用し，原始多項式 $P(x) = x^3 + x + 1$ を用いた多項式基底による 2 元展開を行った際の 2 元重み分布多項式のクラス分けの例を付録 A に記す.

6　2元重み分布多項式のクラス分け2

第6章では原始リード-ソロモン符号の集合族すべてに対して成り立つ，2元重み分布多項式のクラス分けに関する定理を示した．この章では，集合族を限定して更に詳しいクラス分けに関する定理を示す．この章で示す定理より，定理1と同じ部分集合族へのクラス分けが可能であるということわかる．ただし，定理の証明において最小距離 d を奇数に限定しているという課題を残している．

6.1　クラス分けに関する補題4

補題 4 (n,k,d) 原始リード-ソロモン符号 C_{d_0} の生成多項式を $G_{d_0}(x)$，$C_{d_0'}$ の生成多項式を $G_{d_0{}'}(x)$ とおく．ただし，d が奇数のときに限定する．このとき，以下のように $G_{d_0{}''}(x)$ を定義すると，その生成多項式により構成される符号は C_{d_0} と同集合族内に存在している．ただし，$L(x)$ は $G_{d_0}(x)$ と $G_{d_0{}'}(x)$ の連続根を連結した高々 $2(d-1)$ 次の多項式であり，$K(x)$ は根に自身の逆元を持つ多項式である．

$$G_{d_0{}''}(x) = \frac{L(x)}{K(x)} \pmod{x^n-1}, \tag{20}$$

$$L(x) = G_{d_0}(x)\cdot G_{d_0{}'}(x), \tag{21}$$

$$K(x) = \prod_{i=d_0}^{\frac{d-1}{2}+d_0-1} (x-\alpha^i)(x-\alpha^{-i}) \tag{22}$$

□

(証明) $L(x)$ は連続根を持つと定義しているので，$2(d-1)$ 次の適当な連続根を持つ多項式を構成する．すなわち，

$$\begin{aligned} L(x) &= G_{d_0}(x)\cdot G_{d_0{}'}(x), \\ &= (x-\alpha^{d_0})(x-\alpha^{d_0+1})\cdots(x-\alpha^{n-d_0}), \\ &= (x-\alpha^{d_0})\cdots(x-\alpha^{d_0''})\cdots(x-\alpha^{n-d_0}), \\ &= \Big[\prod_{i=d_0}^{\frac{d-1}{2}+d_0-1}(x-\alpha^{i})(x-\alpha^{-i})\Big]\cdot G_{d_0''}(x) \end{aligned}$$

と変形できる．ただし，新たに構成された連続根の始まり位置を d_0'' とする．よって，$K(x)$ を式 (22) のように定義することで同一集合族内に存在する原始リード-ソロモン符号を構成する生成多項式を新たに定義できる．次に，$G_{d_0}{}''(x)$ が $d-1$ 次の多項式になっていることを確認する．

$$\begin{aligned} \deg L(x) &= 2(d-1), \\ \deg K(x) &= d-1 \end{aligned}$$

より，

$$\deg G_{d_0}{}''(x) = \deg L(x) - \deg K(x) = d-1,$$

したがって，$G_{d_0}{}''(x)$ は高々 $d-1$ 次の多項式で，連続根を持つことから (n,k,d) 原始リード-ソロモン符号 C_{d_0} と同集合族に属している符号 $C_{d_0''}$ を構成する生成多項式である．

(証明終)

補題 4 は定理 1 を満たす原始リード-ソロモン符号を構成する生成多項式から，それらと同一な集合族に含まれる符号を構成する生成多項式を導くことができるということを示している．ただし，最小距離 d を奇数に限定している点に注意しなければならない．次に，その特定条件 d_0，d_0'' に関する補題を導く．

6.2　クラス分けに関する補題 5

補題 5 $d_0 = n + \dfrac{2k-n+1}{2} \pmod n$ を満たす d_0 において，$d_0^{''} = \dfrac{d-1}{2} + d_0 \pmod n$ のとき，補題 4 は成り立つ．

□

(証明) $L(x)$ が連続根を持つ為には，式 (17) と

$$d_0^{'} - 1 = n + d + d_0 - 2 \pmod n$$

を同時に満たさねばならない．よって，

$$\begin{aligned} d + d_0 - 1 &= n + k - d_0 + 1, \\ d_0 &= n + \frac{2k-n+1}{2} \pmod n \end{aligned}$$

を得る．このとき，$d_0^{''}$ は $L(x)$ の連続根の中心から求めることができるので，

$$\begin{aligned} d_0^{''} &= \frac{2(d-1)}{2} - \frac{(d-1)}{2} + d_0, \\ &= d_0 + \frac{d-1}{2} \pmod n \end{aligned}$$

で与えられる．これらの条件のときに補題 4 が成り立つ．

(証明終)

補題 4 と 5 より，以下の定理を得る．

6.3 クラス分けに関する定理 2

定理 2 自然数 d_0，d_0'' により与えられる生成多項式 G_{d_0}，$G_{d_0''}(x)$ において，それらが構成する原始リード-ソロモン符号 C_{d_0}，$C_{d_0''}$ の 2 元重み分布多項式は以下のときに等しくなる．

$$A_{d_0}(z) = A_{d_0''}(z), \tag{23}$$

$$d_0 = n + \frac{2k - n + 1}{2} \pmod{n}, \tag{24}$$

$$d_0{}'' = \frac{d-1}{2} + d_0 \pmod{n} \tag{25}$$

となる．ただし，定理 1 とは異なり完全重み分布多項式の一致は保障されない．

□

(証明) 式 (20) より，

$$L(x) = K(x) \cdot G_{d_0''}(x) \pmod{x^n - 1}, \tag{26}$$

も原始リード-ソロモン符号を構成する生成多項式の 1 つである．ここで巡回符号は $GF(q)$ 上のモニック多項式環の剰余類環のイデアル $I_{G_{d_0}}$ である [**?**] という性質を用いると，生成多項式 $G_{d_0''}(x)$ は巡回符号の一クラスである原始リード-ソロモン符号を構成するので，

$$L(x) = G_{d_0}(x) \cdot G_{d_0'}(x) \pmod{x^n - 1} \in C_{d_0}, \tag{27}$$

が成り立つ．また，式 (26) より，

$$K(x) \in R_{x^n - 1},$$

$$G_{d_0''}(x) \in C_{d_0''}$$

を利用して，

$$L(x) = K(x) \cdot G_{d_0''}(x) \pmod{x^n - 1} \in C_{d_0''}, \tag{28}$$

となる．式 (27) と式 (28) より，$L(x) \pmod{x^n-1}$ が構成する符号は C_{d_0} かつ $C_{d_0''}$ であることがわかる．次に，$K(x)$ は高々 $d-1$ 次の多項式であるから式 (28) に分配則を適用し，定理 1 を拡張する．すなわち，

$$\begin{aligned} L(x) &= K(x)\cdot G_{d_0''}(x) \pmod{x^n-1}, \\ &= \sum_{i=1}^{d-1}(\alpha_i x^i G_{d_0''}(x)) \pmod{x^n-1},\ \alpha_i \in GF(q) \end{aligned}$$

となり，$C_{d_0''}$ と等価な符号の符号語の線形結合によって定義される符号と考えることができる．$GF(q)$ 上の加算において，演算後のシンボル系列が陽に与えられていない為，完全重み分布多項式が等しくなることは一般的に言えないが，2 元重み分布多項式は一致する．

(証明終)

限定された集合族に対する 2 元重み分布多項式のクラス分けに関するこの定理 2 は最小距離 d が奇数であるという前提条件を与えた．符号の構成において，最小距離 d は生成多項式の最高次数を決定するという重要なパラメータである．d が奇数ならば，生成多項式は高々 $d-1$ 次の多項式として表現され，連続根の総数は偶数で与えられることになる．ここで，定理 2 を導く際に用いた式 (22) に関して，連続根の総数が奇数ならば $K(x)$ の定義上，$G_{d_0''}(x)$ の存在が保障されなくなる．よって，本定理に関しては d を奇数に限定して証明した．しかしながら，d が偶数においてもこの定理と同様に 2 元重み分布多項式が一致する集合族が存在しているため，検討の余地を残している．

