符号理論およびエントロピーとその応用

多田, 秀樹 / TADA, Hideki

(発行年 / Year)
2007-03-24
(学位授与番号 / Degree Number)
32675甲第183号
(学位授与年月日 / Date of Granted)
2007-03-24
(学位名 / Degree Name)
博士(工学)
(学位授与機関 / Degree Grantor)
法政大学 (Hosei University)
(URL)
https://doi.org/10.15002/00003789

博士論文

符号理論およびエントロピーとその応用

Coding Theory , Entropy and its Application

法政大学大学院工学研究科

システム工学専攻　博士課程

多田 秀樹

目 次

第1章　序論

1.1　符号理論とは

情報を伝送しようとする際には，送りたい情報をデジタル化し，通信路を介して受信者まで送られる．このとき通信路では，熱雑音や物理的な損傷等，さまざまなノイズの影響により送りたい情報が変質してしまう可能性があり，受信者が受け取る情報は，必ずしも元の情報と同じになるとは限らない．こうした通信の誤りの対処法として，誤り訂正・検出符号がある．符号理論とは，符号を用いたときの効率と信頼性の向上を目的とする，誤り訂正・検出符号の構成法および符号化・復号法についての理論である．

符号化による誤りの訂正・検出の原理は簡単である．例えば，送信側が 0 または 1 を送信したいとき，これを 3 回続けて 000 か 111 を送ると決めておく．もし受信側で 101 が受信されたとすれば，これは予め決めておいた 000 でも 111 とは異なるために，誤りが生じていることを検出できる．さらに必要であれば，確率的な部分を考慮して，送られてきた情報は 111 であろうと推測し，訂正する．このように，送りたい情報に一定の規則に従って冗長部分を付加し，受信側はこの規則に従っているかどうかを調べることで，誤りの訂正・検出を行うことができる．

実際に用いられる誤り訂正符号の多くは，優れた符号構成法や復号法が知られている線形符号である．線形符号のなかでも，特に巡回符号は，符号化や復号のための計算が容易に装置化が可能であり，代数的にきれいな枠組みの中で論じることができるために符号を構成し易いことから，最もよく用いられる．本論文の 2 章，3 章で取り扱う，Cyclotomic Duadic 符号および有限環上の符号も巡回符号のひとつである．

1.2　エントロピーと相互情報量

エントロピー (情報量) とは，物理学で用いられていた概念を，情報の量を表す指標として情報理論に導入されたもので，ある出来事 (事象) が起こった際，その出来事がどれほど起こりにくいか (あいまいさ，不確かさ) を表す尺度として用いられる．ある事象に対するエントロピーが小さいときは，その事象のあいまいさ

は小さく，規則性が大きいことを意味し，逆に大きいときは，あいまいさは大きく，規則性が少ないことを意味する．頻繁に起こるありきたりの出来事が起こった事を知ってもそれはたいした情報にはならないが，逆に滅多に起こらない出来事が起これば，それはより多くの情報を含んでいると考えられる．よって，エントロピーは事象がどれだけの情報を持っているかを表す尺度であるともみなす事ができる．

また，相互情報量は，ある二つの事象において，一方を知ることで，他方についてどれくらい情報が得られるかを表す量，すなわち，両者が共有する情報の量を表していて，類似度や相関をはかる指標としても用いられる．

1.3　本論文の構成

本論文は，5 章で構成されており，ここでは以降の各章の主題を総覧し，説明をくわえておく：

まず第 2 章では，巡回符号のひとつであり，平方剰余符号の拡張として与えられる Cyclotomic Duadic 符号を定義し，その有効性と構成法を示す．平方剰余符号と異なる Cyclotomic Duadic 符号があるかどうかは，C. Ding と V. Pless によって提唱された問題である．

次に 3 章では，有限環上での符号を取り扱う．有限環上で符号を構成する場合には，有限体上での符号とは異なり，生成多項式がただ一つに決まるとは限らず，その扱いは難しくなる．しかしながら，符号化および復号処理の高速化を計るためには，多項式表現を与えておくことが望ましい．そこで，符号長に条件を与えた $\mathbf{Z}/p^2\mathbf{Z}$ 上の巡回符号の生成多項式および検査多項式を決定する．

第 4 章では，高次の相関を計る指標として新たに共変指数を導入し，光空間伝送ネットワークの解析を行う．光空間伝送ネットワークはリンクの同時切断の回避を目的として考案されたが，その有効性と改良点を検討する

最後に第 5 章では，第 4 章で導入した共変指数を用いて HIV-1 の V3 loop の解析を行う．V3 loop はアミノ酸の変異性の大きい箇所として知られるが，その変化には何らかの相互依存が存在すると仮定し，アミノ酸ネットワークの解明を目的として実験を行った．

第2章　Duadic符号と巾剰余

2.1　序

符号長 n の巡回符号を構成する際，多項式 $x^n - 1$ を有限体上で因数分解することにより生成多項式を求める．ここで，巡回符号は $e(x) = e(x)^2$ を満たす冪等生成元を持つ性質から，冪等の多項式を求めることで，その生成多項式を決定することが可能である．その代表的な例として平方剰余符号が挙げられ，その拡張として Cyclotomic Duadic (CD) 符号がある．

CD 符号は 2 を冪剰余に持つ素数 p に対し，$\mathbf{F}_p$ を軌道分解し，条件に合う様に軌道を組み合わせることで，分割を構成し，冪等生成元を求めるが，条件を満たす様に軌道の組み合わせを考えることは簡単でない．2.5 節では，2 を $2e$ 乗剰余に持つ素数 p に対し，有限体 $\mathbf{F}_p$ の軌道分解を行い，その軌道の組み合わせ方を考えることによる具体的な分割方法を与える．この場合には，各軌道の元の数が等しくなり，条件を満たす軌道の組み合わせを容易に得ることが可能となる．また，2 を冪乗剰余に持つ素数 p を求めることは高次相互法則と呼ばれ，いくつかの p に対してはその条件が与えられている．2.6 節では，その条件を組み合わせて考えることでより高次の条件が得られること，さらに，そのような素数 p が無限に存在することを示す．

2.2　冪等生成元と平方剰余符号

線形符号は理論的に取り扱いやすく，優れた符号構成法や復号法が知られていることから，実際によく用いられている誤り訂正符号である．CD 符号を含めた巡回符号も線形符号のひとつで，符号化やシンドロームの計算が容易に装置化でき，符号を構成し易いなどの特徴をもっている．

2.2 節では，巡回符号に関する性質と符号化法および平方剰余符号についてまとめておく．

定義 2.2.1: $GF(q)$ 上の n 次元ベクトル空間の部分集合を $C \subset F_q^n$ とする．ここで，

C の任意の元 w_1, w_2 に対して，

$$w = c_1 w_1 + c_2 w_2 \in C \quad (c_1, c_2 \in GF(q))$$

を満たすとき，C を線形符号と呼ぶ．また，符号 C の通報 $i \in F_q^k$ の次元を k，符号語 $w \in F_n^k$ の次元を n とするとき，C を (n, k) 線形符号ともいう．

(例) 2 元線形符号 C : $\{0\ 0\ 0,\ 0\ 1\ 1,\ 1\ 0\ 1,\ 1\ 1\ 0\}$
C の任意の二つの符号語の和は，C の符号語となるので線形符号といえる．

定義 2.2.2: $GF(q)$ 上の (n, k) 線形符号 C の任意の符号語を，

$$w = (w_{n-1}, w_{n-2}, \cdots, w_1, w_0),$$

としたとき，この符号語の成分を巡回置換した

$$w' = (w_{n-1}, w_{n-2}, \cdots, w_1, w_0),$$

が常に C の符号語となるなら，C を巡回符号 (cyclic code) と呼ぶ．

ここで，巡回符号の例をあげる前に以下のことを定義しておく．

定義 2.2.3: $GF(q)$ 上の n 次元ベクトル w を $GF(q)$ 上の多項式

$$W(x) = w_{n-1}x^{n-1} + w_{n-2}x^{n-2} + \cdots + w_1 x + w_0,$$

と表現し，これをベクトルの多項式表現と呼ぶ．特に符号語を多項式で表現したものは符号多項式と呼び，符号語のなかでも，0 でない次数が最小のモニック多項式を生成多項式と呼ぶ．

多項式表現を用いると，w の巡回置換は次のように表せる．

$$w_{n-2}x^{n-2} + w_{n-3}x^{n-3} + \cdots + w_0 x + w_{n-1} = xW(x) \mod(x^n - 1).$$

巡回符号では，符号語を巡回置換したものもふたたび符号語になること，また巡回符号は線形符号であることに注意すると，$A(X)$ を任意の多項式とした

$$A(x)W(x) \mod(x^n - 1),$$

もまた符号語となり，以下の二つの定理が導かれる．

定理 2.2.4: $GF(q)$ 上の $n-1$ 次以下の多項式 $W(x)$ が符号長 n の q 元巡回符号 C の符号多項式となるための必要十分条件は，$W(x)$ が生成多項式 $G(x)$ で割り切れることである．

証明: 符号多項式 $W(x)$ を生成多項式 $G(x)$ で割った剰余を $R(x)$，商を $Q(x)$ とすると

$$W(x) = Q(x)G(X) + R(x), \tag{2.1}$$
$$deg\ R(x)\ <\ deg\ G(x), \tag{2.2}$$
$$deg\ Q(x)G(x) = deg\ W(x) \leq n-1. \tag{2.3}$$

ここで，$G(x)$ は符号多項式であるので，$Q(x)G(x)$ は符号多項式となる．
また，$R(x)$ は (2.1) より，二つの符号多項式の差で表せるので，線形性から $R(x)$ も符号語となる．ところが，(2.2) から $R(x) = 0$ を得る．
よって，$W(x)$ は $G(x)$ で割り切れる■

定理 2.2.5: (n, k) 巡回符号の生成多項式は $x^n - 1$ を割り切る $n-k$ 次の多項式である．また，$GF(q)$ 上の m 次のモニック多項式は $x^n - 1$ を割り切るなら q 元 $(n, n-m)$ 巡回符号の生成多項式となる．

証明: $x^n - 1$ を生成多項式 $G(x)$ で割った剰余を $R(x)$，商を $Q(x)$ とすると

$$x^n - 1 = Q(x)G(x) + R(x), \tag{2.4}$$
$$deg\ R(x)\ <\ deg\ G(x) < n. \tag{2.5}$$

(2.4) の両辺を $x^n - 1$ で割って剰余をとれば,

$$R(x) = -Q(x)G(x)\ \mod x^n - 1. \tag{2.6}$$

定理 2.2.4 での証明同様，(2.5) から $R(x) = 0$ がいえ，生成多項式 $G(x)$ は $x^n - 1$ を割り切る．

また，$G'(x)$ を $x^n - 1$ を割り切る m 次のモニック多項式とする．また，$GF(q)$ 上の $n-1$ 次以下の多項式で $G'(x)$ の倍多項式の集合を M とする．このとき，M の任意の元は，適当な多項式 $A(x)$ を用いて $A(x)G'(x)$ と表されるので，M は線形符号である．また，$A(x)$ の $n-m-1$ 次の係数を a_{n-m-1} とすると，$A(x)G'(x)$ の巡回置換は,

$$[xA(x)G'(x)](\mathrm{mod}\ x^n - 1) = xA(x)G'(x) - a_{n-m-1}(x^n - 1), \tag{2.7}$$

と表され，$G'(x)$ は x^n-1 を割り切ることから，(2.7) の右辺は G'(X) で割り切れる．したがって M の任意の元の巡回置換もまた M に属することから，$G'(X)$ は q 元 $(n, n-k)$ 巡回符号の生成多項式となる．■

(例) $GF(2)$ 上の符号長 $n=4$ の符号 C : {0 0 0 0, 0 0 1 1, 0 1 0 1, 0 1 1 0, 1 0 0 1, 1 0 1 0, 1 1 0 0, 1 1 1 1} は巡回符号である．

実際に C は線形符号であり．それぞれの符号を巡回置換すると図 2.1 のようになり，ふたたび符号語になることがわかる．

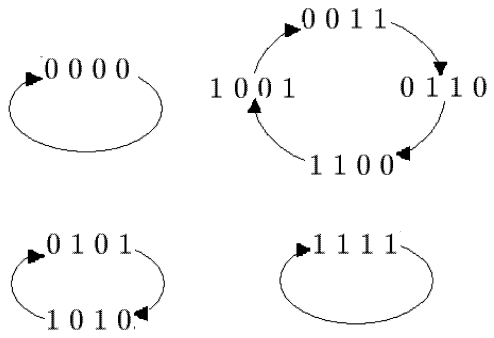


図 2.1 巡回符号の符号語の巡回置換

この巡回符号 C を多項式で表すと $\{0, x+1, x^2+1, x^2+x, x^3+1, x^3+x, x^3+x^2, x^3+x^2+x+1\}$. ここで，生成多項式 $G(x)$ を $x+1$ ととる．任意の通報多項式 $A(x)$ を乗じ，x^n-1 の剰余を考えると，$A(x)G(x)$ もまた符号語となる．

また，巡回符号に対し，次の事が成り立つ．

定理 2.2.5 n を奇数とする．ここで x^n-1 の因子 $G(X)$ を生成多項式とする巡回符号 C について

$$e(x)=\sum_{i=0}^{n-1} e_i x^i = \sum_{i\in E} x^i \in C,$$

とおくとき，$e(x)=e(x)^2$ をみたす多項式が存在し，$e(x)$ を冪等元と呼ぶ．また，冪等元は C の生成多項式として考えられることから，冪等生成元と呼ばれる．

この性質を利用して構成される代表的な符号に平方剰余符号がある．

定義 2.2.3 符号長 n を $p\equiv\pm1(\mathrm{mod}8)$ すなわち，$\left(\frac{2}{p}\right)=1$ をみたすような奇素数 p とし，

$$E=\{i^2; i\in \mathbf{F}_p\},$$

を考える．このとき多項式

$$e(x) = \sum_{i \in E} x^i,$$

は冪等元となり，$e(x)$ で生成される巡回符号 C を平方剰余符号という．

2.3 Duadic 符号

J.S.Leon, J.M.Masley, V.Pless は，これを一般化して次のような問題を提起した ([5]); 自然数 n を固定し，

$$E \cup E^{\perp} = \mathbf{Z}/n\mathbf{Z} - \{0\},$$
$$E \cap E^{\perp} = \phi,\ |E| = |E^{\perp}| = \tfrac{n-1}{2},$$
$$\mu E = E^{\perp},\ \mu E = E^{\perp},\ \mu \in (\mathbf{Z}/n\mathbf{Z})^{\times}$$

と分割 (splitting) したとき，

$$e(x) = \sum_{i \in E} x^i,\ e^{\perp}(x) = \sum_{i \in E^{\perp}} x^i$$

$$1 + e(x) = \sum_{i \in E} x^i,\ 1 + e^{\perp}(x) = \sum_{i \in E^{\perp}} x^i$$

が冪等になるのはどのようなときか？とくに $\mathbf{Z}/p\mathbf{Z} = \mathbf{F}_p$ のとき，平方剰余符号と異なるものはあるか？

本論文では 2 元 Duadic 符号を扱うが，一般的な有限体上 $\mathbf{F}_q$ 上での Duadic 符号の定義と基本的な性質を述べておく;

$\mathbf{F}_q$ 上の n 次元ベクトル $\boldsymbol{a} = (a_0, a_1, \cdots, a_{n-1})$ は $\sum_{i=0}^{n-1} a_i = 0$ のとき，even-like ベクトルという．そうでないとき，odd-like ベクトルという．符号 C の符号語が全て even-like ベクトルのとき，符号 C を even-like 符号，1 つでも odd-like ベクトルを含むとき odd-like 符号という．$R = \mathbf{F}_q[x]/(x^n - 1)$ 内の even-like ベクトル全体の集合 ε は $(n, n-1)$ 巡回符号を作る．$\varepsilon^{\perp} = \langle u(x) \rangle, \varepsilon = \langle 1 - u(x) \rangle$ である．$u(x)$ は冪等生成元で

$$u(x) = \frac{1}{n}(1 + x + x^2 + \cdots + x^{n-1}).$$

C を R 内の $g(x)$ で生成される巡回符号とするとき，

$$C : \text{even-like} \Leftrightarrow u(x) \notin C (\Leftrightarrow x-1 | g(x))$$
$$C : \text{odd-like} \Leftrightarrow u(x) \in C (\Leftrightarrow x-1 \not| g(x))$$

が成立する．2 つの even-like 符号

$$C_1 = \langle e_1(x) \rangle, \quad C_2 = \langle e_2(x) \rangle$$

が even-like duadic 符号の pair であるとは，

$$e_1(x) + e_2(x) = 1 - u(x)$$

かつ座標置換 $\mu_a : i \longrightarrow ai \pmod{n}$,(ただし $(n, a) = 1$) が存在して

$$C_1\mu_a = C_2, C_2\mu_a = C_1$$

をみたすことをいう．一方で, このとき，

$$D_1 = \langle 1 - e_2(x) \rangle, \quad D_2 = \langle 1 - e_1(x) \rangle$$

とおき，odd-like 符号の pair という．

定理 2.3.1([5])

(1) $C_1 \cup C_2 = 0, C_1 + C_2 = \varepsilon$.
(2) n が奇数のとき $\dim C_1 = \dim C_2 = \frac{n-1}{2}$.
(3) D_1 は C_2 の補集合，D_2 は C_1 の補集合.
(4) $D_1\mu_a = D_2, D_2\mu_a = D_1$.
(5) $D_1 = C_1 + \langle u(x) \rangle = \langle u(x) + e_1(x) \rangle$,
$D_2 = C_2 + \langle u(x) \rangle = \langle u(x) + e_2(x) \rangle$.
(6) $D_1 \wedge D_2 = \langle u(x) \rangle, D_1 + D_2 = R$.
(7) $\dim D_1 = \dim D_2 = \frac{n+1}{2}$.
(8) $\mathbf{F}_q$ 上の長さ n の Duadic 符号が存在.
$\Leftrightarrow q : square \mod n$.
(9) 長さ n の 2 元 Duadic 符号が存在
$\Leftrightarrow n = p_1^{a_1} \cdots p_r^{a_r}$ ただし $p_i \equiv \pm 1 \mod 8$
(10) 長さ n の 3 元 Duadic 符号が存在
$\Leftrightarrow n = p_1^{a_1} \cdots p_r^{a_r}$ ただし $p_i \equiv \pm 1 \mod 12$

2.4　2元Duadic符号と軌道分解

2 元巡回符号は，その冪等生成元が，分割 $E \cup E^{\perp} = \mathbf{Z}/n\mathbf{Z} - \{0\}$ から作られる多項式

$$e(x) = \sum_{i \in E} x^i,\ e^{\perp}(x) = \sum_{i \in E^{\perp}} x^i,$$
$$1 + e(x) = \sum_{i \in E} x^i,\ 1 + e^{\perp}(x) = \sum_{i \in E^{\perp}} x^i$$

の何れかであるとき Duadic 符号という．とくに，平方剰余符号は Duadic 符号である．$e(x) = \sum_{i \in E} x^i$ が冪等であるためには，$\mathbf{Z}/n\mathbf{Z}$ を 2 の乗法による作用で軌道分解したとき，E が軌道の和集合になっていればよい; $(\mathbf{Z}/n\mathbf{Z})^{\times}$ の乗法部分群を G とするとき

$$C_a = \{ag : g \in G\} \qquad (a \in \mathbf{Z}/n\mathbf{Z})$$

を a の軌道 (orbit) という．このとき $(\mathbf{Z}/n\mathbf{Z})^{\times}$ は互いに交わらない軌道の和集合に表せる．G としてとくに $g \in (\mathbf{Z}/n\mathbf{Z})^{\times}$ の生成する部分群を取ったとき

$$\mathbf{Z}/n\mathbf{Z} = \bigcup_a C_a, \quad a \neq a' \text{ ならば } C_a \cap C_{a'} = \phi$$