$GF(2^3)$ 上の $(7,5,3)$ 原始リード-ソロモン符号および $GF(2^4)$ 上の $(15,2,14)$ 原始リード-ソロモン符号に対して，この定理 2 を適用し，原始多項式 $P(x)=x^3+x+1$ と原始多項式 $P(x)=x^4+x+1$ を用いた多項式基底による 2 元展開を行った際の 2 元重み分布多項式のクラス分けの例を付録 B に記す．定理 2 は最小距離を奇数に限定していたが，$(15,2,14)$ 原始リード-ソロモン符号においても適用範囲内であることを示している．

7　可変内部符号化された連接符号への拡張

これまでの考察を可変内部符号化された連接符号に適用することを考える．集合族内において，定理 1 あるいは定理 2 により同一クラスに分類される原始リード-ソロモン符号の生成多項式を，生成行列の要素とする Justesen 符号の構造に着目し，その集合族内において 2 元重み分布多項式のクラス分けを行う．

Justesen 符号はその構成法より，2 つのリードソロモン符号を連結した符号であると考えることができる．そこで，2 つのリードソロモン符号に分離させることで Justesen 符号の構造を明らかにし，原始リード-ソロモン符号の集合族に関する分類同様，Justesen 符号の集合族に関する分類の定理を与える．

7.1　クラス分けに関する補題 6

補題 6 Justesen 符号は以下の 2 つの生成多項式から構成される原始リードソロモン符号に分離することができ，更にそれら 2 つの符号は等価である．

$$
\begin{aligned}
&{G^{(\ell)}}_{d_0}(x) = (x-\alpha^{d_0})(x-\alpha^{d_0+1})\cdots(x-\alpha^{d_0+d-2}),\\
&{G^{(r)}}_{d_0}(x) = \alpha^{d-1}\cdot K\cdot {G^{(\ell)}}_{d_0}(x),\\
&K = \alpha^{d_0-1}+\alpha^{d_0+d-2}
\end{aligned}
\tag{29}
$$

□

(証明) Justesen 符号の生成多項式は内部符号であるランダムシフト符号の構成を考慮して，$[G_{d_0}(x), \alpha^i\cdot G_{d_0}(x)]$ と表現することができる．左側の生成多項式を基準としたとき，右側の生成多

項式は

$$\begin{aligned} {G^{(r)}}_{d_0}(x) &= {G^{(\ell)}}_{d_0}(\alpha x) \\ &= (\alpha x - \alpha^{d_0})(\alpha x - \alpha^{d_0+1}) \cdots (\alpha x - \alpha^{d_0+d-2}) \\ &= \alpha^{d-1} \cdot {G^{(\ell)}}_{d_0-1}(x) \\ &= \alpha^{d-1} \cdot \frac{(x - \alpha^{d_0+d-2})}{(x - \alpha^{d_0-1})} \cdot {G^{(\ell)}}_{d_0}(x) \\ &= \alpha^{d-1} \cdot K \cdot {G^{(\ell)}}_{d_0} \end{aligned} \tag{30}$$

とおける．${G^{(r)}}_{d_0}(x)$ は ${G^{(\ell)}}_{d_0}(x)$ を適当な重みだけ拡大縮小した多項式として表すことができるので等価である．

(証明終)

補題 6 は，Justesen 符号の生成多項式が原始リード-ソロモン符号の生成多項式より構成されるということを示している．

7.2 クラス分けに関する補題 7

補題 7 2 元重み分布多項式が同一クラスに分類されるような原始リード-ソロモン符号の生成多項式を要素に持つ Justesen 符号の生成行列 G_{J_1}，G_{J_2} を

$$\begin{aligned} G_{J_1} &= G_{d_0}(x) \begin{bmatrix} 1 & \alpha^{d-1}K \end{bmatrix}, \\ G_{J_2} &= G_{{d_0}^{(j)}}(x) \begin{bmatrix} (\alpha^{d-1}K)^{-1} & 1 \end{bmatrix} \end{aligned} \tag{31}$$

とする．このとき，これらの生成行列から構成される Justesen 符号は等価である．

(証明)

$$\begin{aligned} G_{J_2} &= G_{{d_0}^{(j)}}(x) \begin{bmatrix} (\alpha^{d-1}K)^{-1} & 1 \end{bmatrix} \\ &= (\alpha^{d-1}K)^{-1} G_{{d_0}^{(j)}}(x) \begin{bmatrix} 1 & \alpha^{d-1}K \end{bmatrix} \end{aligned}$$

式 (16) より，各々の生成行列から構成される Justesen 符号は等価である．

(証明終)

7.3 クラス分けに関する補題 8

補題 8 $d_0^{(j)} = d_0' + 1 \pmod n$ を満たす $d_0^{(j)}$ において，補題 7 は成り立つ．

□

(証明) 式 (31) より，

$$\begin{aligned} G_{d_0}(x) &= (\alpha^{d-1}K)^{-1} G_{d_0}{}^{(j)}(x) \\ &= \alpha^{-(d-1)} G_{d_0{}^{(j)}-1}(x) \end{aligned} \tag{32}$$

と変形できる．ここで，

$$(\alpha x - \alpha^{i+1}) = \alpha^{i+1} x(\alpha^{-i} - x)$$

であることを用いて，式 (32) を変形すると

$$G_{d_0{}'}(x) = \alpha^{-(d-1)} G_{d_0}(x)$$

となるので，

$$\begin{aligned} \alpha^{(d-1)} G_{d_0}(x) &= \prod_{i=d_0}^{d_0+d-2} (\alpha x - \alpha^{i+1}) \\ &= \prod_{i=d_0}^{d_0+d-2} \alpha^{i+1} x^{d-1} G_{d_0{}'}(x) \end{aligned}$$

より，$d_0^{(j)} = d_0' + 1 \pmod n$ となる．

(証明終)

これら 3 つの補題を用いて，定理 1 と同様に，Justesen 符号のクラス分けに関する定理を導く．

7.4　クラス分けに関する定理 3

定理 3 自然数 d_0，$d_0^{(j)}$ により与えられる生成行列 $G_{J_{d_0}}$，$G_{J_{d_0^{(j)}}}$ において，それらが構成する Justesen 符号 $C_{J_{d_0}}$，$C_{J_{d_0^{(j)}}}$ の 2 元重み分布多項式 $A_{J_{d_0}}(z)$，$A_{J_{d_0^{(j)}}}(z)$ は

$$A_{J_{d_0}}(z) = A_{J_{d_0^{(j)}}}(z) \tag{33}$$

$$d_0{}' = n + k - d_0 + 1 \pmod{n} \tag{34}$$

$$d_0^{(j)} = d_0' + 1 \pmod{n} \tag{35}$$

を満足する．

□

$GF(2^3)$ 上の $(7, 5, 3)$ 原始リード-ソロモン符号および $GF(2^4)$ 上の $(15, 2, 14)$ 原始リード-ソロモン符号を外部符号に持つ Justesen 符号に対して，この定理 3 を適用し，原始多項式 $P(x) = x^3 + x + 1$ と原始多項式 $P(x) = x^4 + x + 1$ を用いた多項式基底による 2 元展開を行った際の 2 元重み分布多項式のクラス分けの例を付録 C に記す．

以上，6 章以降で示したクラス分けは，2 元展開を行う基底に依存しないという一般的な性質を持つ．これは，今後の更なる解析や展開基底に具体性を持たせたときの分類に有効となる性質であり，更なる解析の余地を残している．