を，g の乗法による作用での軌道分解という．

(例) $\mathbf{Z}/119\mathbf{Z}$ は 2 の乗法による作用で以下のような軌道に分解される．

$$\begin{aligned}
C_0 &= \{0\},\\
C_1 &= \{1,2,4,8,16,32,64,9,18,36,72,25,50,100,\\
&\quad 81,43,86,53,106,93,67,15,30,60\},\\
C_3 &= \{3,6,12,24,48,96,73,27,54,108,97,\\
&\quad 75,31,62,5,10,20,40,80,41,82,45,90,61\},\\
C_7 &= \{7,14,28,56,112,105,91,63\},\\
C_{11} &= \{11,22,44,88,57,114,109,99,79,39,78,37,\\
&\quad 74,29,58,116,113,107,95,71,23,46,92,65\},\\
C_{13} &= \{13,26,52,104,89,59,118,117,115,111,103,\\
&\quad 87,55,110,101,83,47,94,69,19,38,76,33,66\},\\
C_{17} &= \{17,34,68\},\\
C_{21} &= \{21,42,84,49,98,77,35,70\},\\
C_{51} &= \{51,102,85\}.
\end{aligned}$$

ここで,$E = C_1 \cup C_7 \cup C_{11} \cup C_{17},\ E^{\perp} = C_3 \cup C_{13} \cup C_{21} \cup C_{51}$ とおくと $3E = E^{\perp}, 3E = E^{\perp}$ が成り立ち，$E, E^{\perp}$ は $\mathbf{Z}/119\mathbf{Z}$ の分割になる．

2.5 Cyclotomic Duadic 符号

$p = 2ef + 1$ を奇素数とする．$\mathbf{F}_p$ の原始元を g とし，$\mathbf{F}_p^\times$ を g^{2e} の乗法による作用で軌道分解したときの軌道を

$$C_i = \left\{ g^{2ex+i} : 0 \le x \le \frac{p-1}{2e} - 1 \right\} \quad (0 \le i \le 2e-1)$$

と記す．分割 $E, E^\perp$ がこれらの軌道の和集合であるとき，2 元 Duadic 符号を位数 $2e$ の Cyclotomic Duadic 符号という．

定理 2.5.1([1])
(1) p が以下の条件をみたすとき位数 $2e = 4$ の平方剰余符号と異なる Cyclotomic Duadic 符号が存在する．

$$\begin{cases} p \equiv 1 \pmod 8 \\ p = a^2 + 64b^2 \end{cases}$$

(2) p が以下の条件をみたすとき位数 $2e = 6$ の平方剰余符号と異なる Cyclotomic Duadic 符号が存在する．

$$\begin{cases} p \equiv 1, 7 \pmod{24} \\ p = x^2 + 27y^2 \end{cases}$$

(例) $\mathbf{F}_{31}^\times$ の $g^{2e} = 3^6$ による軌道分解は以下の通りである．

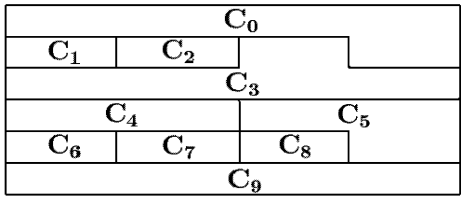
$$\begin{aligned} C_0 &= \{1, 16, 8, 4, 2\}, & C_1 &= \{3, 17, 24, 12, 6\} \\ C_2 &= \{9, 20, 10, 5, 18\}, & C_3 &= \{27, 29, 30, 15, 23\} \\ C_4 &= \{19, 25, 28, 14, 7\}, & C_5 &= \{26, 13, 22, 11, 21\} \end{aligned}$$

これら 6 つの軌道から，4 つの分割

$$\begin{aligned} (E, E^\perp) \;=\; & (C_0 \cup C_2 \cup C_4,\ C_1 \cup C_3 \cup C_5), \\ & (C_0 \cup C_1 \cup C_2,\ C_3 \cup C_4 \cup C_5), \\ & (C_0 \cup C_1 \cup C_5,\ C_2 \cup C_3 \cup C_4), \\ & (C_0 \cup C_4 \cup C_5,\ C_1 \cup C_2 \cup C_3), \end{aligned}$$

が得られ，最初の分割から平方剰余符号，残る分割から [31,16] パンクチャド Reed-Muller 符号と同値な符号が得られる．後者は平方剰余符号と同値でない ([1]).

各軌道の位数が異なる場合と比べ，前頁の例の様に，全ての軌道の位数が同じ場合のほうが組み合わせを考えやすい．



$\mathbf{C_0}$	$\mathbf{C_1}$
$\mathbf{C_2}$	$\mathbf{C_3}$
$\mathbf{C_4}$	$\mathbf{C_5}$
$\mathbf{C_6}$	$\mathbf{C_7}$
$\mathbf{C_8}$	$\mathbf{C_9}$
$\mathbf{C_{10}}$	$\mathbf{C_{11}}$

図 2.2 軌道分解

一般に，2 が mod p で $2e$ 乗剰余，すなわち

$$p \equiv 1 \bmod 2e \text{ かつ } 2^{\frac{p-1}{2e}} \equiv 1 \bmod p$$

のとき，全ての軌道の位数が同じとなり，分割の具体的な構成方法を与えることができる．

定理 2.5.2 $2e/l$ が偶数となるような $2e$ の約数 l に対し，$\mathbf{F}_p^\times$ の分割 $E_{l,m}, E_{l,m}^\perp$ $(0 \leq m \leq l-1)$ が以下の式で与えられる．

$$E_{l,m} = \bigcup_{a \equiv 0,\ldots,l-1 (2l)} C_a,$$
$$E_{l,m}^\perp = \bigcup_{a \equiv l,\ldots,2l-1 (2l)} C_a.$$

ここで $\mu = g^l$ となる．

とくに，$l = 1$ のとき $E_{1,0}, E_{1,0}^\perp$ は平方剰余と非剰余への分割となり，得られる符号は平方剰余符号となる．また，分割の総数は

$$\sum_{l|e} l$$

で与えられる．

(例) 12 乗剰余での例を示す．2 を 12 乗剰余とするような最小の素数は，$p = 601$ であり原始元として $g = 7$ がとれる．このとき軌道 C_i は

$$C_i = \{7^{12x+i} : 0 \leq x \leq 49\} \quad (0 \leq i \leq 11)$$

となる．12 の約数 $l = 1, 2, 3, 4, 6, 12$ の内，$12/l$ が偶数となる $l = 1, 2, 3, 6$ に対し，次の分割が存在する．

(1) $l=1$ のとき ; $E_{1,0} = C_0 \cup C_2 \cup C_4 \cup C_6 \cup C_8 \cup C_{10}$

(2) $l=2$ のとき ; $E_{2,0} = C_0 \cup C_1 \cup C_4 \cup C_5 \cup C_8 \cup C_9$

$E_{2,1} = C_1 \cup C_2 \cup C_5 \cup C_6 \cup C_9 \cup C_{10}$

(3) $l=3$ のとき ; $E_{3,0} = C_0 \cup C_1 \cup C_2 \cup C_6 \cup C_7 \cup C_8$

$E_{3,1} = C_1 \cup C_2 \cup C_3 \cup C_7 \cup C_8 \cup C_9$

$E_{3,2} = C_2 \cup C_3 \cup C_4 \cup C_8 \cup C_9 \cup C_{11}$

(4) $l=6$ のとき ; $E_{6,0} = C_0 \cup C_1 \cup C_2 \cup C_3 \cup C_4 \cup C_5$

$E_{6,1} = C_1 \cup C_2 \cup C_3 \cup C_4 \cup C_5 \cup C_6$

$E_{6,2} = C_2 \cup C_3 \cup C_4 \cup C_5 \cup C_6 \cup C_7$

$E_{6,3} = C_3 \cup C_4 \cup C_5 \cup C_6 \cup C_7 \cup C_8$

$E_{6,4} = C_4 \cup C_5 \cup C_6 \cup C_7 \cup C_8 \cup C_9$

$E_{6,5} = C_5 \cup C_6 \cup C_7 \cup C_8 \cup C_9 \cup C_{10}$

$\mathbf{C_0}$	$\mathbf{C_1}$
$\mathbf{C_2}$	$\mathbf{C_3}$
$\mathbf{C_4}$	$\mathbf{C_5}$
$\mathbf{C_6}$	$\mathbf{C_7}$
$\mathbf{C_8}$	$\mathbf{C_9}$
$\mathbf{C_{10}}$	$\mathbf{C_{11}}$

$\mathbf{C_0}$	$\mathbf{C_1}$
$\mathbf{C_2}$	$\mathbf{C_3}$
$\mathbf{C_4}$	$\mathbf{C_5}$
$\mathbf{C_6}$	$\mathbf{C_7}$
$\mathbf{C_8}$	$\mathbf{C_9}$
$\mathbf{C_{10}}$	$\mathbf{C_{11}}$

$\mathbf{C_0}$	$\mathbf{C_1}$
$\mathbf{C_2}$	$\mathbf{C_3}$
$\mathbf{C_4}$	$\mathbf{C_5}$
$\mathbf{C_6}$	$\mathbf{C_7}$
$\mathbf{C_8}$	$\mathbf{C_9}$
$\mathbf{C_{10}}$	$\mathbf{C_{11}}$

$\mathbf{C_0}$	$\mathbf{C_1}$
$\mathbf{C_2}$	$\mathbf{C_3}$
$\mathbf{C_4}$	$\mathbf{C_5}$
$\mathbf{C_6}$	$\mathbf{C_7}$
$\mathbf{C_8}$	$\mathbf{C_9}$
$\mathbf{C_{10}}$	$\mathbf{C_{11}}$

図 2.3　p=607, m=0 における分割

ここで

$$E_{l,m}^{\perp} = I \backslash E_{l,m} \ , \ I = \bigcup_{0<i<11} C_i.$$

2 を $2e$ 乗剰余に持つ 3000 以下の素数を表にして記載しておく.

表 2.1. 2 を $2e$ **乗剰余に持つ素数** $p(\leq 3000)$

	$l\|e$	p (≤ 3000)
$2e=4$	$1,2$	$73,89,113,233,257,281,337,353,577,593,601,$ $617,881,937,1033,1049,1097,1153,1193,1201,$ $1217,1249,1289,1433,1481,15531601,1609,$ $1721,1753,1777,1801,1889,1913,2089,2113,$ $2129,2273,2281,2393,2441,2473,2593,2657,$ $2689,2833,2857$
$2e=6$	$1,3$	$31,127,223,433,439,457,601,727,919,1327,$ $1399,1423,1471,1657,1753,1777,1801,1831,$ $1999,2017,2089,2113,2413,2281,2287,2383,$ $2671,2689,2767,2791,2833$
$2e=8$	$1,2,4$	$73,89,233,257,337,601,881,937,1217,1249,$ $1289,1433,1553,1609,1721,1777,1801,1913,$ $2089,2113,2441,2593,2657,2833$
$2e=10$	$1,5$	$151,241,431,641,911,2351$
$2e=12$	$1,2,3,6$	$601,1753,1777,1801,2089,2113,2281,2689,2833$
$2e=14$	$1,7$	$631,673,953,2143,2857$
$2e=16$	$1,2,4,8$	$257,337,881,2113,2593,2657$
$2e=18$	$1,3,9$	$127,1657,1801,2089$
$2e=20$	$1,2,5,10$	この範囲には存在しない
$2e=22$	$1,11$	1321
$2e=24$	$1,2,3,4,$ $6,12$	$601,1777,1801,2089,2113,2833$

2.6 高次相互法則

mod p で 2 が $2e$ 乗剰余となるような素数 p が与えられれば，定理 2.5.2 を用いて位数 $2e$ の平方剰余符号と異なる Cyclotomic Duadic 符号を構成できる定理 2.5.1 についていえば，$p\equiv 1(\mathrm{mod}\ 8)$ かつ $p=a^2+64b^2$ をみたす素数が無限個存在することはすでに示されているが，$p\equiv 1,7(\mathrm{mod}\ 24)$ かつ $p=x^2+27y^2$ をみたす素数が無限個存在するかどうかは未解決のまま残されていた 2.6 節では，

そのような素数もまた無限個存在すること，したがって定理 2.5.2 により構成される Duadic 符号は無限個存在することを示す

補題 2.6.1 mod p で 2 が N 乗剰余であるための必要十分条件は

$$x^N \equiv 2 \mod p$$

で相異なる N 個の解をもつことである

(証明) $2^{\frac{p-1}{N}} \equiv 1(\mathrm{mod}\ p)$ ならば 2 を原始元 g のべきで表したときの指数は N の倍数でなければならない $2 = g^{Nl}$. このとき $g^{l+\frac{p-1}{N}k}(0 \leq k \leq N-1)$ は相異なる N 個の解である逆にもし $x^N \equiv 2 \mod\ p$ に解があれば，両辺を $\frac{p-1}{N}$ 乗して $2^{\frac{p-1}{N}} \equiv 1\ (\mathrm{mod}\ p)$ を得る■

定理 2.6.2 $(m,n) = 1$ のとき

$$X^m \equiv a\ ,\ X^n \equiv a\ \ (\mathrm{mod}\ p)$$

が相異なる 1 次式に分解することと

$$X^{mn} \equiv a(\mathrm{mod}\ p)\ \ (\mathrm{mod}\ p)$$

が相異なる 1 次式に分解することは同値である

(証明) m, n は p で割れないと仮定してよく，補題 2.6.1 より

$$a^{\frac{p-1}{m}} \equiv a^{\frac{p-1}{n}} \equiv 1 \bmod p \iff a^{\frac{p-1}{mn}} \equiv 1 \bmod p$$

をいえばよい $(m,n) = 1$ なら $mx + ny = 1$ となる $x, y \in \mathbf{Z}$ が存在し

$$\frac{p-1}{n}x + \frac{p-1}{m}y = \frac{p-1}{mn}$$

がいえるここで，$a^{\frac{p-1}{m}} \equiv a^{\frac{p-1}{n}} \equiv 1(\mathrm{mod}p)$ であるので，先の関係式から

$$a^{\frac{p-1}{mn}} \equiv (a^{\frac{p-1}{m}})^x (a^{\frac{p-1}{n}})^y \equiv 1 \mod p$$

が成り立つまた,

$$a^{\frac{p-1}{m}} = (a^{\frac{p-1}{mn}})^n, a^{\frac{p-1}{n}} = (a^{\frac{p-1}{mn}})^m$$

より逆は明らか■

$f(x) \in \mathbf{Z}[x]$ を $monic$ な既約多項式とする $f(x)$ の係数を p で割った余りで置きかえた $\mathbf{F}_p$ 係数の多項式を $f_p(x)$ とかく $f_p(x)$ が $\mathbf{F}_p[x]$ で相異なる 1 次式に分解するような素数 p の全体を

$$Spl\{f(x)\}$$

と書き，$Spl\{f(x)\}$ に属する素数 p を決定する規則を $f(x)$ の高次相互法則という．例えば，

$$\begin{aligned}
&Spl\{x^2-2\} = \{p : \text{素数} \mid p \equiv \pm 1 (\mathrm{mod}\ 8)\},\\
&Spl\{x^3-2\} = \{p : \text{素数} \mid p = x^2+27y^2, p \equiv 1 (\mathrm{mod}\ 3)\},\\
&Spl\{x^4-2\} = \{p : \text{素数} \mid p = a^2+64b^2, p \equiv 1 (\mathrm{mod}\ 8)\}.
\end{aligned}$$

$\prod$ を素数全体の集合，T をその部分集合とする実数 $x \geq 1$ を取り

$$\sigma(T,x) = \frac{|\{p \in T : p < x\}|}{|\{p \in \prod : p < x\}|}$$

とおく $\lim_{t\to\infty} \sigma(T,x)$ が存在するとき，これを $\sigma(T)$ と書き，T は密度 $\sigma(T)$ をもつという $0 \leq \sigma(T) \leq 1$ である有限集合 T に対しては $\sigma(T) = 0$ であり，したがって，ある条件を満たす素数の集合 T に対し，$\sigma(T) \neq 0$ ならば，T は無限集合である．

定理 2.6.3 (チェボタレフの弱密度定理)
$f(x) \in \mathbf{Z}[x]$ を既約多項式とし，K_f を $f(x)$ の $\mathbf{Q}$ 上の最小分解体とする K_f の $\mathbf{Q}$ 上の拡大次数を $[K_f : \mathbf{Q}] = n$ とすれば

$$\sigma(Spl\{f(x)\}) = \frac{1}{n} (\neq 0).$$

定理 2.6.4 mod p で 2 が $2e$ 乗剰余となるような素数 p は無限個存在するとくに

$$\begin{aligned}
&Spl\{x^6-2\} = \{p : p = x^2+27y^2,\ p \equiv 1, 7 (24)\},\\
&Spl\{x^{12}-2\} = \{p : p = x^2+27y^2 = a^2+64b^2, p \equiv 1 (24)\},
\end{aligned}$$

は無限集合である．

系 2.6.5 位数 $2e$ の Duadic 符号は無限個存在する

第3章　$\mathbf{Z}/p^2\mathbf{Z}$上の長さp^eの巡回符号の多項式表現

3.1　序

誤り訂正符号では，符号アルファベットに有限体の元を用いることが多いが，有限環 $\mathbf{Z}/p^m\mathbf{Z}$ 上の符号は，$\mathbf{Z}_p = \mathbf{Z}/p\mathbf{Z}$ 上の符号をもとに構成した場合，訂正能力を落とさずに，用いるアルファベットを増やすことができるという利点があり，通信の効率化に役立つものと考えられる．とくに $\mathbf{Z}/4\mathbf{Z}$ 上での符号について多くの研究成果が発表されているが，3 章では一般に $\mathbf{Z}_{p^2} = \mathbf{Z}/p^2\mathbf{Z}$ 上の長さ p^e の巡回符号について論じる．ここで，有限環 $\mathbf{Z}/p^m\mathbf{Z}$ 上の符号長 n の線形符号 $\mathcal{C}$ とは $(\mathbf{Z}/p^m\mathbf{Z})^n$ の加法部分群のことであり，巡回符号とは，有限体上の巡回符号と同様，任意の符号語の巡回シフトがまた符号語となるような線形符号のことである．符号語を多項式表現すれば，巡回符号は多項式環 $\mathbf{R}_{p^2} = \mathbf{Z}_{p^2}[x]/(x^n - 1)$ のイデアルと見なすことができるが，有限体上とは異なり，$\mathbf{R}_{p^2}$ が単項イデアル環，すなわち生成多項式がつねにただ一つだけ決まるような環になるのは，符号長 n が p と素の場合に限られ，$(n, p) \neq 1$ の場合には単項イデアル整域ではない ([5])．そのため，符号の構造を調べるにあたっては，$(n, p) = 1$ と条件をつけたり，生成行列が利用されたりすることが多いが，符号化および復号処理の高速化を計るためには，この場合にも多項式表現を与えておくことが望ましい．以下ではとくに，有限環上の符号特有の，符号長 $n = p^e$ の場合の多項式表現を決定する．この場合には，$p = 2$ の場合を論じた [1] にならって，$x - 1$ のベキを $\mathbf{Z}_{p^2}$ 加群としての基底に取るほうが扱い易い．ただし，p を 2 に固定したときに比べるとより精密な議論が必要とされ，必ずしも $p = 2$ のときの議論がそのまま通用するわけではない．$x - 1$ がベキ零であること，とくにそのベキ零指数が $n + \frac{p-1}{p}n$ であることを利用して，3 章では，$\mathbf{Z}_{p^2}$ 上の巡回符号およびその双対符号の生成多項式を決定する．さらに，巡回符号とその双対符号の関係を示すことで，情報系列の多項式表現と符号語数を明らかにし，符号長 $n = p^e$ の巡回符号の構造を決定する．