反対に，双対符号に代表されるような集合族間の解析など抽象度の高い一般的な課題も残している．

8　むすび

本論文は，原始リード-ソロモン符号の集合族を 2 元重み分布多項式が共通となるような部分集合族にクラス分けするための定理を 2 つ示した．1 つはすべての集合族に対して成り立ち，1 つは限定された集合族に対して成り立つ．また，同一の部分集合族に含まれる原始リード-ソロモン符号の生成多項式を要素とする，生成行列により構成される Justesen 符号への拡張にも成功した．クラス分けに関しては，符号理論において長年，未解決問題として残されている 2 元重み分布多項式に着目することで解決の糸口を明らかにする目的で行った．そこで，本研究で明らかになった課題を以下に示す．

原始リード-ソロモン符号および Justesen 符号の 2 元重み分布多項式が等しくなるような部分集合族の中で，最小重みを有する部分集合族を特定できれば，その他の部分集合族に含まれる符号を構成することによって見逃し誤り確率という観点で訂正能力の高い符号を分類できる．具体的には，$(120, 28)$Justesen 符号の集合族内から任意に選んだ符号の見逃し誤り確率は通信路の誤り確率が 0.1 付近で $1.0 * 10^4$ の差が生じている．よって，各部分集合族内から最小重みを有する重み分布を構成する部分集合族を特定することは集合族内での訂正能力の優劣を決定する重要な問題へと発展する．

そして，原始リード-ソロモン符号の集合族内において最小重みを有する部分集合族に含まれる符号より構成される Justesen 符号は，その集合族内においても当然最小重みを有する部分集合族に属していることから Justesen 符号の集合族内において，最も悪い訂正能力を持つ符号であるということがわかる．よって本研究は，原始リード-ソロモン符号および Justesen 符号の集合族内において見逃し誤り確率という観点で符号の訂正能力の優劣を決定する良い解決の糸口となった．

次に，定理 2 の不完全な証明が挙げられる．定理 2 の本質は，定理 1 を満たす原始リード-ソロモン符号を構成する生成多項式の連続根において, 各々の連続根に包含されるような根を持つ生成

多項式の存在である．この性質を定式化する為に定理 2 のような導出を行ったが，最小距離を奇数と限定してしまう導出の為，一般的な証明を与えることができなかった．違った角度からのアプローチが必要である．

謝辞

本研究を行うにあたり，貴重なご助言とご指導を頂いた法政大学情報科学部ディジタルメディア学科西島利尚教授に心より感謝申し上げます．また，大阪産業大学工学部常盤欣一朗教授からも貴重なご助言とご指導を頂いた．ここに深く感謝致します．

参考文献

[1] F. J. MacWilliams and N. J. A. Sloane, The Theory of Error-Correcting Codes, Amsterdom: North-Holland，1977.

[2] C. T. Retter, “The average binary weight-enumerator for a class of generalized Reed-Solomon codes, ” IEEE Trans. Inf. Theory, vol. IT-37, no. 2, pp. 346-349, March 1991.

[3] 遠藤寿之，西島利尚, 常盤欣一朗，鴻巣敏之 “原始リード - ソロモン符号の 2 元重み分布多項式のクラス分けについて” , 信学技報 情報理論, Vol.2008，No.36，pp. 95-98, Sep 2008.

[4] 西島利尚, 遠藤寿之，“可変内部符号化された連接符号の見逃し誤り確率の上界および下界について “, 第 5 回シャノン理論ワークショプ予稿集，pp. 17-21, Sep 2007.

[5] 西島利尚, 常盤欣一朗，鴻巣敏之 “一般化リード-ソロモン符号の集合族における原始リード-ソロモン符号の特定”, 第 31 回情報理論とその応用シンポジウム予稿集， pp. 724-726, Oct 2008 年.

[6] J. Justesen, “A class of constructive asymptotically good algebraic codes,” IEEE Trans. Inf. Theory, vol. IT-18 , no. 5, pp. 652-656, Sep 1972.

[7] Ron M Roth，Gadiel Seroussi, “On Generator Matrices of MDS Codes”, IEEE Trans. Inf. Theory, vol. IT-31, no. 6, pp. 826-830, Nov 1985.

付録 A

•$(7,3,5)$ 原始リード-ソロモン符号の集合族に関する生成多項式と 2 元重み分布多項式

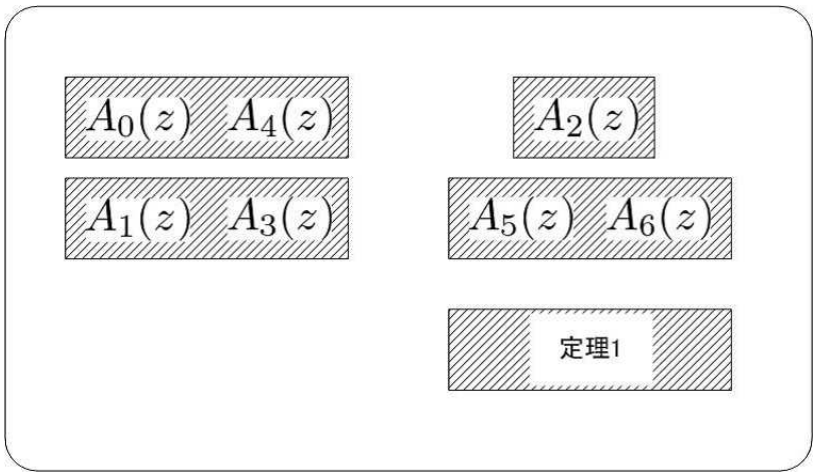

図 1: 原始リード-ソロモン符号の集合族内における 2 元重み分布多項式のクラス分け

表 1: クラス分けされた 2 元重み分布の一部

	多項式の各項													
	z^3	z^4	z^5	z^6	z^7	z^8	z^9	z^{10}	z^{11}	z^{12}	z^{13}	z^{14}	z^{15}	z^{16}
$A_0(z), A_4(z)$	0	0	0	21	0	119	0	154	0	154	0	49	0	14
$A_1(z), A_3(z)$	0	0	0	21	45	21	42	126	126	42	21	45	21	0
$A_2(z)$	0	0	7	7	31	56	56	98	98	56	56	31	7	7
$A_5(z), A_6(z)$	0	0	0	14	0	140	0	140	0	140	0	70	0	7

$\cdot d_0 = 0$ のとき

$\cdot$ 生成多項式

$$G_0(x) = x^4 + \alpha^2 x^3 + \alpha^5 x^2 + \alpha^5 x + \alpha^6$$

$\cdot$ 2 元重み分布多項式

$$A_0(z) = z^0 + 21z^6 + 119z^8 + 154z^{10} + 154z^{12} + 49z^{14} + 14z^{16}$$

$\cdot d_0 = 1$ のとき

$\cdot$ 生成多項式

$$G_1(x) = x^4 + \alpha^3 x^3 + x^2 + \alpha x + \alpha^3$$

$\cdot$ 2 元重み分布多項式

$$A_1(z) = z^0 + 21z^6 + 45z^7 + 21z^8 + 42z^9 + 126z^{10} + 126z^{11}$$

$$+ \quad 42z^{12} + 21z^{13} + 45z^{14} + 21z^{15} + z^{21}$$

$\cdot d_0 = 2$ のとき

$\cdot$ 生成多項式

$$G_2(x) = x^4 + \alpha^4 x^3 + \alpha^2 x^2 + \alpha^4 x + 1$$

$\cdot$ 2 元重み分布多項式

$$A_2(z) = z^0 + 7z^5 + 7z^6 + 31z^7 + 56z^8 + 56z^9 + 98z^{10}$$

$$+ \quad 98z^{11} + 56z^{12} + 56z^{13} + 31z^{14} + 7z^{15} + 7z^{16} + z^{21}$$

$\cdot d_0 = 3$ のとき

$\cdot$ 生成多項式

$$G_3(x) = x^4 + \alpha^5 x^3 + \alpha^4 x^2 + x + \alpha^4$$

$\cdot$ 2 元重み分布多項式

$$A_3(z) = z^0 + 21z^6 + 45z^7 + 21z^8 + 42z^9 + 126z^{10} + 126z^{11}$$

$$+ \quad 42z^{12} + 21z^{13} + 45z^{14} + 21z^{15} + z^{21}$$

・$d_0 = 4$ のとき

・生成多項式

$$G_4(x) = x^4 + \alpha^6 x^3 + \alpha^6 x^2 + \alpha^3 x + \alpha$$

・2 元重み分布多項式

$$A_4(z) = z^0 + 21z^6 + 119z^8 + 154z^{10} + 154z^{12} + 49z^{14} + 14z^{16}$$

・$d_0 = 5$ のとき

・生成多項式

$$G_5(x) = x^4 + x^3 + \alpha x^2 + \alpha^6 x + \alpha^5$$

・2 元重み分布多項式

$$A_5(z) = z^0 + 14z^6 + 140z^8 + 140z^{10} + 140z^{12} + 70z^{14} + 7z^{16}$$

・$d_0 = 6$ のとき

・生成多項式

$$G_6(x) = x^4 + \alpha x^3 + \alpha^3 x^2 + \alpha^2 x + \alpha^2$$

・2 元重み分布多項式

$$A_6(z) = z^0 + 14z^6 + 140z^8 + 140z^{10} + 140z^{12} + 70z^{14} + 7z^{16}$$

付録 B

●$(7,5,3)$ 原始リード-ソロモン符号の集合族に関する生成多項式と 2 元重み分布多項式

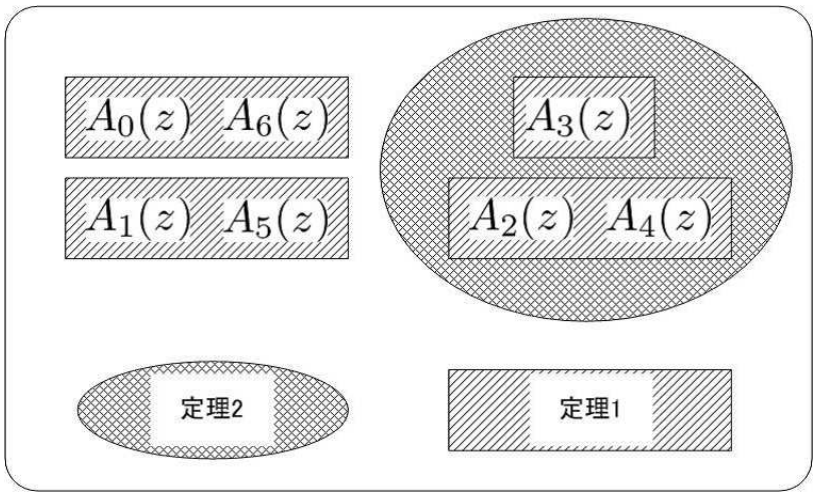

図 2: 原始リード-ソロモン符号の集合族内における 2 元重み分布多項式のクラス分け

表 2: クラス分けされた 2 元重み分布の一部

	符号の重み													
	3	4	5	6	7	8	9	10	11	12	13	14	15	16
A_0, A_6	0	210	0	1638	0	6468	0	10878	0	9310	0	3570	0	651
A_1, A_5	28	84	273	924	1956	2982	4340	5796	5796	4340	2982	1956	924	273
A_2, A_4	21	91	322	875	1809	3129	4585	5551	5551	4585	3129	1809	875	322
A_3	21	91	322	875	1809	3129	4585	5551	5551	4585	3129	1809	875	322

$\cdot d_0 = 0$ のとき

$\cdot$ 生成多項式

$$G_0(x) = x^2 + \alpha^3 x + \alpha$$

$\cdot$ 2 元重み分布多項式

$$\begin{aligned} A_0(z) &= z^0 + 210z^4 + 1638z^6 + 6468z^8 + 10878z^{10} + 9310z^{12} + 3570z^{14} \\ &+ 651z^{16} + 42z^{18} \end{aligned}$$

$\cdot d_0 = 1$ のとき

$\cdot$ 生成多項式

$$G_1(x) = x^2 + \alpha^4 x + \alpha^3$$

$\cdot$ 2 元重み分布多項式

$$\begin{aligned} A_1(z) &= z^0 + 28z^3 + 84z^4 + 273z^5 + 924z^6 + 1956z^7 + 2982z^8 \\ &+ 4340z^9 + 5796z^{10} + 5796z^{11} + 4340z^{12} + 2982z^{13} + 1956z^{14} + 924z^{15} \\ &+ 273z^{16} + 84z^{17} + 28z^{18} + z^{21} \end{aligned}$$

$\cdot d_0 = 2$ のとき

$\cdot$ 生成多項式

$$G_2(x) = x^2 + \alpha^5 x + \alpha^5$$

$\cdot$ 2 元重み分布多項式

$$\begin{aligned} A_2(z) &= z^0 + 21z^3 + 91z^4 + 322z^5 + 875z^6 + 1809z^7 + 3129z^8 \\ &+ 4585z^9 + 5551z^{10} + 5551z^{11} + 4585z^{12} + 3129z^{13} + 1809z^{14} + 875z^{15} \\ &+ 322z^{16} + 91z^{17} + 21z^{18} + z^{21} \end{aligned}$$

$\cdot d_0 = 3$ のとき

$\cdot$ 生成多項式

$$G_3(x) = x^2 + \alpha^6 x + 1$$

$\cdot$ 2 元重み分布多項式

$$\begin{aligned} A_3(z) &= z^0 + 21z^3 + 91z^4 + 322z^5 + 875z^6 + 1809z^7 + 3129z^8 \\ &+ 4585z^9 + 5551z^{10} + 5551z^{11} + 4585z^{12} + 3129z^{13} + 1809z^{14} + 875z^{15} \\ &+ 322z^{16} + 91z^{17} + 21z^{18} + z^{21} \end{aligned}$$

$\cdot d_0 = 4$ のとき

$\cdot$ 生成多項式

$$G_4(x) = x^2 + x + \alpha^2$$

$\cdot$ 2 元重み分布多項式

$$\begin{aligned} A_4(z) &= z^0 + 21z^3 + 91z^4 + 322z^5 + 875z^6 + 1809z^7 + 3129z^8 \\ &+ 4585z^9 + 5551z^{10} + 5551z^{11} + 4585z^{12} + 3129z^{13} + 1809z^{14} + 875z^{15} \\ &+ 322z^{16} + 91z^{17} + 21z^{18} + z^{21} \end{aligned}$$

$\cdot d_0 = 5$ のとき

$\cdot$ 生成多項式

$$G_5(x) = x^2 + \alpha x + \alpha^4$$

$\cdot$ 2 元重み分布多項式

$$\begin{aligned} A_5(z) &= z^0 + 28z^3 + 84z^4 + 273z^5 + 924z^6 + 1956z^7 + 2982z^8 \\ &+ 4340z^9 + 5796z^{10} + 5796z^{11} + 4340z^{12} + 2982z^{13} + 1956z^{14} + 924z^{15} \\ &+ 273z^{16} + 84z^{17} + 28z^{18} + z^{21} \end{aligned}$$

・$d_0 = 6$ のとき

・生成多項式

$$G_6(x) = x^2 + \alpha^2 x + \alpha^6$$

・２元重み分布多項式

$$A_6(z) = z^0 + 210z^4 + 1638z^6 + 6468z^8 + 10878z^{10} + 9310z^{12} + 3570z^{14}$$
$$+ 651z^{16} + 42z^{18}$$