3.2　多項式環 $Z_{p^2}[x]/(x^n-1)$

3 章での目的は，$\mathbf{Z}_{p^2}$ 上の巡回符号の生成多項式および検査多項式の決定であるが，巡回符号は多項式環 $\mathbf{R}_{p^2}=\mathbf{Z}_{p^2}[x]/(x^n-1)$ のイデアルであるから，この節でまず多項式環 $\mathbf{R}_{p^2}$ について，3 章の議論の基礎となる基本性質を述べておく．特に**補題 3.2.1　(2) 式**は，符号長が p と素な場合とそうでないときを区別する性格のものであって，以降の議論で中心的な役割を果たす；まず，$\mathbf{Z}_{p^2}$ の任意の元 c は $a,b\in \mathbf{Z}_p$ をとって $c=a+pb$ と表すことができるから，$\mathbf{R}_{p^2}$ の多項式は
$f_1(x),f_2(x)\in \mathbf{R}_p$
$=\mathbf{Z}_p[x]/(x^n-1)$ をとって，$f(x)=f_1(x)+pf_2(x)$ と表すことができる．さらに，$\mathbf{Z}_p$ 上でのベクトル空間 $\mathbf{R}_p$ での基底として $1,(x-1),\cdots,(x-1)^{n-1}$ がとれるから，$\mathbf{R}_{p^2}$ の多項式は以下の式で表すことができる．

$$\sum_{i=0}^{n-1}c_i(x-1)^i=\sum_{i=0}^{n-1}a_i(x-1)^i+p\sum_{i=0}^{n-1}b_i(x-1)^i$$
$$(c_i=a_i+pb_i\in \mathbf{Z}/p^2\mathbf{Z}).$$

$f(x)$ が $\mathbf{R}_p$(または $\mathbf{R}_{p^2}$) の単元であるとは $f(x)g(x)=1$ となるような $f(x)$ の逆元 $g(x)$ が $\mathbf{R}_p$(または $\mathbf{R}_{p^2}$) 内に存在することを言う．

補題 3.2.1:
(1)　$f(x)=\sum_{i=0}^{n-1}c_i(x-1)^i$ を $\mathbf{R}_p$ の元とする時，$f(1)=c_0\neq 0$ ならば $f(x)$ は $\mathbf{R}_p$ の単元．
(2)　$f(x)=\sum_{i=0}^{n-1}c_i(x-1)^i$ を $\mathbf{R}_{p^2}$ の元とする時，$f(1)=c_0\not\equiv 0 \pmod p$ ならば $f(x)$ は $\mathbf{R}_{p^2}$ の単元．
証明:(1)　$x-1=y$ とおく．$f(x)=\sum_{i=0}^{n-1}c_iy^i$ と $(x-1)^n=y^n$ は $c_0\neq 0$ のとき，またその時に限って $\mathbf{Z}_p[y]$ で互いに素で

$$f(y)g(y)+h(y)y^n=1$$

をみたす $g(y),h(y)\in \mathbf{Z}_p[y]$ が存在する．$n=p^e$ なら
$y^n=(x-1)^n\equiv x^n-1 \pmod p$ だから $\mathbf{R}_p$ では $y^n=0$ で $g(x-1)$ が $f(x)$ の $\mathbf{R}_p$ での逆元である．
(2)　$f(x)=f_1(x)+pf_2(x)$ $(f_1(x),f_2(x)\in \mathbf{R}_p)$ と書くとき $c_0\not\equiv 0 \pmod p$ は $f_1(x)$ が $\mathbf{R}_p$ の単元であることと同値である．したがって (1) より ($\mathbf{R}_p$ で)$f_1(x)g_1(x)=1$ をみたす $g_1(x)\in \mathbf{R}_p$ が存在する．とくに $f_1(x)g_1(x)-1$ は $\mathbf{R}_{p^2}$

では p の倍多項式になるから $f_1(x)$, $f_2(x)$, $g_1(x)$ を与えるとき

$$pg_2(x)f_1(x) \equiv f_1(x)g_1(x) - 1 + pf_2(x)g_1(x) \bmod p^2$$

をみたす

$$g_2(x) = \left\{ \frac{f_1(x)g_1(x) - 1}{p} + f_2(x)g_1(x) \right\} f_1(x)^{-1}$$

が $\mathbf{R}_p$ で一意に決まる．$g(x) = g_1(x) + pg_2(x)$ とおけば $\mathbf{R}_{p^2}$ で

$$f(x)g(x) = 1$$

が成り立ち $g(x) = g_1(x) + pg_2(x)$ が $f(x)$ の $\mathbf{R}_{p^2}$ における逆元である． ■

補題 3.2.2: $n = p^e$ $(e > 0)$ とした時,

$$(x-1)^n \equiv x^n - 1 + p(x-1)^{\frac{n}{p}} G_n(x) \pmod{p^2}.$$

とくに $\mathbf{R}_{p^2}$ において

$$(x-1)^n = p(x-1)^{\frac{n}{p}} G_n(x)$$

となり，$G_n(x)$ は単元である．
証明 : $p = 2$ のときは簡単な計算で $G_n(x) = 1$ がわかることを注意しておく ([1]).
p を奇素数とする．このとき，$(x-1)^p$ を展開すると

$$(x-1)^p = x^p - 1 + \sum_{k=1}^{p-1} \binom{p}{k} x^k (-1)^{p-k}.$$

ここで,

$$\begin{aligned} &\binom{p}{k} x^k (-1)^{p-k} + \binom{p}{p-k} x^{p-k} (-1)^k \\ =&\binom{p}{k} x^k (-1)^k (x^{p-2k} - 1) \end{aligned}$$

が成り立つので,

$$(x-1)^p = x^p - 1 + \sum_{k=1}^{\frac{p-1}{2}} \binom{p}{k} x^k (-1)^k (x^{p-2k} - 1).$$

また，$1 \leq k \leq (p-1)/2$ において $\binom{p}{k} \equiv 0 \pmod{p}$,
$(x-1) \mid (x^{p-2k}-1)$ となるので,

$$(x-1)^p = x^p - 1 + p(x-1)G(x), \tag{1}$$

$$G(x) = \frac{1}{p}\sum_{k=1}^{\frac{p-1}{2}} \binom{p}{k} x^k (-1)^k \sum_{i=0}^{p-2k-1} x^i \tag{2}$$

と表せる．(1) において，x のかわりに $x^{\frac{n}{p}}$ として

$$(x^{\frac{n}{p}}-1)^p = x^n - 1 + p(x^{\frac{n}{p}}-1)G(x^{\frac{n}{p}}). \tag{3}$$

ここで n が p のベキであることに注意して両辺を計算する．$f(x) \equiv g(x) \pmod{p}$ なら $f(x)^p \equiv g(x)^p \pmod{p^2}$ が成り立つことに注意すると

$$(x-1)^{\frac{n}{p}} \equiv x^{\frac{n}{p}} - 1 \pmod{p}$$

この両辺を p 乗して

$$(x-1)^n \equiv (x^{\frac{n}{p}}-1)^p \pmod{p^2}$$

を得る．また，$(x-1)^{\frac{n}{p}} \equiv x^{\frac{n}{p}} - 1 \pmod{p}$ だから

$$p(x-1)^{\frac{n}{p}} \equiv p(x^{\frac{n}{p}}-1) \pmod{p^2}$$

が成り立つ．したがって，(3) から

$$\begin{aligned}(x-1)^n &\equiv x^n - 1 + p(x-1)^{\frac{n}{p}} G(x^{\frac{n}{p}}) \pmod{p^2} \\ &= x^n - 1 + p(x-1)^{\frac{n}{p}} G_n(x)\end{aligned}$$

が成り立つ．ただし $G_n(x) = G(x^{\frac{n}{p}})$.
次に $G_n(1) = G(1) \not\equiv 0 \pmod{p}$ を示すことで $G_n(x)$ が単元であることを示す.
(2) に $x = 1$ を代入して

$$\begin{aligned}G(1) =& \frac{1}{p}\sum_{k=1}^{\frac{p-1}{2}} \binom{p}{k} (-1)^k (p-2k) \\ \equiv& \frac{2}{p}\sum_{k=1}^{\frac{p-1}{2}} \binom{p}{k} (-1)^{k+1} k \pmod{p}\end{aligned} \tag{4}$$

ところで $(x+1)^p = \sum_{k=0}^{p} \binom{p}{k} x^k$ の両辺を微分して，$x=-1$ を代入すると

$$\sum_{k=1}^{p} \binom{p}{k} k(-1)^{k+1} = 0. \tag{5}$$

(5) 式の左辺の $k=a$ の項と $k=p-a$ の項の和は

$$\begin{aligned}
&\binom{p}{a} a(-1)^{a+1} + \binom{p}{p-a}(p-a)(-1)^{p-a-1} \\
=&(-1)^{a+1}\binom{p}{p-a}\left\{a + (-1)^{p-2a}(p-a)\right\} \\
=&(-1)^{a+1}\binom{p}{p-a}(2a-p) \\
\equiv&(-1)^{a+1}\binom{p}{p-a}2a \qquad (\mathrm{mod}\ p^2).
\end{aligned}$$

したがって，(5) は，$k=p$ の項が $p(-1)^{p+1} = p$ になることに注意して，

$$\begin{aligned}
&p + 2\sum_{k=1}^{\frac{p-1}{2}} \binom{p}{k}(-1)^{k+1}k \equiv 0 \quad (\mathrm{mod}\ p^2) \\
\therefore\ \ &2\sum_{k=1}^{\frac{p-1}{2}} \binom{p}{k}(-1)^{k+1}k \equiv -p \pmod{p^2}.
\end{aligned}$$

となる．上式の両辺は p を因数に持つので

$$\frac{2}{p}\sum_{k=1}^{\frac{p-1}{2}} \binom{p}{k}(-1)^{k+1}k \equiv -1 \pmod{p}.$$

よって (4) より

$$G_n(1) = G(1) \equiv -1 \not\equiv 0 \quad (\mathrm{mod}\ p),$$

となり，$G_n(x)$ は $\mathbf{R}_{p^2}$ の単元である　■

補題 3.2.3:　$x-1$ は $\mathbf{R}_{p^2}$ においてベキ零であり，そのベキ零指数，すなわち $(x-1)^\gamma = 0$ をみたす最小の正整数は $\gamma = n + \frac{p-1}{p}n$ である．

証明: $\mathbf{R}_{p^2}$ では**補題 3.2.2** より，

$$(x-1)^n = p(x-1)^{\frac{n}{p}}G_n(x)$$

両辺に $(x-1)^{\frac{p-1}{p}n}$ を掛けて再び上式を用いると，

$$\begin{aligned}(x-1)^{n+\frac{p-1}{p}n} &= p(x-1)^n G_n(x) \\ &\equiv p^2(x-1)^{\frac{n}{p}} G_n(x)^2 \\ &\equiv 0 \pmod{p^2}. \end{aligned} \tag{1}$$

となり $x-1$ は $\mathbf{R}_{p^2}$ でベキ零で $\gamma \leq n + \frac{p-1}{p}$ であることがわかる．ここで l $(\leq \frac{p-1}{p}n)$ に対し，

$$(x-1)^{n+l} \equiv p(x-1)^{l+\frac{n}{p}} G_n(x) \pmod{p^2}. \tag{2}$$

補題 3.2.2 より，$G_n(x)$ は $\mathbf{R}_{p^2}$ で単元であるので，

$$pG_n(x) \not\equiv 0 \pmod{p^2}.$$

したがって，(2) が $\bmod p^2$ で 0 となるためには，$(x-1)^{\frac{n}{p}+l} \equiv 0 \pmod{p}$ でなければならない．ここで，$\frac{n}{p} + l < n$ と仮定すると，$(x-1)^{\frac{n}{p}+l}$ は最高次の係数が 1 で次数が n 未満の多項式だから，とくに

$$(x-1)^{\frac{n}{p}+l} \not\equiv 0 \pmod{p}$$

よって $\frac{n}{p} + l \geq n$ すなわち $l \geq \frac{p-1}{p}n$ でなければならない．(1) と合わせて考えると，ベキ零指数 γ は $n + \frac{p-1}{p}n$ となる．■

3.3 イデアル基底

3.3 節ではまず，**定理 3.3.1** として，$\mathbf{Z}_{p^2}$ 上における符号長 $n = p^e$ の巡回符号の生成多項式が，$p = 2$ のときと同様 3 通りに分けて与えられることを述べる．以下 $f(x)$ で生成されるイデアルを記号 $\langle f(x) \rangle$ で表す.

定理 3.3.1: $\mathcal{I}$ は R_{p^2} のイデアルとする．
(1) モニック多項式を含まないとき；正整数 m が唯一つ存在して

$$\mathcal{I} = \langle\ p(x-1)^m\ \rangle.$$

(2) モニック多項式を含む単項イデアルのとき；次の形の生成元が一意的に決まる．

$$\mathcal{I} = \langle (x-1)^s + p\sum_{i=0}^{m-1} c_i(x-1)^i \rangle.$$

ここで s は $\mathcal{I}$ に含まれる最小次数のモニック多項式の次数，m は $p(x-1)^m \in \mathcal{I}$ である様な最小の正整数である (m の上限を**定理 3.3.2** で与える).
(3) 単項ではないとき；

$$\mathcal{I} = \langle\ (x-1)^s + p\sum_{i=0}^{m-1} c_i(x-1)^i\ ,\ p(x-1)^m\ \rangle.$$

s は $\mathcal{I}$ の中で次数の最小のモニック多項式の次数，m は $p(x-1)^m \in \mathcal{I}$ となる最小の正整数とする．ただし，

$$p(x-1)^m \notin \langle (x-1)^s + p\sum_{i=0}^{m-1} c_i(x-1)^i \rangle.$$

証明：(1) $f(x) = \sum_{i=0}^{m} c_i(x-1)^i$ を $\mathcal{I}$ の中で最も次数の低い 0 でない多項式とし，その次数を m とする．仮定より $f(x)$ はモニックではないので $c_m \equiv 0 \pmod{p}$ となる．実際，$c_m \not\equiv 0 \pmod{p}$ ならば，c_m の逆元 c_m^{-1} が存在し，$c_m^{-1}f(x)$ は $\mathcal{I}$ に含まれるモニック多項式である．
また，$k < m$ に対し，$c_k \not\equiv 0 \pmod{p}$ が存在すると仮定すると，$pf(x)$ は 0 でなく m よりも次数の低い多項式となり条件に反する．よって，$0 \le i \le m$ で $c_i \equiv 0 \pmod{p}$ となり

$$f(x) = p\sum_{i=0}^{m} d_i(x-1)^i \quad (d_i \in \mathbf{Z}_p). \tag{1}$$

さらに，イデアル $\mathcal{I}$ に含まれる多項式 $\sum_{i=0}^{n-1} a_i(x-1)^i$ について，
$a_i \not\equiv 0 \pmod{p}$ かつ $m+1 \le i$ であるような i のうち最大のものを j とする．いま $a_{n-1} = p\alpha_{n-1}$ $(\alpha_{n-1} \in \mathbf{Z}_p)$ とすると

$$\sum_{i=0}^{n-1} a_i(x-1)^i - \alpha_{n-1}d_m^{-1}(x-1)^{n-1-m}f(x)$$

は $n-2$ 次以下で，p で割れない最大次数が j の多項式となる．同様に繰り返して次数を下げてゆくと，最高次の係数が p で割れないような，j 次の多項式が $\mathcal{I}$ に含まれることとなり，モニック多項式を含まないという仮定に反する．よって，全ての $0 \le i \le n-1$ について $a_i \equiv 0 \pmod{p}$ がいえる．言いかえると $\mathcal{I}$ に含まれる全ての多項式の係数は全て p で割り切れる．
ここで (1) 式において，t を $d_t \not\equiv 0 \pmod{p}$ である最小の正整数と仮定すると，

$$f(x) = p(x-1)^t\left\{ d_t + \sum_{i=t+1}^{m} d_i(x-1)^{i-t} \right\}.$$

補題 3.2.1 より $\left\{ d_t + \sum_{i=t+1}^{m} d_i(x-1)^{i-t} \right\}$ は $\mathbf{R}_{p^2}$ の単元であり，$\mathcal{I}$ に含まれる多項式の最小次数は m であるので，$\mathcal{I}$ には $p(x-1)^m$ が含まれる．$\mathcal{I}$ に含まれる多項式は m 次以上で，係数は全て p で割れているから，$p(x-1)^m$ がイデアル $\mathcal{I}$ の生成元となる．

(2) $\mathcal{I} = \langle\, f(x) \,\rangle$ とする．$f(x)$ はモニック多項式とするので，
$f(x) = f_1(x) + pf_2(x)$, $f_i(x) \in \mathbf{R}_p$, $f_1(x) \neq 0$ と表せる．$f_1(x)$ は $\mathbf{R}_p$ の巡回符号の生成多項式になるので $f_1(x) = (x-1)^s$, $(0 < s < n)$ となる．したがって

$$f(x) = (x-1)^s + p\sum_{i=0}^{n-1} c_i(x-1)^i.$$

m を $p(x-1)^m \in \mathcal{I}$ となる最小の正整数とすると

$$\mathcal{I} = \langle\, (x-1)^s + p\sum_{i=0}^{m-1} c_i(x-1)^i \,\rangle.$$

一意性を示す．$\mathcal{I} = \langle\, g(x) \,\rangle$ となる $\mathbf{R}_{p^2}$ の多項式 $g(x)$ が存在するとすると，$g(x)$ は以下の形をとる．

$$g(x) = (x-1)^s + p\sum_{i=0}^{m-1} d_i(x-1)^i.$$

$f(x) \neq g(x)$ なら $pc_i \neq pd_i$ となる i があるから，k を $pc_k \neq pd_k$ となる最小の正整数とする．この時

$$f(x) - g(x) = p(x-1)^k \sum_{i=0}^{m-1-k} (c_i - d_i)(x-1)^i \in \mathcal{I}. \ (1)$$

ここで $c_k - d_k \not\equiv 0 \pmod{p}$ だから

$$\sum_{i=0}^{m-1-k}(c_i - d_i)(x-1)^i = c_k - d_k + \sum_{i=1}^{m-1-k}(c_i - d_i)(x-1)^i$$

は単元であり，したがって (1) より $p(x-1)^k \in \mathcal{I}$. しかし $k < m$ だから，これは m の最小性に反する．よって，$f(x) = g(x)$ であり，基底は一意的である．■

定理 3.3.2: $\mathcal{I}$ をモニック多項式で生成されるような $\mathbf{R}_{p^2}$ の単項イデアルとし，生成元を

$$\begin{aligned} f(x) =&(x-1)^s + p\sum_{i=0}^{m-1} c_i(x-1)^i \\ =&(x-1)^s + p(x-1)^t h(x) \\ &(\text{ここで } t \text{ は } c_t \not\equiv 0 \pmod p \text{ となる最小の正整数}) \end{aligned}$$

とおく．

(**Case 1**) $h(x) \neq 0$ ならば

$p \neq 2$: (1) $\dfrac{n}{p} \neq n+t-s$; $m \leq \min\{s, \dfrac{n}{p}, n+t-s\}$.

(2) $\dfrac{n}{p} = n+t-s$; $m \leq \min\{s, n+k-s\}$.

ここで k は $c_k \neq 0$ となる，t よりも大きい最小の正整数.

$p = 2$: (1) $\dfrac{n}{p} \neq n+t-s$; $m = \min\{s, \dfrac{n}{p}\}$.

(2) $\dfrac{n}{p} = n+t-s$; $m = \min\{s, n+k-s\}$.

k は$a_k = 1$ となる t よりも大きい最小の正整数.

k が存在しないときは $m = s$.

(**Case 2**) $h(x) = 0$ の時. $m = \{s, \dfrac{n}{p}\}$.

証明:(Case 1) $p = 2$ の場合については [1] を参照.
$p \neq 2$ の時を示す．生成多項式 $f(x)$ の両辺に p を掛けると $pf(x) = p(x-1)^s$ より，

$$p(x-1)^s \in \mathcal{I}.$$

また，両辺に $(x-1)^{n-s}$ を掛けると，**補題 3.2.2** より，

$$\begin{aligned} & f(x)(x-1)^{n-s} \\ =& (x-1)^n + p(x-1)^{n+t-s}h(x) \\ =& -p(x-1)^{\frac{n}{p}}G_n(x) + p(x-1)^{n+t-s}h(x). \end{aligned}$$

ここで，$h(0) \not\equiv 0 \pmod p$, $G_n(0) = 1$.
(1) $\frac{n}{p} \leq n+t-s$ の時.

$$f(x)(x-1)^{n-s} = -p(x-1)^{\frac{n}{p}}\{G_n(x) + (x-1)^{n+t-s-\frac{n}{p}}h(x)\}.$$

ここで，$f_0(x) = (x-1)^{n+t-s-\frac{n}{p}} h(x)$ とすると，

$$deg\, G_n(x) < n\ ,\ G_n(0) = 0,$$
$$deg\, f_0(x) < n\ \ ,\ \ f_0(0) \not\equiv 0\ \ (mod\ p),$$

であるので，$f_0(x) + f_1(x)$ は単元となる．よって，

$$p(x-1)^{\frac{n}{p}} \in \mathcal{I}.$$

(2) $\frac{n}{p} > n + t - s$ の時.

$$f(x)(x-1)^{n-s} = p(x-1)^{n+t-s}\left\{(x-1)^{\frac{n}{p}-n-t+s} G_n(x) + h(x)\right\}.$$

ここで，$f_2(x) = (x-1)^{\frac{n}{p}-n-t+s} G_n(x)$ とすると，
$deg\, f_2(x) < n$ ，$f_2(0) = 0$ であるので，$f_2(x) + h(x)$ は単元となる．よって，

$$p(x-1)^{n+t-s} \in \mathcal{I}.$$

(Case 2) R_{p^2} の任意の元は以下のように表せる．

$$g(x) = \sum_{i=0}^{n-1} c_i (x-1)^i + p \sum_{i=0}^{n-1} d_i (x-1)^i.$$

ここで $f(x)g(x) = p(x-1)^m$ が成り立つとすると，

$$\sum_{i=0}^{n-1} c_i (x-1)^{i+s} \equiv 0\ \ (mod\ p).$$

この時，$i \leq n - s - 1$ で $c_i = 0$ は明らか．よって，

$$f(x)g(x) = p(x-1)^{\frac{n}{p}} A(x) + p(x-1)^s B(x)$$
$$(A(x), B(x) \text{ は単元}).$$

Case 1 と同様に考えると，$m \leq \min\{s, \frac{n}{p}\}$. ■

3.4　双対符号

3.3 前節の結果を踏まえて 3.4 節では，巡回符号 $\mathcal{C}$ を与えたとき，その双対符号 $\mathcal{C}^{\perp}$ の生成多項式を決定する．$a(x)$ の次数を r とし，$a^*(x) = x^r a\left(\frac{1}{x}\right)$ を $a(x)$ の相反多項式とする． また，イデアル $\mathcal{I}$ に対し

$$\mathcal{A}_{\mathcal{I}} = \{g(x) \mid f(x)g(x) = 0\ (\forall f(x) \in \mathcal{I})\}$$

を$\mathcal{I}$の零化イデアル (annihilator) と呼ぶ．$\mathcal{I}$に対応する巡回符号を$\mathcal{C}$とした時，双対符号$\mathcal{C}^{\perp}$に対応するイデアルは

$$\mathcal{A}_{\mathcal{I}}^{*} = \{g(x)^{*} \mid g(x) \in \mathcal{A}_{\mathcal{I}}\}$$

で与えられる．以下$\mathcal{A}_{\mathcal{I}}$を決定する．

補題 3.4.1[1]: $\mathcal{I} = \langle (x-1)^{s} + p(x-1)^{t}h(x)\ ,\ p(x-1)^{m} \rangle$ なら $p(x-1)^{r} \in A_{\mathcal{I}}$ となる最小の正整数rは，

$$r = n - s.$$

定理 3.4.2: $\mathcal{I} = \langle (x-1)^{s} \rangle$, $(s < n)$ とすると

$$(1)\ s > \frac{n}{p}:\ \mathcal{A}_{\mathcal{I}} = \langle (x-1)^{\frac{p-1}{p}n} - pG_{n}(x)\ ,\ p(x-1)^{n-s} \rangle.$$
$$(2)\ s \leq \frac{n}{p}:\ \mathcal{A}_{\mathcal{I}} = \langle (x-1)^{n-s} - p(x-1)^{\frac{n}{p}-s}G_{n}(x) \rangle.$$

証明: (1) のみ示す ((2)) についても同様).
(1) $s > \frac{n}{p}$ なら $n + s - \frac{n}{p} \geq n$ だから**補題 3.2.2** より

$$(x-1)^{\frac{p-1}{p}n+s} = p(x-1)^{s}G_{n}(x)$$

したがって，イデアル$\mathcal{I}$の基底$(x-1)^{s}$に対して，

$$\left\{(x-1)^{\frac{p-1}{p}n} - pG_{n}(x)\right\}(x-1)^{s} = 0.$$
$$\therefore\ \ (x-1)^{\frac{p-1}{p}n} - pG_{n}(x) \in \mathcal{A}_{\mathcal{I}}.$$

とくに，$\mathcal{A}_{\mathcal{I}}$はモニック多項式を含むので，**定理 3.3.1** より

$$\begin{cases} \mathcal{A}_{\mathcal{I}} = \langle F(x)\ ,\ p(x-1)^{j} \rangle. \\ F(x) = (x-1)^{u} + p(x-1)^{v}H(x),\ \ u \leq \dfrac{p-1}{p}n. \end{cases}$$

とおくことができる．**補題 3.4.1** より $j = n - s$. $\mathcal{A}_{\mathcal{I}} \ni pF(x) \equiv p(x-1)^{u} \bmod p^{2}$ で j の最小性より $n - s \leq u$. 結局

$$0 \leq v < n - s,\ \ n - s \leq u \leq \frac{p-1}{p}n \tag{1}$$

である．いま $\mathbf{R}_{p^2}$ で，

$$(x-1)^s F(x) = (x-1)^{u+s} + p(x-1)^{s+v} H(x) = 0$$

であるが，この中辺は，$u+s \geq n$ より**補題 3.2.2** を用いて
$(x-1)^{u+s} = p(x-1)^{u+s-\frac{p-1}{p}n} G_n(x)$ なので

$$p(x-1)^s \Big\{ (x-1)^{u-\frac{p-1}{p}n} G_n(x) + (x-1)^v H(x) \Big\} = 0.$$

が成り立たねばならないが，$H(x), G_n(x)$ はどちらも単元だから，$u - \frac{p-1}{p}n \neq v$ なら $\{\ \}$ 内は単元で，これは不可能．ゆえに $u = v + \frac{p-1}{p}n \geq \frac{p-1}{p}n$. (1) と合わせて，

$$u = \frac{p-1}{p}n,\ v = 0,\ H(x) = -G_n(x).$$
$$\therefore\quad \mathcal{A}_{\mathcal{I}} = \langle (x-1)^{\frac{p-1}{p}n} - pG_n(x),\ p(x-1)^{n-s} \rangle.\ \blacksquare$$

定理 3.4.3: $\mathcal{I} = \langle f(x) \rangle$ は $\mathbf{R}_{p^2}$ の単項イデアルで，
$f(x) = (x-1)^s + p(x-1)^t h(x)$, (ただし $h(x)$ は $\mathbf{R}_p$ での単元) とすると，
(1) $s < \frac{n}{p}$ のとき．

$$\mathcal{A}_{\mathcal{I}} = \langle\ (x-1)^{n-s} - p(x-1)^{\frac{n}{p}-s} G_n(x) - p(x-1)^{n+t-2s} h(x)\ \rangle.$$

(2) $\frac{n}{p} \leq s < t + \frac{p-1}{p}n$ のとき．

$$\mathcal{A}_{\mathcal{I}} = \langle\ (x-1)^{\frac{p-1}{p}n} - p(x-1)^{\frac{p-1}{p}n+t-s} h(x) - pG_n(x), p(x-1)^{n-s} \rangle.$$

(3) $s = t + \frac{p-1}{p}n$ のとき．
(i) $G_n(x) + h(x)$ が単元のとき．

$$\mathcal{A}_{\mathcal{I}} = \langle (x-1)^{\frac{p-1}{p}n} - p\big\{G_n(x) + h(x)\big\}, p(x-1)^{n-s} \rangle.$$

(ii) $G_n(x) + h(x)$ が単元でないとき．

$$\mathcal{A}_{\mathcal{I}} = \langle (x-1)^{\frac{p-1}{p}n-k} - pB(x),\ p(x-1)^{n-s} \rangle.$$

ただし $p\{G_n(x) + h(x)\} = p(x-1)^k B(x)$ とおいた．
(4) $s > t + \frac{p-1}{p}n$ のとき．

$$\mathcal{A}_{\mathcal{I}} = \langle (x-1)^{s-t} - p(x-1)^{s-t-\frac{p-1}{p}n} G_n(x) - ph(x), p(x-1)^{n-s} \rangle.$$

(注意)$p=2$ のとき $\frac{n}{p}=\frac{p-1}{p}n=\frac{n}{2}$([8], theorem 24)

証明 : 各場合について，$\mathcal{A}_{\mathcal{I}}$ を生成するモニック多項式を $Q(x)$ とすると，
$f(x)Q(x)=0$ が成り立つことは容易に確かめられ，$\mathcal{A}_{\mathcal{I}}$ がモニック多項式を含むことがわかる．そこで**定理 3.3.1** より，基底は

$$\begin{aligned}\mathcal{A}_{\mathcal{I}} =&\langle F(x), p(x-1)^j\rangle,\\ F(x) =&(x-1)^u+p(x-1)^vH(x)\end{aligned}$$

とおける．ここで $H(x)$ は単元，**補題 3.4.1** より $j=n-s$. また**定理 3.3.1** で注意した u の最小性より ($(1)\sim(4)$ の場合をまとめて $Q(x)=(x-1)^S+pR(x)$ と略記すれば) $u\leq S$ である．
以下，s, t, $h(x)$ を与えられたものとして，$\mathbf{R}_{p^2}$ で $f(x)F(x)=0$ が成り立つような u, v, $H(x)$ を決定する．その際

$$\begin{aligned}f(x)F(x)&=\left\{(x-1)^s+p(x-1)^th(x)\right\}\times\left\{(x-1)^u+p(x-1)^vH(x)\right\}\\ &\equiv(x-1)^{s+u}+p(x-1)^{s+v}H(x)+p(x-1)^{t+u}h(x).\end{aligned}$$

だから $f(x)F(x)=0$ のためには $s+u\geq n$ が必要で，その時**補題 3.2.2** より

$$p(x-1)^{s+u-\frac{p-1}{p}n}G_n(x)+p(x-1)^{s+v}H(x)+p(x-1)^{t+u}h(x)=0. \qquad (*)$$

上式を成り立たせる u,v,$H(x)$ の存在がいえればよい．
$G_n(x), H(x), h(x)$ は単元なので，左辺の各項の次数最小の項を比較したとき，次の 4 つの場合の何れかが成り立っていなければならない．

$$\begin{cases}(1)\ s+u-\frac{p-1}{p}n=s+v<t+u\\ (2)\ s+v=t+u<s+u-\frac{p-1}{p}n\\ (3)\ s+u-\frac{p-1}{p}n=t+u<s+v\\ (4)\ s+u-\frac{p-1}{p}n=s+v=t+u\end{cases}$$

ただし (4) の場合が生じるのは $p\neq 2$ のときに限る．(1) このとき $s<t+\frac{p-1}{p}n$, $u=v+\frac{p-1}{p}n\geq\frac{p-1}{p}n$. (i) $s<\frac{n}{p}$ のとき；既に注意したように $s+u\geq n$ したがって $u\geq n-s$. また，u の最小性から $u\leq n-s$.

$$\begin{aligned}&\therefore\quad u=n-s,\quad v=\frac{n}{p}-s,\\ H(x)&=-G_n(x)-(x-1)^{t-s+\frac{p-1}{p}n}h(x).\end{aligned}$$

ここで，$pF(x)=p(x-1)^{n-s}\in\langle F(x)\rangle$ となるので $\mathcal{A}_{\mathcal{I}}$ は単項イデアルで

$$\mathcal{A}_{\mathcal{I}}=\langle\ (x-1)^{n-s}-p(x-1)^{\frac{n}{p}-s}G_n(x)-p(x-1)^{n+t-2s}h(x)\ \rangle.$$

(ii) $\frac{n}{p}\le s<t+\frac{p-1}{p}n$ のとき ; (1) より $u\ge\frac{p-1}{p}n$. u の最小性から $u\le(p-1)n/p$.

$$\therefore\ u=\frac{p-1}{p}n\ ,\ v=0, H(x)=-G_n(x)-(x-1)^{t-s+\frac{p-1}{p}n}h(x).$$

$$\therefore\ \mathcal{A}_{\mathcal{I}}=\langle\ (x-1)^{\frac{p-1}{p}n}-p(x-1)^{\frac{p-1}{p}n+t-s}h(x)-pG_n(x)\ ,\ p(x-1)^{n-s}\rangle.$$

(2) このとき $t+\frac{p-1}{p}n<s$.

$$u=s+v-t>u+\frac{p-1}{p}n>\frac{p-1}{p}n.$$

u の最小性より $u=s-t, v=0$.

$$H(x)=-(x-1)^{s-t-\frac{p-1}{p}n}G_n(x)-h(x),$$
$$\mathcal{A}_{\mathcal{I}}=\langle(x-1)^{s-t}-p(x-1)^{s-t-\frac{p-1}{p}n}G_n(x)-ph(x), p(x-1)^{n-s}\ \rangle.$$

(3), (4) このときまず $s=t+\frac{p-1}{p}n$ で $(*)$ は

$$p(x-1)^{s+v}H(x)+p(x-1)^{s+u-\frac{p-1}{p}n}\big\{G_n(x)+h(x)\big\}=0$$

とくに (4) が成り立つためには $G_n(x)+h(x)$ が単元でなければならないことに注意. (i) $G_n(x)+h(x)$ が単元のとき ; $s+u-\frac{p-1}{p}n=s+v$ より
$u=v+\frac{p-1}{p}n\ge\frac{p-1}{p}n$. u の最小性から $u\le\frac{p-1}{p}n$.

$$\therefore\quad u=\frac{p-1}{p}n,\ v=0\ ,\ H(x)=-G_n(x)-h(x),$$
$$\therefore\quad \mathcal{A}_{\mathcal{I}}=\langle(x-1)^{\frac{p-1}{p}n}-p\big\{G_n(x)+h(x)\big\}, p(x-1)^{n-s}\rangle.$$

(ii) $G_n(x)+h(x)$ が単元でないとき ;

$$G_n(x)+h(x)\equiv\sum_{i\ge k}a_i(x-1)^i=(x-1)^kB(x)(\mathrm{mod}p)$$

ただし $a_k\not\equiv 0\ (\mathrm{mod}\ p)$ とすると $(*)$ は

$$\begin{aligned}&p(x-1)^{s+v}H(x)+p(x-1)^{s+u-\frac{p-1}{p}n}\big\{G_n(x)+h(x)\big\}\\&=p(x-1)^{s+v}H(x)+p(x-1)^{s+u-\frac{p-1}{p}n+k}B(x)\\&=0.\end{aligned}$$

$s+u-\frac{p-1}{p}n+k=s+v$ でなければならないから

$$u=v+\frac{p-1}{p}n-k.$$

特に $v=0$ とすると，$v=\frac{p-1}{p}n-k$, $H(x)=-B(x)$.

$$\therefore \mathcal{A}_{\mathcal{I}}=\langle\ (x-1)^{\frac{p-1}{p}n-k}-pB(x), p(x-1)^{n-s}\rangle.\ \blacksquare$$

定理 3.4.4: イデアル $\mathcal{I}=\langle p(x-1)^m\rangle$ に対応する符号を $\mathcal{C}$ とする時，$\mathcal{C}^{\perp}$ はイデアル $\mathcal{A}_{\mathcal{I}}=\langle(x-1)^{n-m}\ ,\ p\rangle$ に対応する．

定理 3.4.5: イデアル $\mathcal{I}=\langle f(x)\ ,\ p(x-1)^m\rangle$ に対応する符号を $\mathcal{C}$ とする時，$\mathcal{C}^{\perp}$ はイデアル $\mathcal{A}_{\mathcal{I}_1}\bigcap\mathcal{A}_{\mathcal{I}_2}, \mathcal{I}_1=\langle f(x)\rangle, \mathcal{I}_2=\langle p(x-1)^m\rangle$ に対応する．

3.5 情報多項式と符号語数

3.5 節では情報多項式の選択についての注意を与える．有限体上の巡回符号については情報多項式は生成多項式の次数で決まる．しかしながら，有限環 $\mathbf{Z}_{p^2}$ 上においては，係数にも零因子が現れるので，情報系列と符号語を一意的に対応させるためには，次数のみならず係数の範囲にも制限を加えておく必要がある．そこで本節では，巡回符号とその双対符号の対応を利用して，情報多項式の取り方と符号語の個数を明らかにする： 一般に C を $\mathbf{Z}_{p^2}$ 上の符号とし，

$$C_1=\{c\in C : c \bmod p=0\},\quad C_0\cong C/C_1$$

とおくと C_1, C_0 は $\mathbf{Z}_p$ 上の符号と見なせて

$$(C^{\perp})_1\cong(C_0)^{\perp},\quad (C^{\perp})_0\cong(C_1)^{\perp}.$$

実際，$\mathbf{x}\in(C^{\perp})_1$ なら $\mathbf{x}=p\mathbf{x_1}, \mathbf{x_1}\in\mathbf{Z}_p^n$ と書けて任意の $\mathbf{y}\in C$ に対し

$$\mathbf{x}\cdot\mathbf{y}\equiv 0\ \pmod{p^2}\quad\therefore\quad \mathbf{x_1}\cdot\mathbf{y}\equiv 0\ \pmod{p}$$

をみたす．$\mathbf{y}\equiv\mathbf{y}_0\ (\mathrm{mod}\ p)$, $\mathbf{y}_0\in C_0$ だから $\mathbf{x_1}\in(C_0)^{\perp}$ である．逆に $\mathbf{x}\in(C_0)^{\perp}$ なら $p\mathbf{x}\in(C^{\perp})_1$ だから，$(C_0)^{\perp}\subset(C^{\perp})_1$ も成り立ち $(C^{\perp})_1\cong(C_0)^{\perp}$ である．C の代わりに $C^{\perp}$ をとれば $C^{\perp\perp}=C$ より $(C^{\perp})_1=(C_0)^{\perp}$ が成り立つ．

定理 3.5.1:　$\mathbf{Z}_{p^2}$ のイデアル $\mathcal{I} = \langle f(x) \rangle$ に対応する長さ n の巡回符号を $\mathcal{C}$，その双対符号 $\mathcal{C}^{\perp}$ のイデアルを $\mathcal{A}_{\mathcal{I}}^{*} = \langle g(x)\ ,\ p(x-1)^m \rangle$ とする．

$$\begin{aligned} f(x) =& (x-1)^s + p(x-1)^t h_1(x), \\ g(x) =& (x-1)^{s'} + p(x-1)^{t'} h_2(x), \\ (h_1(x), h_2(x) \text{は} R_p \text{での単元}\ ,\ & s < n\ ,\ m < s' < n), \end{aligned}$$

とおく．ただしここで，$\mathcal{A}_{\mathcal{I}} = \langle f(x) + pg(x), pq(x) \rangle$ ならば，
$\mathcal{A}_{\mathcal{I}}^{*} = \langle f(x)^* + px^{s-s'} g^*(x), pq^*(x) \rangle$ が成り立ち ([1])，s', t' は**定理 3.4.3** から知られることに注意する．この時，情報多項式を以下の様にとることで，情報系列と符号語が一意的に対応する．

$$\begin{aligned} &\sum_{i=0}^{n-s-1} (a_i + pb_i)(x-1)^i + \sum_{i=n-s}^{s'-1} c_i (x-1)^i, \\ &(a_i, b_i, c_i\ \in\ \mathbf{Z}/p\mathbf{Z} = \{0, 1, \cdots, p-1\}). \end{aligned}$$