●$(15, 2, 14)$ 原始リード-ソロモン符号の集合族に関する生成多項式と 2 元重み分布多項式

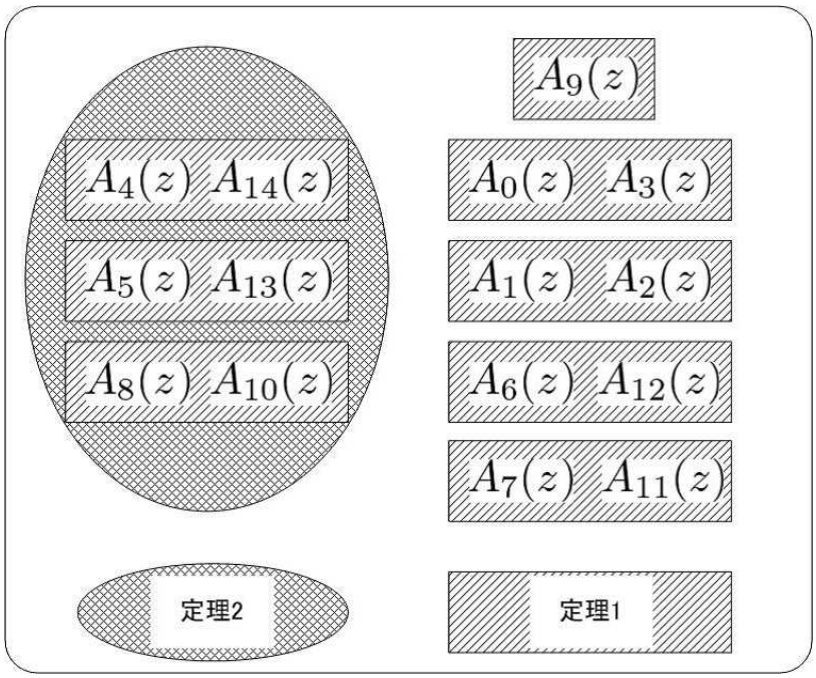

図 3: 原始リード-ソロモン符号の集合族内における 2 元重み分布多項式のクラス分け

表 3: クラス分けされた 2 元重み分布の一部

	多項式の各項													
	z^{13}	z^{14}	z^{15}	z^{16}	z^{17}	z^{18}	z^{19}	z^{20}	z^{21}	z^{22}	z^{23}	z^{24}	z^{25}	z^{26}
$A_0(z), A_3(z)$	0	0	0	0	0	0	0	0	0	0	0	60	0	0
$A_1(z), A_2(z)$	0	0	4	0	0	0	0	0	0	0	0	0	0	0
$A_4(z), A_{14}(z)$	0	0	0	0	0	0	0	0	0	0	0	15	0	45
$A_5(z), A_{13}(z)$	0	0	0	0	0	0	0	0	0	0	0	15	0	45
$A_6(z), A_{12}(z)$	0	0	0	0	0	0	0	0	0	0	0	15	0	45
$A_7(z), A_{11}(z)$	0	0	0	0	0	0	0	0	0	0	0	0	0	30
$A_8(z), A_{10}(z)$	0	0	0	0	0	0	0	0	0	0	0	15	0	45
$A_9(z)$	0	0	0	0	0	0	0	0	0	0	0	15	0	30

$\cdot d_0 = 0$ のとき

・生成多項式

$$\begin{aligned} G_0(x) &= x^{13} + \alpha^2 x^{12} + \alpha^6 x^{11} + \alpha^6 x^{10} + \alpha^{13} x^9 + \alpha^{14} x^8 + \alpha^8 x^7 + \alpha^{14} x^6 + \alpha^2 x^5 + \alpha^{13} x^4 \\ &+ \alpha^3 x^3 + x^2 + \alpha^8 x + \alpha^3 \end{aligned}$$

・２元重み分布多項式

$$A_0(z) = z^0 + 60z^{24} + 195z^{32}$$

$\cdot d_0 = 1$ のとき

・生成多項式

$$\begin{aligned} G_1(x) &= x^{13} + \alpha^3 x^{12} + \alpha^8 x^{11} + \alpha^9 x^{10} + \alpha^2 x^9 + \alpha^4 x^8 + \alpha^{14} x^7 + \alpha^6 x^6 + \alpha^{10} x^5 + \alpha^7 x^4 \\ &+ \alpha^{13} x^3 + \alpha^{11} x^2 + \alpha^5 x + \alpha \end{aligned}$$

・２元重み分布多項式

$$\begin{aligned} A_1(z) &= z^0 + 4z^{15} + 15z^{28} + 60z^{29} + 96z^{30} + 60z^{31} + 15z^{32} \\ &+ 4z^{45} + z^{60} \end{aligned}$$

$\cdot d_0 = 2$ のとき

・生成多項式

$$\begin{aligned} G_2(x) &= x^{13} + \alpha^4 x^{12} + \alpha^{10} x^{11} + \alpha^{12} x^{10} + \alpha^6 x^9 + \alpha^9 x^8 + \alpha^5 x^7 + \alpha^{13} x^6 + \alpha^3 x^5 + \alpha x^4 \\ &+ \alpha^8 x^3 + \alpha^7 x^2 + \alpha^2 x + \alpha^{14} \end{aligned}$$

・２元重み分布多項式

$$\begin{aligned} A_2(z) &= z^0 + 4z^{15} + 15z^{28} + 60z^{29} + 96z^{30} + 60z^{31} + 15z^{32} \\ &+ 4z^{45} + z^{60} \end{aligned}$$

$\cdot d_0 = 3$ のとき

· 生成多項式

$$\begin{aligned} G_3(x) &= x^{13} + \alpha^5 x^{12} + \alpha^{12} x^{11} + x^{10} + \alpha^{10} x^9 + \alpha^{14} x^8 + \alpha^{11} x^7 + \alpha^5 x^6 + \alpha^{11} x^5 + \alpha^{10} x^4 \\ &+ \alpha^3 x^3 + \alpha^3 x^2 + \alpha^{14} x + \alpha^{12} \end{aligned}$$

· 2 元重み分布多項式

$$A_3(z) = z^0 + 60z^{24} + 195z^{32}$$

$\cdot d_0 = 4$ のとき

· 生成多項式

$$\begin{aligned} G_4(x) &= x^{13} + \alpha^6 x^{12} + \alpha^{14} x^{11} + \alpha^3 x^{10} + \alpha^{14} x^9 + \alpha^4 x^8 + \alpha^2 x^7 + \alpha^{12} x^6 + \alpha^4 x^5 + \alpha^4 x^4 \\ &+ \alpha^{13} x^3 + \alpha^{14} x^2 + \alpha^{11} x + \alpha^{10} \end{aligned}$$

· 2 元重み分布多項式

$$\begin{aligned} A_4(z) &= z^0 + 15z^{24} + 45z^{26} + 15z^{28} + 85z^{30} + 60z^{32} + 15z^{34} \\ &+ 5z^{36} + 15z^{38} \end{aligned}$$

$\cdot d_0 = 5$ のとき

· 生成多項式

$$\begin{aligned} G_5(x) &= x^{13} + \alpha^7 x^{12} + \alpha x^{11} + \alpha^6 x^{10} + \alpha^3 x^9 + \alpha^9 x^8 + \alpha^8 x^7 + \alpha^4 x^6 + \alpha^{12} x^5 + \alpha^{13} x^4 \\ &+ \alpha^8 x^3 + \alpha^{10} x^2 + \alpha^8 x + \alpha^8 \end{aligned}$$

· 2 元重み分布多項式

$$\begin{aligned} A_5(z) &= z^0 + 15z^{24} + 45z^{26} + 15z^{28} + 85z^{30} + 60z^{32} + 15z^{34} \\ &+ 5z^{36} + 15z^{38} \end{aligned}$$

・$d_0 = 6$ のとき

・生成多項式

$$G_6(x) = x^{13} + \alpha^8 x^{12} + \alpha^3 x^{11} + \alpha^9 x^{10} + \alpha^7 x^9 + \alpha^{14} x^8 + \alpha^{14} x^7 + \alpha^{11} x^6 + \alpha^5 x^5 + \alpha^7 x^4$$
$$+ \alpha^3 x^3 + \alpha^6 x^2 + \alpha^5 x + \alpha^6$$

・２元重み分布多項式

$$A_6(z) = z^0 + 15z^{24} + 45z^{26} + 15z^{28} + 102z^{30} + 15z^{32} + 45z^{34}$$
$$+ 15z^{36} + 3z^{40}$$

・$d_0 = 7$ のとき

・生成多項式

$$G_7(x) = x^{13} + \alpha^9 x^{12} + \alpha^5 x^{11} + \alpha^{12} x^{10} + \alpha^{11} x^9 + \alpha^4 x^8 + \alpha^5 x^7 + \alpha^3 x^6 + \alpha^{13} x^5 + \alpha x^4$$
$$+ \alpha^{13} x^3 + \alpha^2 x^2 + \alpha^2 x + \alpha^4$$

・２元重み分布多項式

$$A_7(z) = z^0 + 30z^{26} + 105z^{28} + 52z^{30} + 30z^{34} + 35z^{36} + 3z^{40}$$

・$d_0 = 8$ のとき

・生成多項式

$$G_8(x) = x^{13} + \alpha^{10} x^{12} + \alpha^7 x^{11} + x^{10} + x^9 + \alpha^9 x^8 + \alpha^{11} x^7 + \alpha^{10} x^6 + \alpha^6 x^5 + \alpha^{10} x^4$$
$$+ \alpha^8 x^3 + \alpha^{13} x^2 + \alpha^{14} x + \alpha^2$$

・２元重み分布多項式

$$A_8(z) = z^0 + 15z^{24} + 45z^{26} + 15z^{28} + 85z^{30} + 60z^{32} + 15z^{34}$$
$$+ 5z^{36} + 15z^{38}$$

·$d_0 = 9$ のとき

· 生成多項式

$$G_9(x) = x^{13} + \alpha^{11}x^{12} + \alpha^9 x^{11} + \alpha^3 x^{10} + \alpha^4 x^9 + \alpha^{14}x^8 + \alpha^2 x^7 + \alpha^2 x^6 + \alpha^{14}x^5 + \alpha^4 x^4$$
$$+ \alpha^3 x^3 + \alpha^9 x^2 + \alpha^{11}x + 1$$

· 2 元重み分布多項式

$$A_9(z) = z^0 + 15z^{24} + 30z^{26} + 60z^{28} + 60z^{30} + 30z^{32} + 30z^{34}$$
$$+ 30z^{36}$$

·$d_0 = 10$ のとき

· 生成多項式

$$G_{10}(x) = x^{13} + \alpha^{12}x^{12} + \alpha^{11}x^{11} + \alpha^6 x^{10} + \alpha^8 x^9 + \alpha^4 x^8 + \alpha^8 x^7 + \alpha^9 x^6 + \alpha^7 x^5 + \alpha^{13}x^4$$
$$+ \alpha^{13}x^3 + \alpha^5 x^2 + \alpha^8 x + \alpha^{13}$$

· 2 元重み分布多項式

$$A_{10}(z) = z^0 + 15z^{24} + 45z^{26} + 15z^{28} + 85z^{30} + 60z^{32} + 15z^{34}$$
$$+ 5z^{36} + 15z^{38}$$

·$d_0 = 11$ のとき

· 生成多項式

$$G_{11}(x) = x^{13} + \alpha^{13}x^{12} + \alpha^{13}x^{11} + \alpha^9 x^{10} + \alpha^{12}x^9 + \alpha^9 x^8 + \alpha^{14}x^7 + \alpha x^6 + x^5 + \alpha^7 x^4$$
$$+ \alpha^8 x^3 + \alpha x^2 + \alpha^5 x + \alpha^{11}$$

· 2 元重み分布多項式

$$A_{11}(z) = z^0 + 30z^{26} + 105z^{28} + 52z^{30} + 30z^{34} + 35z^{36} + 3z^{40}$$

$\cdot d_0 = 12$ のとき

$\cdot$ 生成多項式

$$\begin{aligned} G_{12}(x) &= x^{13} + \alpha^{14}x^{12} + x^{11} + \alpha^{12}x^{10} + \alpha x^9 + \alpha^{14}x^8 + \alpha^5 x^7 + \alpha^8 x^6 + \alpha^8 x^5 + \alpha x^4 \\ &+ \alpha^3 x^3 + \alpha^{12}x^2 + \alpha^2 x + \alpha^9 \end{aligned}$$

$\cdot$ 2 元重み分布多項式

$$\begin{aligned} A_{12}(z) &= z^0 + 15z^{24} + 45z^{26} + 15z^{28} + 102z^{30} + 15z^{32} + 45z^{34} \\ &+ 15z^{36} + 3z^{40} \end{aligned}$$

$\cdot d_0 = 13$ のとき

$\cdot$ 生成多項式

$$\begin{aligned} G_{13}(x) &= x^{13} + x^{12} + \alpha^2 x^{11} + x^{10} + \alpha^5 x^9 + \alpha^4 x^8 + \alpha^{11} x^7 + x^6 + \alpha x^5 + \alpha^{10} x^4 \\ &+ \alpha^{13} x^3 + \alpha^8 x^2 + \alpha^{14} x + \alpha^7 \end{aligned}$$

$\cdot$ 2 元重み分布多項式

$$\begin{aligned} A_{13}(z) &= z^0 + 15z^{24} + 45z^{26} + 15z^{28} + 85z^{30} + 60z^{32} + 15z^{34} \\ &+ 5z^{36} + 15z^{38} \end{aligned}$$

$\cdot d_0 = 14$ のとき

$\cdot$ 生成多項式

$$\begin{aligned} G_{14}(x) &= x^{13} + \alpha x^{12} + \alpha^4 x^{11} + \alpha^3 x^{10} + \alpha^9 x^9 + \alpha^9 x^8 + \alpha^2 x^7 + \alpha^7 x^6 + \alpha^9 x^5 + \alpha^4 x^4 \\ &+ \alpha^8 x^3 + \alpha^4 x^2 + \alpha^{11} x + \alpha^5 \end{aligned}$$

$\cdot$ 2 元重み分布多項式

$$\begin{aligned} A_{14}(z) &= z^0 + 15z^{24} + 45z^{26} + 15z^{28} + 85z^{30} + 60z^{32} + 15z^{34} \\ &+ 5z^{36} + 15z^{38} \end{aligned}$$

付録 C

• 外部符号に $(7, 5, 3)$ 原始リード-ソロモン符号を持つ Justesen 符号の集合族に関する 2 元重み分布多項式

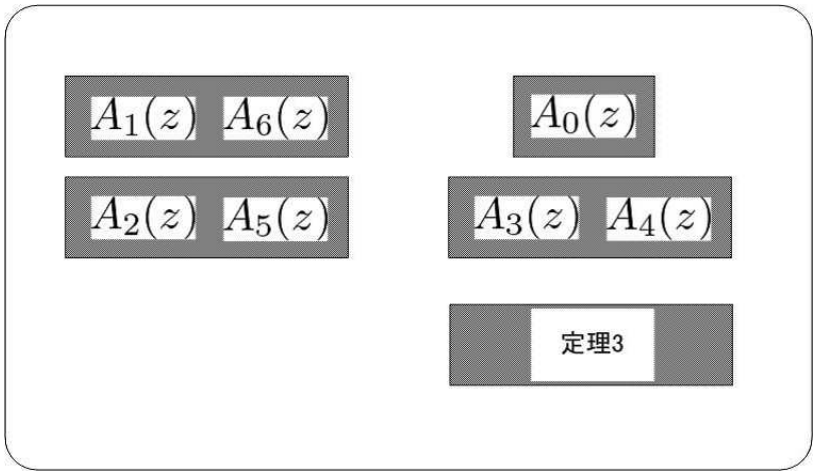

図 4: 原始リード-ソロモン符号の集合族内における 2 元重み分布多項式のクラス分け

表 4: クラス分けされた 2 元重み分布の一部

	多項式の各項													
	z^2	z^3	z^4	z^5	z^6	z^7	z^8	z^9	z^{10}	z^{11}	z^{12}	z^{13}	z^{14}	z^{15}
$A_0(z)$	0	0	0	0	0	0	49	0	232	0	534	0	1236	0
$A_3(z), A_4(z)$	0	0	0	0	2	11	28	54	90	152	271	458	685	993
$A_2(z), A_5(z)$	0	0	0	0	0	11	37	48	81	161	268	474	663	998
$A_1(z), A_6(z)$	0	0	0	0	0	12	19	60	106	161	288	410	665	1003