また $\mathcal{I}, \mathcal{A}_{\mathcal{I}}^{*}$ に対応する符号 $\mathcal{C}, \mathcal{C}^{\perp}$ の符号語の個数は

$$\sharp\mathcal{C} = p^{n+s'-s}, \quad \sharp\mathcal{C}^{\perp} = p^{n+s-s'}.$$

証明：$\mathcal{C}_0$ は $(x-1)^s$ を生成多項式とする $\mathbf{Z}_p$ 上の巡回符号なので，次元は $\dim_{\mathbf{Z}_p} \mathcal{C}_0 = n - s$ である．$(\mathcal{C}^{\perp})_1 \cong (\mathcal{C}_0)^{\perp}$ より

$$\dim_{\mathbf{Z}_p} (\mathcal{C}^{\perp})_1 = \dim_{\mathbf{Z}_p} (\mathcal{C}_0)^{\perp} = n - \dim_{\mathbf{Z}_p} \mathcal{C}_0 = s.$$

同様に $\dim_{\mathbf{Z}_p} (\mathcal{C}^{\perp})_0 = n - s'$ から

$$\dim_{\mathbf{Z}_p} \mathcal{C}_1 = n - \dim_{\mathbf{Z}_p} (\mathcal{C}^{\perp})_0 = s'.$$

$\dim_{\mathbf{Z}_p} \mathcal{C} = \dim_{\mathbf{Z}_p} \mathcal{C}_1 + \dim_{\mathbf{Z}_p} \mathcal{C}^1 = n - s + s'$ より

$$\sharp\mathcal{C} = p^{n+s'-s}.$$

同様に，$\dim_{\mathbf{Z}_p} \mathcal{C}^{\perp} = n - s' + s$ より，

$$\sharp\mathcal{C}^{\perp} = p^{n+s-s'}.$$

次に，$k_1(x), k_2(x)$ が情報多項式，つまり

$$\sum_{i=0}^{n-s-1} (a_i + pb_i)(x-1)^i + \sum_{i=n-s}^{s'-1} c_i (x-1)^i$$

のように書けていて，$k_1(x) \neq k_2(x)$ かつ $f(x)k_1(x) = f(x)k_2(x)$ を仮定する．$f(x)\big\{k_1(x) - k_2(x)\big\} = 0$ より，$k(x) = k_1(x) - k_2(x) \in \langle g(x) \rangle$ でなければならないが，$k(x)$ がモニックのときには $deg\ k(x) < s'$ となり s' の最小性に矛盾．$k(x)$ がモニックでないとすると，$c_i, c_i' \in \{0, 1, \cdots, p-1\}$ かつ $c_i \neq c_i'$ なら $c_i - c_i' \neq 0 \mod p$ より $k(x) = p\sum_{i=0}^{n-s-1} b_i(x-1)^i$ と書けて，$deg\ k(x) < n - s$ となり，**補題 3.4.1** に矛盾する．ゆえに $k_1(x) \neq k_2(x)$ なら $f(x)k_1(x) \neq f(x)k_2(x)$ となり，情報多項式の選び方は $p^{n+s'-s}$ 個あるから定理は成り立つ．　■

第4章　共変指数とそのメッシュ型通信路の解析への応用

4.1　序

4 章では, 離散系列の相関を示す指標として共変指数を導入し, さらに, ネットワークの信頼性評価に利用できることをフィールド実験データの解析の試みを通じて示す. バイオインフォマティクス等の分野では, 高次の相関をはかる際には専ら相互情報量が用いられてきたが, 共変指数はその改良の必要から導入されたものであり, 例えば, 広く認知された相関係数とは違い, 対象が 2 つ以上の場合にも適用できる.

以下ではまず 4.2 節で高次相互情報量について復習する．確率変数 $X_1, \cdots, X_m$ が共通してもつエントロピーは m 次相互情報量で表され，m 次相互情報量が正の値をとるならば，確率変数 $X_1, \cdots, X_m$ のあいだには何らかの相関があるとみなすことができる．そこで, エイズウイルスのアミノ酸配列の相関を調べる指標に，これを応用することが提案された ([14], [20])．しかし，高次相互情報量は各確率変数の情報量の大きさに依存してしまい，相関の強さを表す尺度として高次相互情報量の値を直接用いることは必ずしも妥当ではない．4.3 節では，例を挙げてこの点に注意を促すと同時に，この欠点を補うために共変指数を導入する．これは，各々の確率変数が持つエントロピーに対する相互情報量の割合の，算術平均として定義される情報理論的な量である．

具体的な応用として，4.4 節では光空間伝送ネットワークのフィールド実験データを共変指数を用いて解析する．光空間伝送における回線の劣化ないし遮断は，現実には，天候や交通量の影響で起こる減衰の他，建設工事等による障害物の発生や, ビル屋上排気ダクトからの水蒸気など，システム稼動前には予測困難な複数の要因によってもたらされうる．しかし原因はどうあれ運用上は，ネットワークの一部が孤立してしまうような事態が引き起こされないことが要求される．したがって情報伝達の信頼性向上のためには，回線劣化要因の特定およびそれらを考慮した回線品質向上の努力とは別に，あらかじめ複数経路を用意しておくようなネットワーク設計が望ましい．そしてそのようなメッシュ型ネットワークを有効

に機能させるためには，当然のことながら，複数の回線が同時には断線してしまわないことが望ましい．そこで，その評価のひとつの試みとして，各回線の稼動状況を離散系列に変換し，共変指数を用いた解析を試みる．各回線間の共変指数を計算することで，同時に切断が起こりやすくなっている箇所を洗い出すことが目的である．

4.2　高次相互情報量と共変指数

4.2.1　エントロピーと相互情報量

X_1 を $\{a_1, a_2, \cdots, a_{N_1}\}$ 上の確率変数とする．$X_1 = a_i$ となる確率を $P(a_i)$ $(1 \leq i \leq N_1)$ で表す．この時，X_1 に関するエントロピー (entoropy) は

$$H(X_1) = -\sum_{i=1}^{N_1} P(a_i) \log P(a_i)$$

で定義される．$H(X_1)$ は，エントロピー関数と呼ばれ，確率変数 X_1 のもつ不確かさの尺度として用いられる．エントロピーは，確率変数 X_1 に現れる元が多様なほど高い値を示す．

(例) 対数の底を 2，$N_1 = 2$ とした場合の 2 元エントロピー関数を図示する．エントロピーは，確率 $P(a_1) = 1 - P(a_2) = 1/2$ のとき最大値 1 をとる．

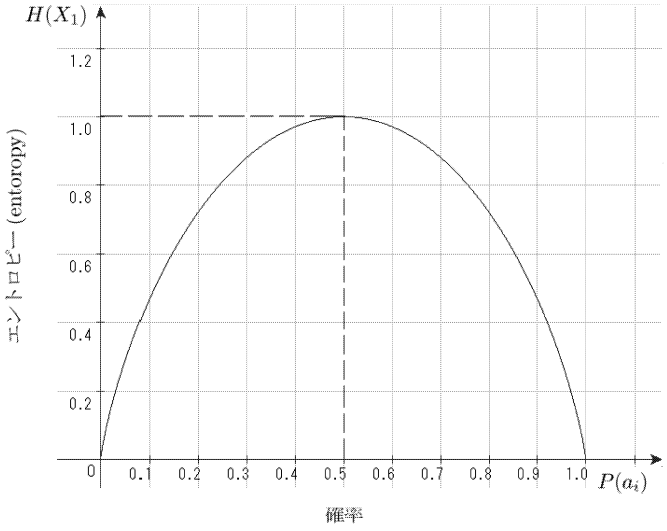


図 4.1　2 元エントロピー関数

さらに $\{b_1, b_2, \cdots, b_{N_2}\}$ 上の確率変数を X_2 とし，$X_1 = a_i$ かつ $X_2 = b_j$ となる同時確率を $P(a_i, b_j)$ と記す．結合エントロピー $H(X_1, X_2)$ は

$$H(X_1, X_2) = -\sum_{i=1}^{N_1}\sum_{j=1}^{N_2} P(a_i, b_j)\log P(a_i, b_j)$$

で定義される．また，X_2 の値が b_j であるとき，X_1 の値が a_i となる条件付き確率を $P(a_i|b_j)$ とすれば，条件付きエントロピー $H(X_1|X_2)$ は，

$$H(X_1|X_2) = -\sum_{i=1}^{N_1}\sum_{j=1}^{N_2} P(a_i|b_j)\log P(a_i|b_j)$$

で表され，確率変数 X_1 と X_2 の間の相互情報量 $M(X_1, X_2)$ との間に次の関係が成り立つ；

$$\begin{aligned} M(X_1, X_2) &= H(X_1) - H(X_1|X_2) \\ &= H(X_2) - H(X_2|X_1) \\ &= H(X_1) + H(X_2) - H(X_1, X_2). \end{aligned} \tag{4.1}$$

相互情報量は，X_2(または X_1) の値を知ることにより得られる X_1(または X_2) に関するエントロピー，すなわち X_1 と X_2 が共通してもつエントロピーと解釈される．2 つの確率変数 X_1, X_2 が完全に独立なとき，$M(X_1, X_2)$ の値は最小値 0 をとる．また X_1, X_2 の相関が強くなるほど $M(X_1, X_2)$ の値は大きくなる．また，相互情報量は，エントロピーの性質を集合的に解釈し，以下のような関係で表わされる．

$$\begin{aligned} H(X_1, X_2) &= H(X_1) \cup H(X_2) \\ H(X_1|X_2) &= H(X_1) \cap \overline{H(X_2)} \\ M(X_1, X_2) &= H(X_1) \cap H(X_2) \end{aligned}$$

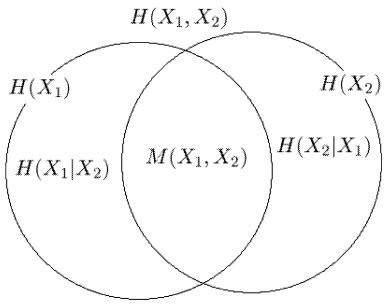


図 4.2 相互情報量の集合的解釈

4.2.2　高次相互情報量

一般に m 個の確率変数 X_1,$\cdots$,X_m についての高次相互情報量 $M(X_1,\cdots,X_m)$ も，$m-1$ 個の確率変数についての高次相互情報量と条件付き相互情報量を用いて帰納的に定義することができる；X_i の取りうる元の集合を $A_i=\{a_{in_i};1\leq n_i\leq N_i\}$ とする．$X_i=a_{in_i}$ $(1\leq i\leq m)$ となる結合事象の生じる確率を

$$P(a_{1n_1},a_{2n_2},\cdots,a_{mn_m}).$$

また $X_j=a_{jn_j}$ のとき $X_i=a_{in_i}$ $(i\neq j)$ となる条件付き確率を

$$P(a_{1n_1},\cdots,a_{j-1\,n_{j-1}},a_{j+1\,n_{j+1}}\cdots,a_{mn_m}|a_{jn_j})$$

で表す．以下では簡単のために，$\boldsymbol{a}=(a_{1n_1},a_{2n_2},\cdots,a_{mn_m})$ から j 番目を除いたものを

$$\check{\boldsymbol{a}}=(a_{1n_1},\cdots,a_{j-1\,n_{j-1}},a_{j+1\,n_{j+1}}\cdots,a_{mn_m})$$

と記すことにして $P(\boldsymbol{a})$, $P(\check{\boldsymbol{a}}|a_{jn_j})$ のように表すとき

$$P(\boldsymbol{a})=P(a_{jn_j})\ P(\check{\boldsymbol{a}}|a_{jn_j}) \tag{4.2}$$

が成り立ち，結合エントロピー $H(X_1,\cdots,X_m)$, 条件付きエントロピー $H(X_1,\cdots,X_{j-1},X_{j+1},\cdots,X_m|X_j)$ はそれぞれ一般に以下の式で表される．

$$\begin{aligned}&H(X_1,\cdots,X_m)=-\sum P(\boldsymbol{a})\log P(\boldsymbol{a}).\\&H(X_1,\cdots,X_{j-1},X_{j+1},\cdots,X_m|X_j)=-\sum P(a_{jn_j})P(\check{\boldsymbol{a}}|a_{jn_j})\log P(\check{\boldsymbol{a}}|a_{jn_j}).\end{aligned}\tag{4.3}$$

(4.3) 式の右辺に (4.2) を代入すると

$$\begin{aligned}H(X_1,\cdots,X_m)&=-\sum P(a_{jn_j})P(\check{\boldsymbol{a}}|a_{jn_j})\log\left\{P(a_{jn_j})P(\check{\boldsymbol{a}}|a_{jn_j})\right\}\\&=-\sum P(a_{jn_j})P(\check{\boldsymbol{a}}|a_{jn_j})\left\{\log P(a_{jn_j})+\log P(\check{\boldsymbol{a}}|a_{jn_j})\right\}\\&=-\sum P(a_{jn_j})\log P(a_{jn_j})\left\{\sum P(\check{\boldsymbol{a}}|a_{jn_j})\right\}\\&\qquad\qquad-\sum P(a_{jn_j})\ P(\check{\boldsymbol{a}}|a_{jn_j})\log P(\check{\boldsymbol{a}}|a_{jn_j}).\end{aligned}$$

ここで，$\sum\limits_{\check{\boldsymbol{a}}}P(\check{\boldsymbol{a}}|a_{jn_j})=1$ より，結合エントロピーと条件付きエントロピーのあいだには次の関係式が成り立つ;

$$H(X_1,\cdots,X_m)=H(X_j)+H(X_1,\cdots,X_{j-1},X_{j+1},\cdots,X_m|X_j). \tag{4.4}$$

ここで，高次相互情報量 $M(X_1,\cdots,X_m)$ を

$$\begin{aligned} M(X_1,\cdots,X_m) = M(X_1,\cdots,X_{j-1},X_{j+1},\cdots,X_m) \\ - M(X_1,\cdots,X_{j-1},X_{j+1},\cdots,X_m|X_j) \end{aligned}$$

で帰納的に定義する．このとき結合エントロピーによる以下の表示が成り立つ．

$$M(X_1,\cdots,X_m) = \sum_{k=1}^{m}(-1)^{k-1}\sum_{1\le i_1<\cdots<i_k\le m} H(X_{i_1},\cdots,X_{i_k}). \tag{4.5}$$

例えば，確率変数が 3 つのときの 3 次相互情報量は，

$$M(X_1,X_2,X_3) = M(X_1,X_2) - M(X_1,X_2|X_3) \tag{4.6}$$

である．(4.1) で X_1, X_2 のかわりに $X_1|X_3$, $X_2|X_3$ とすれば $M(X_1|X_3,X_2|X_3)$ $= M(X_1,X_2|X_3)$ だから右辺の条件付相互情報量 $M(X_1,X_2|X_3)$ は

$$\begin{aligned} M(X_1,X_2|X_3) &= M(X_1|X_3,X_2|X_3) \\ &= H(X_1|X_3) + H(X_2|X_3) - H(X_1,X_2|X_3) \\ &= H(X_1,X_3) - H(X_3) - H(X_1,X_2,X_3) + H(X_2,X_3). \end{aligned}$$

この式と (4.1) を (4.6) に代入すると

$$M(X_1,X_2,X_3) = \sum_{i=1}^{3} H(X_i) - \sum_{1\le i<j\le 3} H(X_i,X_j) + H(X_1,X_2,X_3).$$

一般の場合も，同様に，まず $M(X_1,\cdots,X_m)$ を $m-1$ 個の確率変数についての結合エントロピー及び条件付エントロピーで表し，(4.4) を用いて

$$\begin{aligned} H(X_1|X_m,\cdots,X_{m-1}|X_m) =& H(X_1,\cdots,X_{m-1}|X_m) \\ =& H(X_1,\cdots,X_{m-1},X_m) - H(X_m) \end{aligned}$$

と変形できることに注意して計算すれば (4.5) が成り立つことが確かめられる．
高次相互情報量 $M(X_1,\cdots,X_m)$ も 2 次相互情報量同様, 確率変数
$X_1,X_2,\cdots,X_m$ が共通してもつエントロピーと解釈される．3 次元以上の相互情報量は負の値も取ることを注意しておく．

4.3　共変指数

4.3.1　共変指数

4.1 節で述べたように，高次相互情報量はしばしば相関を示す指標として用いられる．しかしながら，1 次エントロピーの小さい確率変数間の相互情報量よりも，1 次エントロピーの大きい確率変数間の相互情報量の方が大きい値をとり易くなる．4.3.2 節で具体例を踏まえて詳述するが，これは，高次相互情報量が，各確率変数が共通してもつ情報量として定義されているため，1 次エントロピーの値を越えるような値を取り得ないからである．以上の理由から，高次相互情報量は, 相関の有無をある程度は判断できるものの，指標として用いるのは妥当ではない．そこで共変指数 K を新たに次式で定義する;

$$K(X_1, \cdots, X_m) = \frac{M(X_1, \cdots, X_m)}{m} \sum_{i=1}^{m} \frac{1}{H(X_i)}.$$

共変指数は，各確率変数の持つエントロピーに対する m 次相互情報量の割合の平均を示し，共変指数の値が 1 に近いほど m 個の確率変数の相関は強いと判断することができる．実用上は共変指数の閾値を適切に定めておくことが望ましい．

4.3.2　情報源の相関

前節で導入した共変指数は，エイズウイルスの DNA 配列変化に共通する規則性を見つけ出す目的で [25] で導入された．詳細は省略するが，情報理論の観点から見ると，これは，情報源からの出力記号を時系列にそって並べた離散系列から，情報源の相互の相関を調べることに相当する．この節では，この情報理論的な見方に立って，相互情報量との相違を説明する．

(例) 0 または 1 を出力する 3 つの情報源を確率変数 X_1, X_2, X_3 で表す．3 パターンの例について，各情報源から出力される 2 元系列から 3 次相互情報量，共変指数をそれぞれ計算し，相関の様子がどのように記述されるかを比較する．

(A)　X_1 : 00000000000000000000000000000001
　　X_2 : 00000000000000000000000000000001
　　X_3 : 11111111111111111111111111111110

$$M(X_1, X_2, X_3) = 0.0634,\ K(X_1, X_2, X_3) = 1.0000$$

$$
\begin{aligned}
\text{(B)}\quad X_1 &: \ 00000000000000001111111111111111\\
X_2 &: \ 00000000000000001111111111111111\\
X_3 &: \ 11111111111111110000000000000000
\end{aligned}
$$

$$M(X_1, X_2, X_3) = 0.3000,\ K(X_1, X_2, X_3) = 1.0000$$

$$
\begin{aligned}
\text{(C)}\quad X_1 &: \ 00000000000000001111111111111111\\
X_2 &: \ 00000000000011111111111111111111\\
X_3 &: \ 00000000111111111111111111111111
\end{aligned}
$$

$$M(X_1, X_2, X_3) = 0.0913,\ \ K(X_1, X_2, X_3) = 0.3264$$

(A),(B) では 3 つの情報源が完全な相関を持つ．すなわち，(A),(B) では，ある時点での X_1, X_2, X_3 のいずれか 1 つの値が明らかになれば，その他 2 つの情報源から出力されるその時点での値も明らかになる．しかし (C) では，例えば $X_1 = 0$ のとき,X_2 については $X_2 = 0$ である可能性が高いと考えられるものの，X_3 での値を推測する手掛かりとはなりえず，そうした意味で, 相関は見られるものの,(A),(B) に比べれば相関は弱いと考えることができる．(A),(B) の共変指数は 1 となるが，各々の 3 次相互情報量をみるとその値は大きく異なる．また (A),(C) を比べると，(A) のほうが相関が強いと考えられるにもかかわらず，3 次相互情報量は (C) のほうが大きな値をとっていることからも，相関を示す指標に相互情報量を用いるのは妥当ではないと考えられる．理由を了解するためには各々のエントロピーをベン図で表してみるのがよい (図 4.3)；個々の円は X_1, X_2, X_3 がもつ 1 次エントロピーに，斜線部は 3 次相互情報量に対応する．円の大きさは情報量の大小を反映している (ただし (A),(B) では完全な相関をもつため円が 3 重に重なっている).