$\cdot d_0 = 0$ のとき

$\cdot$ 2 元重み分布多項式

$$\begin{aligned} A_0(z) &= z^0 + 49z^8 + 232z^{10} + 534z^{12} + 1236z^{14} + 2849z^{16} + 4800z^{18} \\ &+ 6148z^{20} + 6488z^{22} + 5751z^{24} + 2872z^{26} + 1510z^{28} + 244z^{30} + 54z^{32} \end{aligned}$$

$\cdot d_0 = 1$ のとき

$\cdot$ 2 元重み分布多項式

$$\begin{aligned} A_1(z) &= z^0 + 12z^7 + 19z^8 + 60z^9 + 106z^{10} + 161z^{11} + 288z^{12} \\ &+ 410z^{13} + 665z^{14} + 1003z^{15} + 1363z^{16} + 1877z^{17} + 2322z^{18} + 2766z^{19} \\ &+ 3180z^{20} + 3328z^{21} + 3334z^{22} + 3102z^{23} + 2649z^{24} + 2162z^{25} + 1610z^{26} \\ &+ 1089z^{27} + 676z^{28} + 350z^{29} + 153z^{30} + 59z^{31} + 16z^{32} + 5z^{33} \\ &+ 2z^{34} \end{aligned}$$

$\cdot d_0 = 2$ のとき

$\cdot$ 2 元重み分布多項式

$$\begin{aligned} A_2(z) &= z^0 + 11z^7 + 37z^8 + 48z^9 + 81z^{10} + 161z^{11} + 268z^{12} \\ &+ 474z^{13} + 663z^{14} + 998z^{15} + 1424z^{16} + 1773z^{17} + 2324z^{18} + 2768z^{19} \\ &+ 3142z^{20} + 3398z^{21} + 3344z^{22} + 3101z^{23} + 2623z^{24} + 2172z^{25} + 1619z^{26} \\ &+ 1079z^{27} + 686z^{28} + 320z^{29} + 161z^{30} + 74z^{31} + 11z^{32} + 7z^{33} \end{aligned}$$

$\cdot d_0 = 3$ のとき

$\cdot$ 2 元重み分布多項式

$$\begin{aligned} A_3(z) &= z^0 + 2z^6 + 11z^7 + 28z^8 + 54z^9 + 90z^{10} + 152z^{11} \\ &+ 271z^{12} + 458z^{13} + 685z^{14} + 993z^{15} + 1375z^{16} + 1835z^{17} + 2338z^{18} \\ &+ 2786z^{19} + 3128z^{20} + 3314z^{21} + 3338z^{22} + 3103z^{23} + 2712z^{24} + 2186z^{25} \\ &+ 1572z^{26} + 1086z^{27} + 657z^{28} + 340z^{29} + 167z^{30} + 61z^{31} + 20z^{32} \\ &+ 5z^{33} \end{aligned}$$

$\cdot d_0 = 4$ のとき

$\cdot$ 2 元重み分布多項式

$$\begin{aligned} A_4(z) &= z^0 + 2z^6 + 11z^7 + 28z^8 + 54z^9 + 90z^{10} + 152z^{11} \\ &+ 271z^{12} + 458z^{13} + 685z^{14} + 993z^{15} + 1375z^{16} + 1835z^{17} + 2338z^{18} \\ &+ 2786z^{19} + 3128z^{20} + 3314z^{21} + 3338z^{22} + 3103z^{23} + 2712z^{24} + 2186z^{25} \\ &+ 1572z^{26} + 1086z^{27} + 657z^{28} + 340z^{29} + 167z^{30} + 61z^{31} + 20z^{32} \\ &+ 5z^{33} \end{aligned}$$

$\cdot d_0 = 5$ のとき

$\cdot$ 2 元重み分布多項式

$$\begin{aligned} A_5(z) &= z^0 + 11z^7 + 37z^8 + 48z^9 + 81z^{10} + 161z^{11} + 268z^{12} \\ &+ 474z^{13} + 663z^{14} + 998z^{15} + 1424z^{16} + 1773z^{17} + 2324z^{18} + 2768z^{19} \\ &+ 3142z^{20} + 3398z^{21} + 3344z^{22} + 3101z^{23} + 2623z^{24} + 2172z^{25} + 1619z^{26} \\ &+ 1079z^{27} + 686z^{28} + 320z^{29} + 161z^{30} + 74z^{31} + 11z^{32} + 7z^{33} \end{aligned}$$

・$d_0 = 6$ のとき

・２元重み分布多項式

$$
\begin{aligned}
A_6(z) &= z^0 + 12z^7 + 19z^8 + 60z^9 + 106z^{10} + 161z^{11} + 288z^{12} \\
&+ 410z^{13} + 665z^{14} + 1003z^{15} + 1363z^{16} + 1877z^{17} + 2322z^{18} + 2766z^{19} \\
&+ 3180z^{20} + 3328z^{21} + 3334z^{22} + 3102z^{23} + 2649z^{24} + 2162z^{25} + 1610z^{26} \\
&+ 1089z^{27} + 676z^{28} + 350z^{29} + 153z^{30} + 59z^{31} + 16z^{32} + 5z^{33} \\
&+ 2z^{34}
\end{aligned}
$$