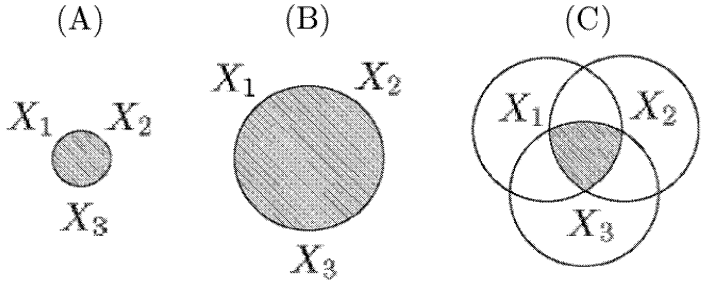


図 4.3 3 次相互情報量のベン図

共変指数は 0 から 1 までの値を取り，相関が強くなるにつれて急速に 1 に近くなる．k 次共変指数は k 変数の関数なのでグラフを描くことはできないが，目安として，長さ 30 の 2 元系列について，3 次共変指数の分布を図 4.4 に示す．縦軸が 3 次共変指数の値である．横軸は直観的には相関の強さを表す: (A),(B) のように, ある情報源が 0 (または 1) を出力するとき，他の 2 つの情報源からの出力が各々 0 または 1 のどちらか一方に偏っていればいるほど相関は強くなる．そこで 30 個の出力を同時点で比較して，そのような偏った出力の組み合わせの最大度数を横軸にとる. すなわち，長さ 30 の 3 つの 2 元系列 (これも X_1, X_2, X_3 で表す) の時点 i での出力を並べたものを $\boldsymbol{x} = (x_{1i}, x_{2i}, x_{3i})$ とし，

$$\mathcal{X}(X_1, X_2, X_3) = \max_{\boldsymbol{a} \in \mathbf{F}_2^3} \Big\{ \#\{i : \boldsymbol{x} = \boldsymbol{a} \text{ or } \overline{\boldsymbol{a}}\} \Big\}$$

とおく．ただし $\boldsymbol{a} = (a_1, a_2, a_3)$ のとき

$$\overline{\boldsymbol{a}} = (\overline{a_1}, \overline{a_2}, \overline{a_3}), \quad \overline{a_i} = a_i + 1 \bmod 2$$

例えば (C) では $\boldsymbol{a} = (111)$ のときが最大で,

$$\mathcal{X}(X_1, X_2, X_3) = 22$$

なので $K(X_1, X_2, X_3) = 0.3264$ は 図 4.4 の横軸が $\mathcal{X} = 22$ の座標にプロットされる. このようにして，長さ 30 の 2 元系列の全ての組み合わせについて共変指数を計算し，3 次共変指数の最大値, 最小値の各々を線で結んで視覚化したものが図 4.4 である ；

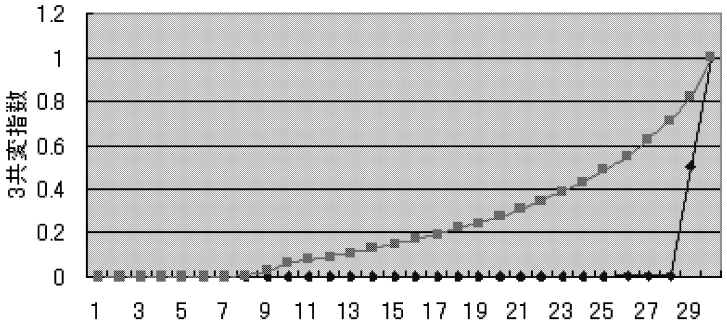


図 4.4 3 次共変指数

$\mathcal{X}$ が高くなるに従いとりうる最大値は急速に高くなるが, その場合でも最小値は極めて 0 に近い値をとることがあり得る.

4.3.3　共変指数による相関のモデル化

独立した情報源を結んだネットワークはしばしば情報源を端点とするグラフで表される．以下では，独立とは限らない複数の情報源があるとき，共変指数を利用してそれらの相関をモデル化することを考える．情報源 $X_1,\cdots,X_m$ は適当に定めた閾値 K_m に対し，共変指数が

$$K(X_1,\cdots,X_m)\geq K_m$$

をみたすとき相関があるものと見なすことにして

$$C_m=\{\langle X_1\cdots X_m\rangle\,;\,K(X_1,\cdots,X_m)\geq K_m\}$$

とおく．記号 $\langle X_1\cdots X_m\rangle$ はグラフ理論で，頂点 e_1 と e_2 を結ぶ辺を $\langle e_1e_2\rangle$ 等と表すことの類似である．なお，$m=1$ のときは $K(X_1)=H(X_1)$ とする．通常は，任意の $\{X_{i_1},\cdots,X_{i_n}\}\subset\{X_1,\cdots,X_m\}$ について，$K(X_{i_1},\cdots,X_{i_n})\geq K_n$ が成り立つとき $X_1,\cdots,X_m$ は共変していると見なす．これは $\langle X_1\cdots X_m\rangle$ が $m-1$ 次元の単体的複体であると仮定するのと同値であることに注意する．言い換えれば，情報源の相関は，高次元の多面体としてモデル化することができる．

(例) 情報源 $X_1,\cdots,X_5$ は 0 または 1 を出力するものとする．(A),(B) の 2 つの場合について，受け取った系列から相関のモデルを構成する;

(A)
X_1 : 0 0 0 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1 1 1
X_2 : 1 1 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0
X_3 : 1 1 1 1 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 0
X_4 : 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 0 0 0
X_5 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 1 1 1 1

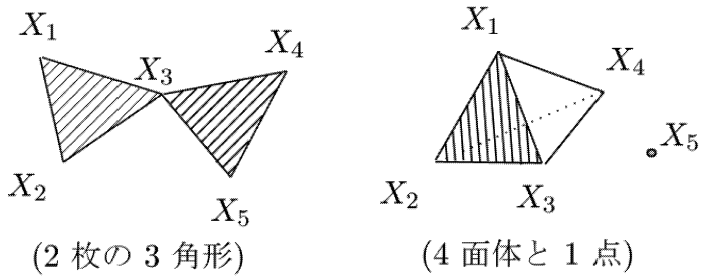
共変指数の分布はここでは省略するが，下記のように閾値を定めて相関を判定すれば

$$\begin{aligned}
C_1 &= \{\langle 1\rangle,\langle 2\rangle,\langle 3\rangle,\langle 4\rangle,\langle 5\rangle\} && (K_1=0.244)\\
C_2 &= \{\langle 12\rangle,\langle 13\rangle,\langle 23\rangle,\langle 34\rangle,\langle 35\rangle,\langle 45\rangle\} && (K_2=0.485)\\
C_3 &= \{\langle 123\rangle,\langle 345\rangle\} && (K_3=0.500)\\
C_4 &= \phi && (K_4=0.100)
\end{aligned}$$

(B)
X_1 : 0 0 0 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1 1 1
X_2 : 1 1 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0
X_3 : 1 1 1 1 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 0
X_4 : 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0
X_5 : 0 0 0 0 0 1 1 1 1 1 0 0 0 0 0 1 1 1 1 1

$$
\begin{aligned}
C_1 &= \{\langle 1\rangle, \langle 2\rangle, \langle 3\rangle, \langle 4\rangle, \langle 5\rangle\} && (K_1 = 0.292)\\
C_2 &= \{\langle 12\rangle, \langle 13\rangle, \langle 14\rangle, \langle 23\rangle, \langle 24\rangle, \langle 34\rangle\} && (K_2 = 0.432)\\
C_3 &= \{\langle 123\rangle, \langle 124\rangle, \langle 134\rangle, \langle 234\rangle\} && (K_3 = 0.428)\\
C_4 &= \{\langle 1234\rangle\} && (K_4 = 0.426)
\end{aligned}
$$

(A) には 頂点を共有する 2 枚の三角形，(B) には四面体と 1 点からなるモデルを与えることができる．



(2 枚の 3 角形)　　(4 面体と 1 点)

図 4.5　相関のモデル

NOTE.(共変指数の多重化) 共変指数は情報源からの出力を，同時刻で比較して相関を判定するものである．本論文では使用しないが，より精密に，k 個の連続する出力を比較することによって共変指数を多重化することが考えられる．すなわち，X_i が k 個の値 $a_{in_{i1}}, \cdots, a_{in_{ik}}$ を続けて出力したときの同時生起確率を

$$
P(\mathcal{A}_k) \quad \text{ただし} \quad \mathcal{A}_k = \begin{bmatrix} a_{1n_{11}} & \cdots & a_{mn_{m1}} \\ \vdots & \ddots & \vdots \\ a_{1n_{1k}} & \cdots & a_{mn_{mk}} \end{bmatrix}
$$

とおいて k 重化共変指数 $K^{(k)}$ を同様に定義することができる．これは次のような相関を区別するために導入される；いま情報源 X_1, X_2, X_3 から次のような長さ 16 の系列が得られたとする．

$$
\begin{aligned}
X_1 &: \ 0\,0\,0\,0\,1\,1\,1\,1\,0\,0\,0\,0\,1\,1\,1\,1\\
X_2 &: \ 0\,1\,0\,1\,1\,1\,0\,1\,0\,1\,0\,1\,0\,0\,0\,1\\
X_3 &: \ 0\,1\,1\,0\,1\,1\,0\,1\,1\,0\,0\,1\,0\,0\,0\,1
\end{aligned}
$$

(A)X_1 と X_2, (B) X_1 と X_3 のそれぞれについて，相関を共変指数を利用して比較すると

$$
P(0,0) = P(1,0) = P(0,1) = P(1,1) = \tfrac{1}{4}
$$

より，2 次相互情報量，共変指数ともに 0 となるが，$k = 2$ とすると

$$\text{(A)}:P[^{00}_{01}] = \tfrac{4}{15}, P[^{01}_{01}] = 0, P[^{01}_{00}] = \tfrac{2}{15}, P[^{00}_{00}] = 0$$

$$\text{(B)}:P[^{00}_{01}] = \tfrac{2}{15}, P[^{01}_{01}] = \tfrac{1}{15}, P[^{01}_{00}] = \tfrac{2}{15}, P[^{00}_{00}] = \tfrac{1}{15}$$

という違いがあることから ($P[^{1*}_{1*}]$ の確率分布は同じ)，観測回数を増やしてゆくと，X_1 が 00 のとき，X_2 については 01 の可能性が高いのではないかと考えることもでき，事実，2 重化共変指数 $K^{(2)}$ は

$$K^{(2)}(X_1, X_2) = 0.3194, \quad K^{(2)}(X_2, X_3) = 0.1630.$$

と異なる値を取る.

4.4　共変解析 (メッシュ型通信路)

4.4.1　光空間伝送実験概要

まずこの 4.4.1 節で，KDDI 研究所によって行われた実験の概要を紹介する．この実験は,2001 年 7 月から翌 2002 年 2 月まで, 東京都内半蔵門周辺 1 km 四方 9 箇所に光空間伝送装置を設置して実験用通信網を構築し (以下東京実験網と呼称) 各装置の稼動データを秒単位で計測したものである．東京実験網を図 4.6 に光空間伝送装置を設置したビル高を表 4.1 に記す.

表 4.1 設置装置高さ

装置番号	設置高さ
①	$112.09m$
②	$110.75m$
③	$124.57m$
④	$127.59m$
⑤	$122.28m$
⑥	$140.07m$
⑦	$198.44m$
⑧	$157.58m$
⑨	$214.53m$

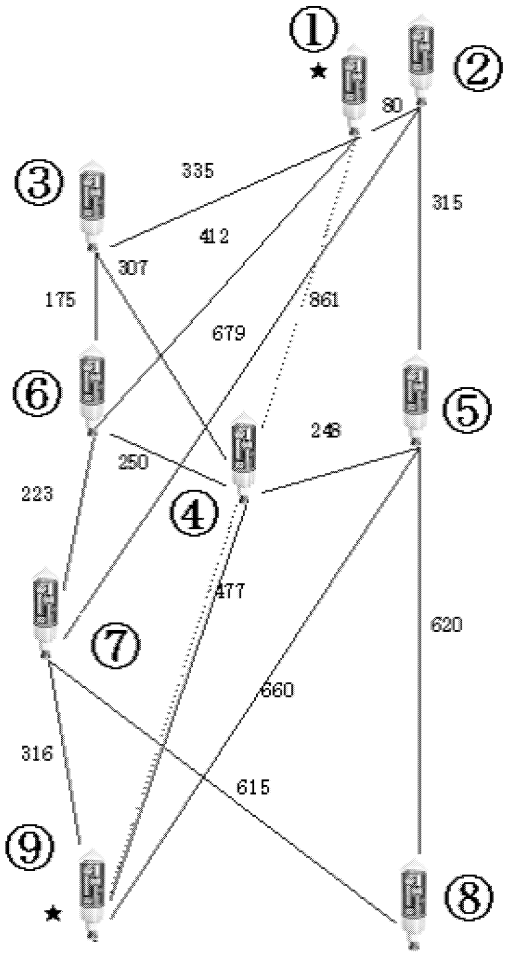
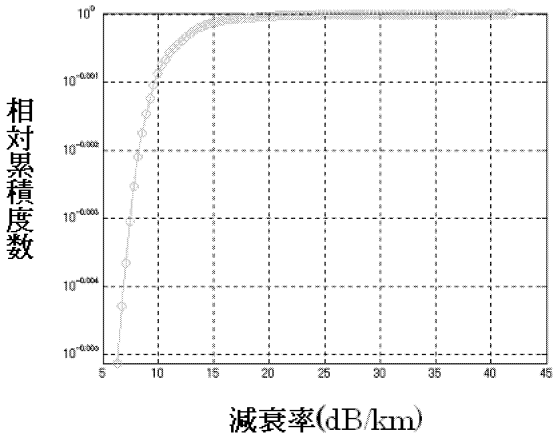


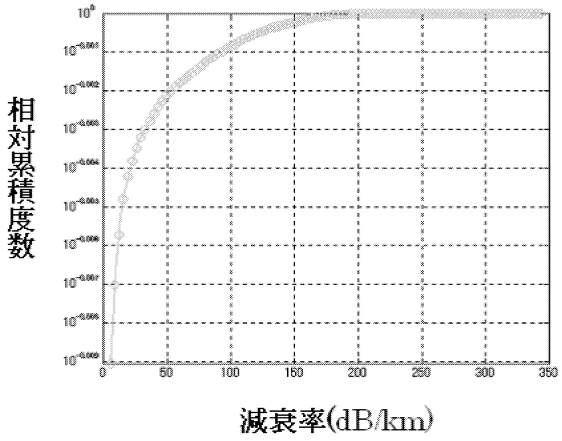
図 4.6 東京実験網

図中の数字はリンク距離 [m] である. 装置から装置へ直接光空間伝送回線が確立しているものをリンクと呼ぶ. リンク間距離が長いほど装置が不稼働に陥る割合は高くなるが, リンク距離から求まる最短経路が不稼働率を最小にする経路とならないことがある. 実験期間中 ①と⑨に現在天気計を設置し,1 分平均視程[1]および 1 分平均降雨強度 [mm/hour] データを 30 秒間間隔で取得している. この天気計データから得られる ①,⑨ の 2 箇所における減衰率の相対累積度数分布グラフを示す.①における減衰率の相対累積度数分布グラフは 2001.8.20〜2002.2.5 までの計 463, 539 データ,⑨では 2001.7.1〜2002.1.5 までの計 543, 314 データを使用した.

[1]Meteological Optical Range. 送信された光量を 100% として, これが 5% にまで減衰する距離 [m]2000m まで (減衰率に変換すると 6.5[dB/km] まで) 計測可能.



①ビル減衰率



⑨ビル減衰率

図 4.7 減衰率累積度数分布グラフ

相対累積度数分布グラフの他, 減衰率の最大値もそれぞれ①:41.935 dB/km に対し, ⑨:342.105dB/km と大きく異なり, 設置ビルの高さや設置場所が異なると減衰率の分布が異なることが確認されている.[2]([16],[15],[17],[18],[19],[23],[24]) また, 降雨強度が視程に及ぼす影響については [24] に報告されている.

以下, 装置の稼動ないし不稼動に各々 0, 1 を対応させて, 取得データを 1 時間刻みで離散化した 2 値データを稼動状態時系列データと呼ぶ. 稼動状態時系列データから共変指数を求め, 切断に相関の見られるリンクを特定し, ネットワークから孤立してしまうおそれのある箇所を検討する. 4 リンク間の共変指数は全

[2]⑨での減衰率が大となったのは, ビルが高く屋上に雲がかかることが多かったためと考えられている.

て 0 であったため，以下では 3 リンク間までの共変指数について検討を加えることとする．

4.4.2　双方向共変指数

各装置は 2 つの一方向回線により双方向に通信可能なように連結されている．まず，各々の回線のエントロピーを図 4.8 に示す．図 4.6 の装置番号のもとで，番号 ⓘ と ⓙ の装置を結ぶリンクを L_{ij} で表す．断線が頻繁なほどエントロピーの値は高くなる．

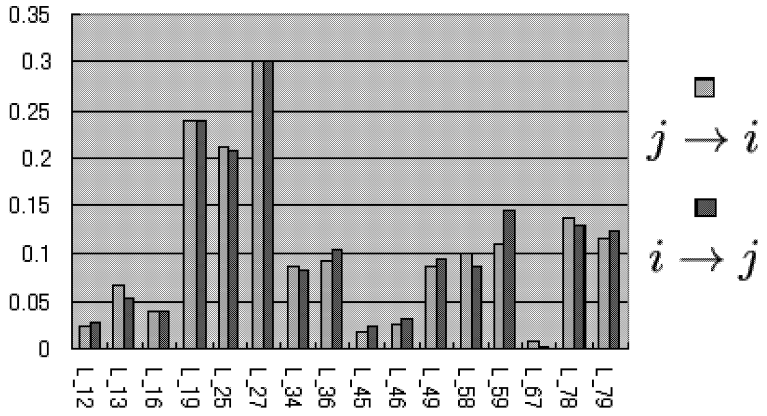


図 4.8　回線のエントロピー

次に，各リンク毎にこれら 2 回線の稼動状態の相関を調べた (表 4.2)．L_{67} を除き各リンクとも強い相関が見られる．これは各リンクで回線切断が起きる場合には，2 回線とも同時に切断してしまうことが多いことを意味する．そこで，次の 4.4.3 節では L_{ij} を ⓘ から ⓙ $(i < j)$ 方向への回線で代表させてリンク間共変指数を計算する．

表 4.2 双方向共変指数

リンク	共変指数	リンク	共変指数
L_{12}	0.32041	L_{45}	0.55095
L_{13}	0.70339	L_{46}	0.70139
L_{16}	0.90155	L_{49}	0.40243
L_{19}	0.90247	L_{58}	0.50183
L_{25}	0.93258	L_{59}	0.56057
L_{27}	1.00000	L_{67}	0.00018
L_{34}	0.32916	L_{78}	0.69915
L_{36}	0.47925	L_{79}	0.51849

4.4.3　リンク間共変指数

まず 2 リンク間共変指数 $K(L_{ab}, L_{cd})$ を次頁表 4.4 に，比較のために，稼動状態時系列データを 2 元ベクトルと見なしたときの相関係数を次頁表 4.5 に示す．解析の対象によって閾値を選ぶ必要はあるが，一般的に相関係数は 0.2 以上の値をとる場合に’相関あり’として判断されることから，本例では，共変指数が 0.1 以上のとき，稼動状況に相関が見られるものと考え，それを太字で示した．例えば

$$K(L_{58}, L_{78}) = 0.166$$

だから，装置 ⑧ に関するリンク L_{58}，L_{78} は同時に切断してしまう可能性が高く，しかもこれらより他にリンクを有しないから，装置 ⑧ は物理的にネットワークから孤立してしまう可能性が高いと考えられる．また，装置 ⑨ に関する 2 リンク間共変指数は

$$K(L_{49}, L_{59}) = 0.397, \quad K(L_{49}, L_{79}) = 0.509,$$
$$K(L_{59}, L_{79}) = 0.472$$

といずれも高い値を示している．ここでさらに，表 4.3 に示すように 3 リンク間共変指数は

表 4.3 リンク間共変指数 (上位 6 リンク群)

$K(L_{49}, L_{59}, L_{79})$	0.349
$K(L_{12}, L_{13}, L_{16})$	0.086
$K(L_{59}, L_{78}, L_{79})$	0.060
$K(L_{45}, L_{59}, L_{79})$	0.043
$K(L_{45}, L_{49}, L_{79})$	0.033
$K(L_{45}, L_{49}, L_{59})$	0.031

であって，3 リンク間共変指数 $K(L_{49}, L_{59}, L_{79})$ が高くなっていることから，装置 ⑨ に関するリンク L_{49}，L_{59}，L_{79} は，いずれかが切断しているときには，他の 2 つも同時に切断している可能性が高い．
一方，装置 ① に関する 2 リンク間共変指数も

$$K(L_{12}, L_{13}) = 0.152, \quad K(L_{12}, L_{16}) = 0.273, \quad K(L_{13}, L_{16}) = 0.154$$

と高い値を示す．しかし，3 リンク間の共変指数は

表 4.4 2 リンク間共変指数 (0.1 以上)
Table.3 Covariant indices between 2-links.