● 外部符号に $(15, 2, 14)$ 原始リード-ソロモン符号を持つ Justesen 符号の集合族に関する 2 元重み分布多項式

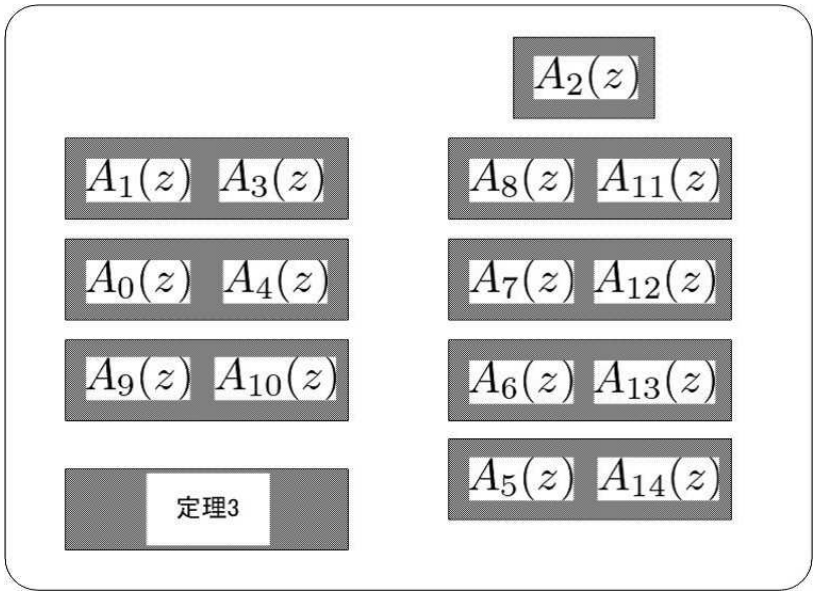

図 5: 原始リード-ソロモン符号の集合族内における 2 元重み分布多項式のクラス分け

表 5: クラス分けされた 2 元重み分布の一部

	多項式の各項													
	z^{13}	z^{14}	z^{15}	z^{16}	z^{17}	z^{18}	z^{19}	z^{20}	z^{21}	z^{22}	z^{23}	z^{24}	z^{25}	z^{26}
$A_2(z)$	0	0	8	0	0	0	0	0	0	0	0	1	8	28
$A_1(z), A_3(z)$	0	0	4	0	0	0	0	4	16	24	16	0	0	0
$A_0(z), A_4(z)$	0	0	0	4	0	12	0	4	0	20	0	23	0	37
$A_9(z), A_{10}(z)$	0	0	0	1	0	5	0	11	0	23	0	29	0	33
$A_8(z), A_{11}(z)$	0	0	0	0	0	2	0	13	0	25	0	23	0	45
$A_7(z), A_{12}(z)$	0	0	0	0	0	2	0	13	0	25	0	25	0	46
$A_6(z), A_{13}(z)$	0	0	0	1	0	6	0	11	0	17	0	37	0	24
$A_5(z), A_{14}(z)$	0	0	0	1	0	6	0	11	0	16	0	37	0	30

$\cdot d_0 = 0$ のとき

・2元重み分布多項式

$$\begin{aligned} A_0(z) &= z^0 + 4z^{48} + 12z^{50} + 4z^{52} + 20z^{54} + 23z^{56} + 37z^{58} \\ &+ 11z^{60} + 69z^{62} + 48z^{64} + 11z^{66} + 5z^{68} + 11z^{70} \end{aligned}$$

$\cdot d_0 = 1$ のとき

・2元重み分布多項式

$$\begin{aligned} A_1(z) &= z^0 + 4z^{47} + 4z^{52} + 16z^{53} + 24z^{54} + 16z^{55} + 11z^{60} \\ &+ 44z^{61} + 72z^{62} + 44z^{63} + 15z^{64} + 4z^{77} + z^{92} \end{aligned}$$

$\cdot d_0 = 2$ のとき

・2元重み分布多項式

$$\begin{aligned} A_2(z) &= z^0 + 8z^{47} + z^{56} + 8z^{57} + 28z^{58} + 56z^{59} + 68z^{60} \\ &+ 48z^{61} + 28z^{62} + 8z^{77} + 2z^{92} \end{aligned}$$

$\cdot d_0 = 3$ のとき

・2元重み分布多項式

$$\begin{aligned} A_3(z) &= z^0 + 4z^{47} + 4z^{52} + 16z^{53} + 24z^{54} + 16z^{55} + 11z^{60} \\ &+ 44z^{61} + 72z^{62} + 44z^{63} + 15z^{64} + 4z^{77} + z^{92} \end{aligned}$$

$\cdot d_0 = 4$ のとき

・2元重み分布多項式

$$\begin{aligned} A_4(z) &= z^0 + 4z^{48} + 12z^{50} + 4z^{52} + 20z^{54} + 23z^{56} + 37z^{58} \\ &+ 11z^{60} + 69z^{62} + 48z^{64} + 11z^{66} + 5z^{68} + 11z^{70} \end{aligned}$$

$\cdot d_0 = 5$ のとき

・2元重み分布多項式

$$
\begin{aligned}
A_5(z) &= z^0 + z^{48} + 6z^{50} + 11z^{52} + 16z^{54} + 37z^{56} + 30z^{58} \\
&+ 37z^{60} + 54z^{62} + 25z^{64} + 8z^{66} + 21z^{68} + 6z^{70} + 2z^{72} \\
&+ z^{76}
\end{aligned}
$$

$\cdot d_0 = 6$ のとき

$\cdot$ 2 元重み分布多項式

$$
\begin{aligned}
A_6(z) &= z^0 + z^{48} + 6z^{50} + 11z^{52} + 17z^{54} + 37z^{56} + 24z^{58} \\
&+ 46z^{60} + 48z^{62} + 25z^{64} + 15z^{66} + 17z^{68} + z^{70} + 6z^{72} \\
&+ z^{74}
\end{aligned}
$$

$\cdot d_0 = 7$ のとき

$\cdot$ 2 元重み分布多項式

$$
\begin{aligned}
A_7(z) &= z^0 + 2z^{50} + 13z^{52} + 25z^{54} + 25z^{56} + 46z^{58} + 34z^{60} \\
&+ 43z^{62} + 27z^{64} + 18z^{66} + 6z^{68} + 10z^{70} + 5z^{72} + z^{76}
\end{aligned}
$$

$\cdot d_0 = 8$ のとき

$\cdot$ 2 元重み分布多項式

$$
\begin{aligned}
A_8(z) &= z^0 + 2z^{50} + 13z^{52} + 25z^{54} + 23z^{56} + 45z^{58} + 49z^{60} \\
&+ 31z^{62} + 16z^{64} + 27z^{66} + 15z^{68} + 4z^{70} + 2z^{72} + 2z^{74} \\
&+ z^{76}
\end{aligned}
$$

・$d_0 = 9$ のとき

・2 元重み分布多項式

$$\begin{aligned} A_9(z) &= z^0 + z^{48} + 5z^{50} + 11z^{52} + 23z^{54} + 29z^{56} + 33z^{58} \\ &+ 42z^{60} + 35z^{62} + 33z^{64} + 20z^{66} + 17z^{68} + 2z^{70} + 2z^{72} \\ &+ 2z^{74} \end{aligned}$$

・$d_0 = 10$ のとき

・2 元重み分布多項式

$$\begin{aligned} A_{10}(z) &= z^0 + z^{48} + 5z^{50} + 11z^{52} + 23z^{54} + 29z^{56} + 33z^{58} \\ &+ 42z^{60} + 35z^{62} + 33z^{64} + 20z^{66} + 17z^{68} + 2z^{70} + 2z^{72} \\ &+ 2z^{74} \end{aligned}$$

・$d_0 = 11$ のとき

・2 元重み分布多項式

$$\begin{aligned} A_{11}(z) &= z^0 + 2z^{50} + 13z^{52} + 25z^{54} + 23z^{56} + 45z^{58} + 49z^{60} \\ &+ 31z^{62} + 16z^{64} + 27z^{66} + 15z^{68} + 4z^{70} + 2z^{72} + 2z^{74} \\ &+ z^{76} \end{aligned}$$

・$d_0 = 12$ のとき

・2 元重み分布多項式

$$\begin{aligned} A_{12}(z) &= z^0 + 2z^{50} + 13z^{52} + 25z^{54} + 25z^{56} + 46z^{58} + 34z^{60} \\ &+ 43z^{62} + 27z^{64} + 18z^{66} + 6z^{68} + 10z^{70} + 5z^{72} + z^{76} \end{aligned}$$

$\cdot d_0 = 13$ のとき

・2元重み分布多項式

$$\begin{aligned} A_{13}(z) &= z^0 + z^{48} + 6z^{50} + 11z^{52} + 17z^{54} + 37z^{56} + 24z^{58} \\ &+ 46z^{60} + 48z^{62} + 25z^{64} + 15z^{66} + 17z^{68} + z^{70} + 6z^{72} \\ &+ z^{74} \end{aligned}$$

$\cdot d_0 = 14$ のとき

・2元重み分布多項式

$$\begin{aligned} A_{14}(z) &= z^0 + z^{48} + 6z^{50} + 11z^{52} + 16z^{54} + 37z^{56} + 30z^{58} \\ &+ 37z^{60} + 54z^{62} + 25z^{64} + 8z^{66} + 21z^{68} + 6z^{70} + 2z^{72} + z^{76} \end{aligned}$$