	L_{12}	L_{13}	L_{16}	L_{19}	L_{25}	L_{27}	L_{34}	L_{36}	L_{45}	L_{46}	L_{49}	L_{58}	L_{59}	L_{67}	L_{78}
L_{13}	**0.152**	–	–	–	–	–	–	–	–	–	–	–	–	–	–
L_{16}	**0.273**	**0.154**	–	–	–	–	–	–	–	–	–	–	–	–	–
L_{19}	0.001	0.010	0	–	–	–	–	–	–	–	–	–	–	–	–
L_{25}	0.002	0.009	0.000	0.021	–	–	–	–	–	–	–	–	–	–	–
L_{27}	0.010	0.009	0.000	0.023	0.010	–	–	–	–	–	–	–	–	–	–
L_{34}	0.005	0.015	0.000	0.030	0.004	0.004	–	–	–	–	–	–	–	–	–
L_{36}	0.006	0.006	0.049	0.015	0.003	0.010	**0.397**	–	–	–	–	–	–	–	–
L_{45}	0.001	0.001	0.002	0.000	0.010	0.000	0.026	0.000	–	–	–	–	–	–	–
L_{46}	0.001	0.004	**0.185**	0.000	0.005	0.005	0.034	**0.134**	0.064	–	–	–	–	–	–
L_{49}	0.005	0.000	0.001	0.008	0.000	0.004	0.000	0.000	**0.174**	0.024	–	–	–	–	–
L_{58}	0.006	0.000	0.018	0.002	0.005	0.000	0.002	0.000	0.003	0.011	0.010	–	–	–	–
L_{59}	0.000	0.001	0.009	0.008	0.000	0.004	0.006	0.004	0.058	0.000	**0.397**	0.013	–	–	–
L_{67}	0.000	0.015	0.026	0.022	0.029	0.014	0.010	0.040	0.000	0.109	0.043	0.037	0.032	–	–
L_{78}	0.010	0.003	0.004	0.000	0.003	0.000	0.007	0.002	0.011	0.000	0.019	**0.166**	0.066	0.024	–
L_{79}	0.008	0.007	0.000	0.001	0.000	0.001	0.010	0.008	0.091	0.000	**0.509**	0.006	**0.472**	0.031	**0.117**

表 4.5 2 リンク間相関係数 (0.2 以上)
Table.4 Correlation coefficients between 2-links.

	L_{12}	L_{13}	L_{16}	L_{19}	L_{25}	L_{27}	L_{34}	L_{36}	L_{45}	L_{46}	L_{49}	L_{58}	L_{59}	L_{67}	L_{78}
L_{13}	**0.281**	–	–	–	–	–	–	–	–	–	–	–	–	–	–
L_{16}	**0.439**	**0.283**	–	–	–	–	–	–	–	–	–	–	–	–	–
L_{19}	−0.017	−0.064	0.000	–	–	–	–	–	–	–	–	–	–	–	–
L_{25}	−0.021	−0.061	−0.002	0.156	–	–	–	–	–	–	–	–	–	–	–
L_{27}	−0.044	−0.070	−0.012	0.167	0.108	–	–	–	–	–	–	–	–	–	–
L_{34}	−0.022	0.087	0.001	−0.111	−0.048	−0.054	–	–	–	–	–	–	–	–	–
L_{36}	−0.023	0.056	0.156	−0.089	−0.041	−0.083	**0.632**	–	–	–	–	–	–	–	–
L_{45}	−0.008	0.013	−0.011	−0.007	0.045	0.007	0.085	0.004	–	–	–	–	–	–	–
L_{46}	−0.009	0.032	**0.345**	0.000	0.036	−0.032	0.110	**0.251**	0.161	–	–	–	–	–	–
L_{49}	−0.022	−0.007	0.019	0.071	0.010	0.049	0.020	−0.015	**0.272**	0.089	–	–	–	–	–
L_{58}	−0.024	−0.004	0.087	−0.037	−0.054	0.004	−0.029	0.002	0.026	0.056	0.076	–	–	–	–
L_{59}	−0.006	−0.022	0.061	0.081	−0.017	0.054	−0.045	−0.041	0.133	0.009	**0.628**	0.091	–	–	–
L_{67}	−0.004	0.043	0.066	0.042	0.051	0.030	0.034	0.074	−0.004	0.191	0.080	0.071	0.063	–	–
L_{78}	−0.031	−0.036	0.041	0.008	−0.047	0.002	−0.051	−0.034	0.050	0.000	0.112	**0.390**	**0.236**	0.051	–
L_{79}	−0.027	−0.045	0.016	0.031	−0.024	0.034	−0.056	−0.052	0.172	−0.01	**0.713**	0.062	**0.708**	0.061	**0.327**

$$K(L_{12}, L_{13}, L_{16}) = 0.086$$

であって相関はほとんど見られない．つまり装置 ① では 3 本のリンクのうち 2 本は同時に切断することはあっても 3 本全てが同時に切断する可能性は低く，メッシュネットワークの利点が活かされているといえる．以上，相関の強く見られたリンク群を図 4.9 に示す．3 リンク間での相関が見られるグループは太線で，2 リンク間で相関が見られる組を太点線で結んだ．

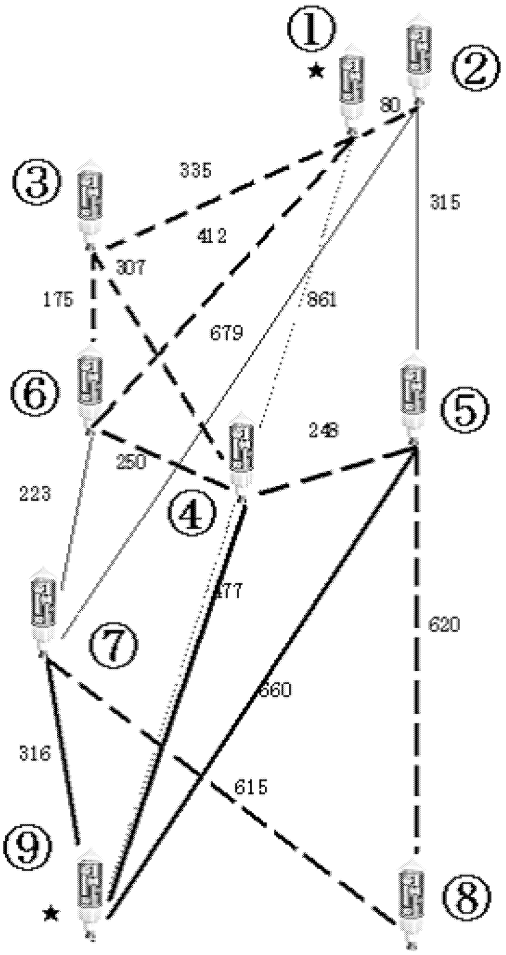


図 4.9 相関のあるリンク群

ここで，エントロピーの値 (図 4.8) を見ると，装置 ⑨ に関するリンク L_{19} は全てのリンクの中で頻繁に回線遮断が起きている．リンク L_{19} とリンク L_{49}，L_{59}，L_{79} では，リンク間距離に著しい違いがあり，そのため，リンク L_{19} の切断を引き起こす原因は，リンク間距離の長さとともに装置の設置場所の高さの 2 つが考えられる [17]．したがって複数の原因が影響して切断が起きていると思われるリ

ンク L_{19} とリンク L_{49}，L_{59}，L_{79} での 4 リンク間では相関を示さないが，エントロピーと 3 リンク間共変指数をあわせて考えると，装置 ⑧，⑨ はネットワークから孤立してしまう可能性が高いと考えられる．L_{19} については頻繁に切断が起きてしまうものの，装置 ① については前述の理由から，孤立の可能性はより低いと考えられる．

装置 ⑥ に関するリンクは，これと対照的な挙動を示す．4 リンク間共変指数は $K(L_{16}, L_{36}, L_{46}, L_{67}) = 0$ だが，3 リンク間共変指数 $K(L_{16}, L_{36}, L_{46})$ は月によっては高い値を示す (表 4.6)．

表 4.6　3 リンク間共変指数 $K(L_{16}, L_{36}, L_{46})$

7 月	**0.2944**
8月	0.0000
9月	0.0000
10月	0.0667
11月	**0.2234**
12月	0.0000
1 月	**0.2843**
2 月	**0.3084**

しかし，エントロピーの値 (図 4.8) からもわかるように，L_{67} はほとんど切断を起こさない．つまり，装置 ⑥ における通信の信頼性は，メッシュ化による向上効果がほとんど見込めず，実際には L_{67} の回線品質に依存しており，L_{67} が切断されるような悪条件下では，やはりネットワークから孤立してしまう可能性が高い．

4.4.4　考察

まず，共変指数を用いる意義を念のため確認しておこう．いま仮に，3 リンクからなる装置 ⓘ, ⓙ の稼動状態時系列データが以下のように得られたとする．
('0,1' をそれぞれ稼動，不稼動に対応)．

ⓘ　L_1 : 0 1 0 0 0 0
　　L_2 : 0 1 1 0 1 0
　　L_3 : 0 1 1 0 1 0

ⓙ　L_1 : 0 1 0 0 0 0
　　L_2 : 0 1 1 0 1 0
　　L_3 : 0 1 0 1 0 1

どちらの装置も同程度の回線品質 (= 1 の現れる確率) のリンクで連結されており，また，全ての回線が同時に切断してしまう同時確率はどちらも $\frac{1}{6}$ で変わらない．しかし，メッシュ化が有効に機能しているのは明らかに後者である．なぜならば，前者は，L_2 と L_3 が似たような挙動を示すため，実際にはこれは 2 つのリ

ンクのみを有するのと変わらず，3 リンクで連結するコストが無駄になっている．しかも L_1 が断線したときには $\frac{1}{2}$ の確率で全回線が不通になる可能性があって，ⓘ における通信の信頼性は，メッシュ化によるというよりは，実際は L_1 の回線品質に依存しているのである．この例からもわかるように，メッシュネットワークの有効性評価は，例えば，複数リンクの同時切断確率によるだけでは十分ではないのである．

4 章で示した解析結果と回線切断要因との関連について，推測されることを参考程度に触れておこう．まず，装置 ⑨ についてはネットワーク内において最も高い位置に設置されていることから，装置自体が雲にかかり易いのではないかと考えることができる[3]．また，地図を見直してみたところ，装置 ⑧ は首都高速道路のすぐ脇のビルに設置されていることから，こちらは排気ガスの影響を強く受けているのではないかと推測される[4]．理由はどうであれ，ネットワーク内で孤立する可能性がある装置 ⑥,⑧,⑨ のような設置環境は，メッシュネットワークを構築するにあたって問題となる可能性が高いため，装置やリンクを増やすか設置位置を変更してリンク間の距離を短く設計し直す等といった対策をとっておくことが推奨される．

本研究は，ネットワークを構成する各回線の稼動状態を 0,1 の 2 元系列として離散データに変換し，ネットワークシステムの安定性の評価を試みたものである．評価の指標として共変指数を用いることにより，似通った挙動を示す回線を抽出できることが示された．共変指数は，もともと DNA 配列のような離散系列の相関を計る指標として導入されたものであるが，今回の解析データのように 0,1 の分布に極端な偏りがある 2 値データの場合には，実用上は系列の類似性を評価するものと考えてよく，解析結果は，回線品質劣化をもたらす要因が，実際にはどの回線に影響しているかという事実を指摘する結果と考えることができる．1 次エントロピー等を用いた回線の稼動状況評価とあわせて考察すれば，ネットワークの安定性をより詳しく検討することができる．通信分野のみならず，分子生物学の分野における，アミノ酸やタンパク質などのネットワーク的側面からの研究に今回の手法が応用されることを期待したい．

[3]現場で実験に携わった KDDI 研究所の金子尚史氏の示唆による

[4]ここでは省略するが，平日と休日を比較すると交通量の多い平日のほうが, 回線の遮断が頻繁に起こる傾向が見られる

第5章　HIV-1の情報理論的解析

5.1　序

世界中で深刻な社会問題を引き起こしているウイルスの一つにHIV-1 いわゆるエイズウイルスがある．感染予防のためのワクチンの開発，および実用化を妨げている理由は，HIV-1 が免疫応答の中枢にあるヘルパーT 細胞を破壊してしまう特性をもつこと，優れた動物モデルが無いこと，など多岐にわたるが，なかでも抗原構造が著しい変異性を持つことが，大きな障害の一つとして挙げられる．とくにアミノ酸配列のなかの V3 loop と呼ばれる領域は，劇的な変異性を持つことで知られ，機能上，免疫学上の両面において，重要な研究対象となっている．

V3 loop には，実際さまざまなアミノ酸配列が現れるが，それらがまったく独立かつ不規則な変化のすえに生じているとはむしろ考えにくく，特定の位置ないしアミノ酸の変異については，生物現象特有の有機的な結びつきが隠れていることも十分考えられる．そこで，5 章では，幾つかのアミノ酸が何らかの関連を持ちながら変化しているのではないかという仮説のもとに，4 章で導入した共変指数を用いることでV3 loop 内の位置間に働く相互依存性を探り，共変グループの特定とアミノ酸ネットワークの解明を目的とし実験を行った．

5.2　基本事項

5.2.1　タンパク質

多くの生物の遺伝情報は，4 種類の塩基 (アデニン，チミン，シトシン，グアニン) からなるDNA という形で細胞内に蓄えられている．DNA は，転写をおこしRNA となり，これがコドン表 (表 5.2) に従って，コドン (3 塩基) 単位でアミノ酸に翻訳されることによって必要なタンパク質が合成されている．しかし，今回取り扱うHIV-1 は，生物界で唯一逆転酵素をもつレトロウィルスと呼ばれるものに属し，遺伝情報はRNA の形で蓄えられている．

タンパク質は，一本の鎖状につながった20 種類のアミノ酸が複雑な立体構造を成して形成されていて，タンパク質ごとに構成アミノ酸の種類・数・結合順は異

なる．この構造及び機能を解析することはポストゲノムと呼ばれ，多くの研究機関が取り組んでいる問題でもある．以下に 20 種類のアミノ酸とそのアミノ酸コードを示す (表 5.1).

表 5.1 アミノ酸コード表

A	*Alanine*	R	*Arginine*
N	*Asparagine*	D	*Asparticacid*
C	*Cysteine*	Q	*Glutamine*
E	*Glutamicacid*	G	*Glycine*
H	*Histidine*	I	*Isoleucine*
L	*Leucine*	K	*Lysine*
M	*Methionine*	F	*Phenylalanine*
P	*Proline*	S	*Serine*
T	*Threonine*	W	*Tryptophan*
Y	*Tyrosine*	V	*Valine*

表 5.2 コドン表

	U	C	A	G
U	(F) UUU	(S) UCU	(Y) UAU	(C) UGU
	UUC	UCC	UAC	UGC
	(L) UUA	UCA	ST UAA	ST UGA
	UUG	UCG	UAG	(W) UGG
C	(L) CUU	(P) CCU	(H) CAU	(R) CGU
	CUC	CCC	CAC	CGC
	CUA	CCA	(Q) CAA	CGA
	CUG	CCG	CAG	CGG
A	(I) AUU	(T) ACU	(N) AAU	(S) AGU
	AUC	ACC	AAC	AGC
	AUA	ACA	(K) AAA	(R) AGA
	(M) AUG	ACG	AAG	AGG
G	(V) GUU	(A) GCU	(D) GAU	(G) GGU
	GUC	GCC	GAC	GGC
	GUA	GCA	(E) GAA	GGA
	GUG	GCG	GAG	GGG

5.2.2 HIV-1 と V3 loop

HIV-1 は直径 110nm，約 9500 塩基からなる RNA 型エンベロープウィルスであり，逆転酵素などを含むキャプシドと，それを取り囲むエンベロープにより構成されている．エンベロープには，糖タンパク質 gp120 と糖二重層を貫く糖タンパク質 gp41 があり，gp120 内に存在する V3 loop 領域は非常に変化の富んだ領域 (様々な配列が現れる) であり，機能上・免疫学上の両面において重要とされ多くの研究の対象となっている．

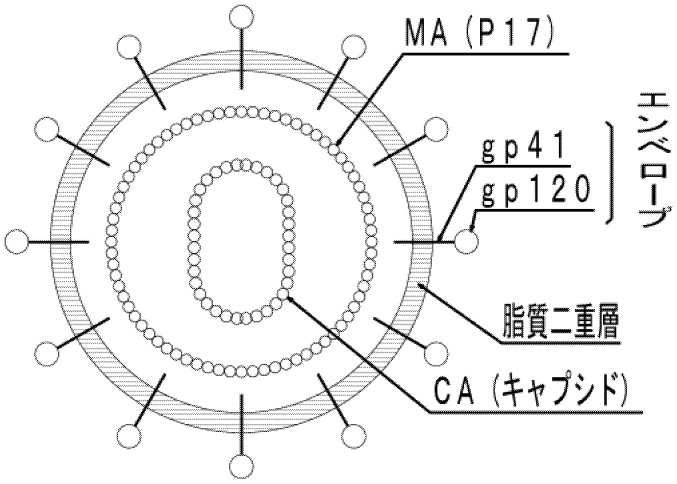


図 5.1 HIV-1 の構造

V3 loop 領域は，両末端を Cysteine(C) でジスルフィド結合をしたループ構造をしていて，抗体や T 細胞を中和する効力を持つ．

図 5.2 は V3 loop の一例の抽象的なモデル図である．アルファベットはそれぞれアミノ酸コードに対応し，それらの外に添えてある数字は解析を行う上での便宜上の位置 (site) を表している．また，V3 loop の 14〜17 の位置におけるアミノ酸配列が GPGQ であればアフリカ分離株，GPGR であれば欧米分離株と呼ばれる．異なる配列モデルの場合，アミノ酸の配列は異なり，本論文では，異なる位置にあるアミノ酸が，何らかの関連をもって同時に変化することを共変と呼ぶ．

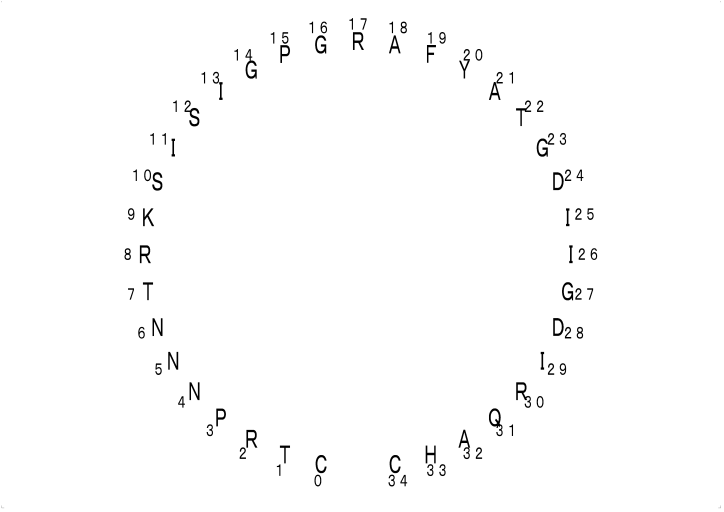


図 5.2 V3 loop のモデル図

図 5.2 の各位置における，20 種のアミノ酸が現れる確率 (生起確率) を，データベース (National Center for Biotechnology Information(NCBI)[7]) に実在する約 17000 例の V3 loop の配列から求め，各位置における生起確率を用いて，アミノ酸の変化量をエントロピーの概念を用いて定量的に表現する．

5.2.3 アライメント (alignment)

アライメントとは，配列の類似する部分，または同一となる部分を縦に揃えて並べ合わせる操作のことを言い，アミノ酸配列の類似性解析の基本的なものの一つである．二本のアミノ酸配列 HEAGAWGHEE と EGWHEAE のアラインメントを行うと以下のようになる．

$$
\begin{array}{cccccccccc}
H & E & A & G & A & W & G & H & E & E \\
E & G & W & H & E & A & E & & &
\end{array}
$$

$$
\Downarrow
$$

$$
\begin{array}{cccccccccc}
H & E & A & G & A & W & G & H & E & - & E \\
- & E & - & G & - & W & - & H & E & A & E
\end{array}
$$

図 5.3 アライメント

同じアミノ酸や性質の似たアミノ酸が縦に，同じ位置になるように，ところどころハイフン (−) が挿入されている．生化学的にはこれらのギャップ (gap) は遺伝子の欠損等によりアミノ酸が出現していないことを意味する．縦方向に揃った代表的文字で構成される配列をコンセンサス配列 (consensus sequence) と呼び，この中に見られるパターンがアライメントされた配列群を特徴付けるものと判断できるとき，このパターンをモチーフ (motif) と呼ぶ．また，ギャップの入り方の相対的に少ない領域を保存部位 (conservative site) と言い，保存性の高い部位は配列の中でもタンパク質の構造や機能の実現の上で重要な部分であると推測できる．重要な配列部分は進化の過程の中で保存されているため，生物の同種のタンパク質をアライメントで調べると保存部位を発見できる．

対象となる配列が 2 本のときはペアワイズアライメント (pairwise alignment) と呼び，基本的には配列と配列の類似性を求めることに使われる．また，3 本以上の配列を扱う場合はマルチプルアライメント (multiple alignment) と呼んで区別され，ペアワイズアライメントよりも効果的に配列の共通性を見出せる．

5.3 共変解析 (V3 loop)

V3 loop のそれぞれの位置では様々なアミノ酸が現れる場合もあれば，逆にほぼ決まったアミノ酸が現れる場合もある．そこで, V3 loop 内の位置の相関を，4 章で導入した共変指数を用いてはかり，共変グループの特定とアミノ酸ネットワークの解明を目的とて実験を行う．ここで，位置 i $(0 \leqq i \leqq 34)$ に現れるアミノ酸を $A^{(i)}$ ，アミノ酸の生起確率を $P(A^{(i)})$ とし，A はアミノ酸コードに対応する 20 種類のアルファベットをわたるものとする．

このとき，エントロピー $H(i)$，結合エントロピー $H(i_0, i_1, \cdots, i_m)$，高次相互情報量 $M(i_0, i_1, \cdots, i_m)$，共変指数 $K(i_0, \cdots, i_m)$ はそれぞれ以下の式で表せる．

$$
\begin{aligned}
H(i) &= -\sum_{A^{(i)}} P(A^{(i)}) \log P(A^{(i)}), \\
H(i_0, i_1, \cdots, i_m) &\stackrel{def}{=} -\sum_{A^{(i_j)}} P(A^{(i_0)}, A^{(i_1)}, \cdots, A^{(i_m)}) \log P(A^{(i_0)}, A^{(i_1)}, \cdots, A^{(i_m)}), \\
M(i_0, i_1, \cdots, i_m) &= \sum_{k=0}^{m} (-1)^{k-1} \sum_{1 \leq i_0 < \cdots < i_k \leq m} H(i_0, i_1, \cdots, i_k), \\
K(i_0, \cdots, i_m) &= \frac{M(i_0, \cdots, i_m)}{m+1} \sum_{j=i_0}^{i_m} \frac{1}{H(j)}.
\end{aligned}
$$

エントロピー $H(i)$ は非負であり，現れるアミノ酸が多様であるほど高い値を示す．また，$M(i_0,\cdots,i_m)$ の値は，位置 $i_0,\cdots,i_m$ の相関が強くなるほど大きくなる．具体的な実験手順を以下に示す．

m 位置共変グループ特定までのながれ

1. マルチプルアライメントを行って，配列長の同じアミノ酸配列データを作成する．
2. m 位置までの同時確率データの計算をする．
3. 2. で得られた同時確率データから，2 位置間から m 位置間までの全ての相互情報量を計算する．

$$\left(\begin{array}{l} m \text{ 位置間までの相互情報量のなかに，一つでも負の値を} \\ \text{とるものがあれば，共変なし} \end{array}\right)$$

4. 3. で得られた相互情報量から，2 位置間から m 位置間までの全ての共変指数を計算する．

$$\left(\begin{array}{l} 2\sim m \text{ 位置間までの共変指数のうち，一つでもその値が} \\ \text{閾値未満のとき，共変なし} \end{array}\right)$$

5. $m+1$ 位置での共変指数を考えた時，全ての位置における共変指数が閾値未満のとき，m 位置からなる共変グループが存在すると考えられる．

5.3.1 データ群の作成

V3 loop に関するアミノ酸配列のデータは NCBI のホームページから約 17000 例取り出す事ができる．これにいったん PAPIA システム [8] によるアライメントをかけて Cysteine から始まり Cysteine に終る長さ 35 前後の配列のみを取り出し，実験用のデータとした．さらに，HIV-1 の V3 loop におけるアミノ酸配列は，位置 14〜17 付近が GPGR(欧米分離株) のものと GPGQ(アフリカ分離株) のものとに分類されるため，この 2 種にデータ群を GPGR(8340 例) と GPGQ(4033 例) に大別した．このようにして得られたデータを最新版 clustal W にかけ，マルチプルアライメントを行った．さらに今回の実験では，ギャップの挿入の見られた位置は考察の対象からははずして，アミノ酸のみで構成される，位置のみを比較の対象とすることにして，配列長を 35 とした．従来の clustal W ver. 1.82 には，最

長配列×配列数 ≤ 10000 という処理上の制限があるため，一度に何千本もの配列のアライメントを行うことが不可能であったが，今回，これらの処理を国立遺伝学研究所にお願いすることで実現した．

5.4 実験結果

各位置におけるエントロピーを計算して，アミノ酸がどの程度変化しているのかを求める．また，2〜4 位置間での共変指数を算出する事により，アミノ酸が共変している可能性が高いと思われる位置を示す．

5.4.1 位置 i におけるエントロピー

V3 loop 領域における各位置のエントロピーの値を図 4 に示す．V3 loop 領域は両末端位置 0 と 34 に Cysteine(C) を持つ．また，位置 $14 \leq i \leq 17$ は，GPGR 型，GPGQ 型のみを実験の対象としているため，それらの位置についてはエントロピーの値は 0 となる．また，エントロピーの値が相対的に低い位置 $(2, 3, 5$〜$8, 27, 29, 30, 32)$ は保存性があり，エントロピーの高い位置 $(4, 9$〜$12, 18, 21, 24)$ は変異性に富んだ部位であると思われる．

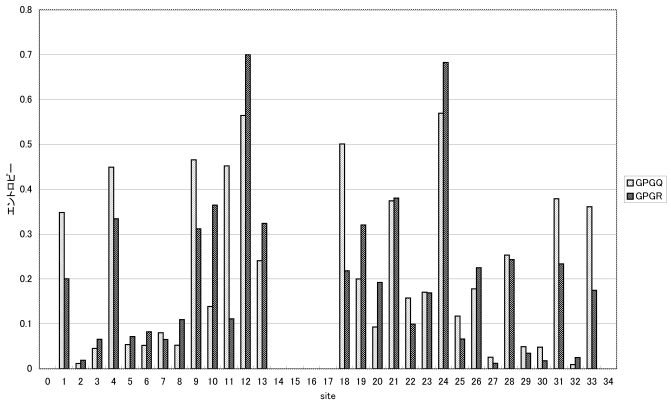


図 5.4 エントロピー $H(i)$

5.4.2 2 位置 (i, j) における共変指数

図 5.5，図 5.6 は 2 位置間での共変指数のグラフである．両位置におけるアミノ酸が完全な共変を示す時は最大値 1，完全に独立な変動，もしくは変動が無い時

には最小値 0 を示す．両型共に 2 位置間共変指数は，V3 loop の中間部分にあたる位置 4〜24 に他への依存度が大きいと思われる位置が多く現れる．

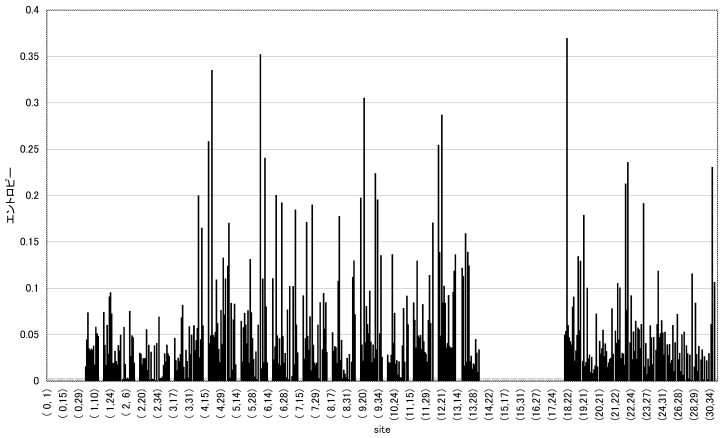


図 5.5 GPGQ 型：共変指数 $K(i,j)$

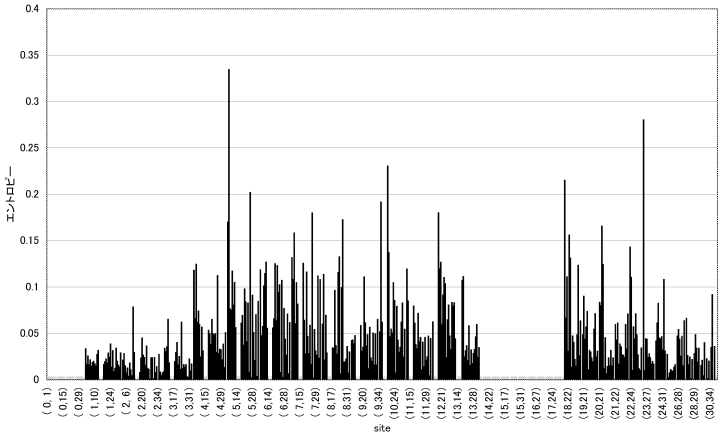


図 5.6 GPGR 型：共変指数 $K(i,j)$

5.4.3　3位置 (i, j, k) における共変指数

3位置間での共変指数の値が高いものから順に20組をGPGQ・GPGR型について表5.3に示す．また，図5.7, 図5.8は共変指数が高く，3位置の間で共変していると思われる位置グループを実線で結んだものである．GPGQ・GPGR型ともに，位置14〜17の左側のせまい位置間での3位置共変指数が高く見られ，また右側の位置では離れたいくつかの決まった位置が，3位置での共変に関与していると思われる．

表5.3　共変指数 $K(i, j, k)$

site(GPGQ)	共変指数
$(4, 18, 21)$	0.22516
$(9, 18, 21)$	0.17517
$(6, 7, 11)$	0.16845
$(4, 9, 21)$	0.15701
$(12, 18, 21)$	0.15215
$(9, 21, 31)$	0.15112
$(9, 21, 33)$	0.14668
$(6, 7, 21)$	0.13935
$(21, 31, 33)$	0.12926
$(4, 12, 21)$	0.12912
$(6, 7, 26)$	0.12611
$(9, 31, 33)$	0.11978
$(18, 21, 31)$	0.11328
$(6, 11, 21)$	0.10546
$(4, 9, 18)$	0.09917
$(4, 21, 31)$	0.09337
$(4, 12, 18)$	0.09289
$(18, 21, 33)$	0.09226
$(9, 12, 21)$	0.09052
$(12, 21, 33)$	0.09040
⋮	⋮

site(GPGR)	共変指数
$(10, 18, 19)$	0.09635
$(5, 7, 26)$	0.09522
$(5, 7, 10)$	0.08287
$(10, 12, 18)$	0.07499
$(4, 5, 7)$	0.05755
$(5, 6, 26)$	0.05650
$(10, 18, 31)$	0.05612
$(18, 23, 24)$	0.05568
$(5, 22, 28)$	0.05090
$(18, 19, 31)$	0.05025
$(7, 8, 10)$	0.05020
$(5, 6, 22)$	0.04636
$(7, 8, 26)$	0.04411
$(7, 10, 18)$	0.04402
$(12, 18, 19)$	0.04377
$(20, 23, 24)$	0.04351
$(5, 7, 8)$	0.04219
$(5, 10, 26)$	0.04171
$(7, 18, 21)$	0.04154
$(7, 18, 31)$	0.04113
⋮	⋮

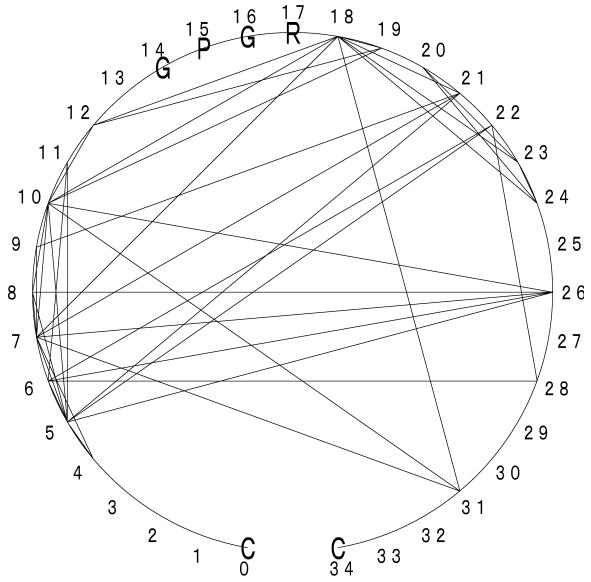


図 5.7 3 位置共変 (GPGR 型)

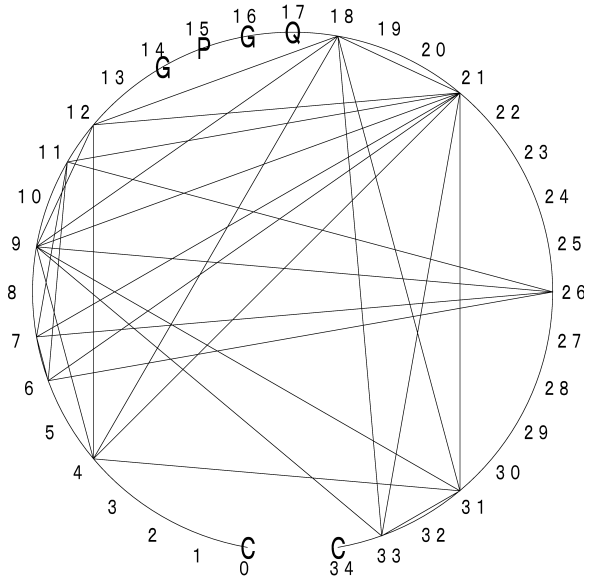


図 5.8 3 位置共変 (GPGQ 型)

5.4.4　4位置 (i, j, k, l) における共変指数

3位置間での共変指数で特に値の高かった GPGR 型の位置 (5,7,26)，(10,18,19)，GPGQ 型の位置 (4,9,18)，(6,7,11) について，これらの3位置と V3 loop 内の任意の位置における4位置での共変指数をそれぞれ図 5.9〜図 5.12 に示す．図 5.9 より，GPGR 型，3位置 (5,7,26) においては位置 $5, 8, 10, 22$ が，図 5.10 より (10,18,19) においては位置 $4, 7, 12, 31$ が4位置目の共変グループ候補としてあげられる．また，GPGQ 型の3位置 (4,9,18) においては，位置 21 が他の位置に比べ強い相関が見られる．同様に，(6,7,11) は位置 $11, 18, 21$ との強い相関が見られる．それぞれの4位置では，共変指数が他と比べ高い値をとる位置が存在することから，さらに4位置での共変指数の高い値を示した位置との5位置の共変指数を考えることで共変している可能性のある位置を絞り込み，共変グループの特定を行うことができると考える．この際，求める5位置での共変指数において，任意の 3〜4 位置の共変指数はすべて閾値以上の値をとり，さらに5位置の共変指数が閾値以上のものを，共変しているものとみなす．

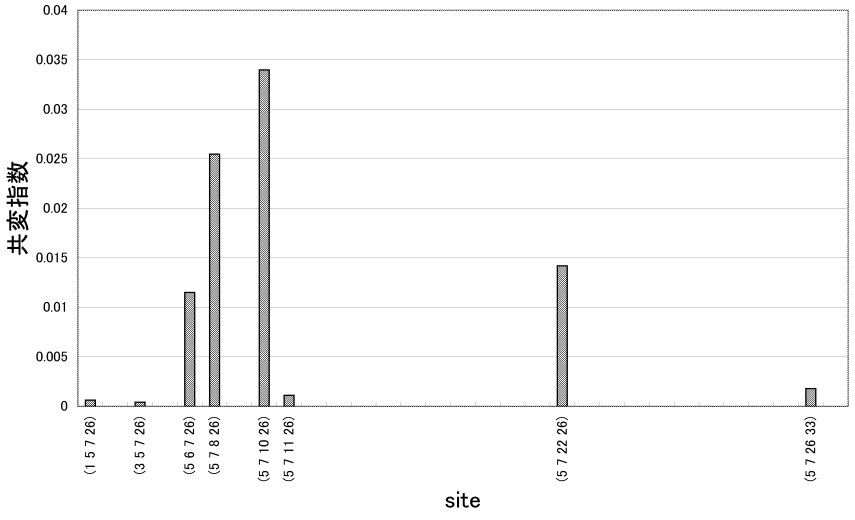


図 5.9　GPGR 型：共変指数 $K(5, 7, 26, i)$

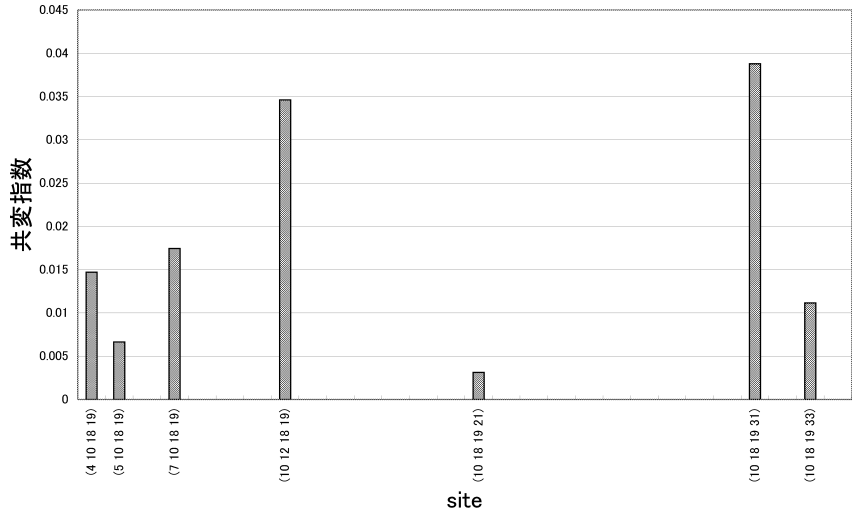


図 10　GPGR 型：共変指数 $K(10, 18, 19, i)$

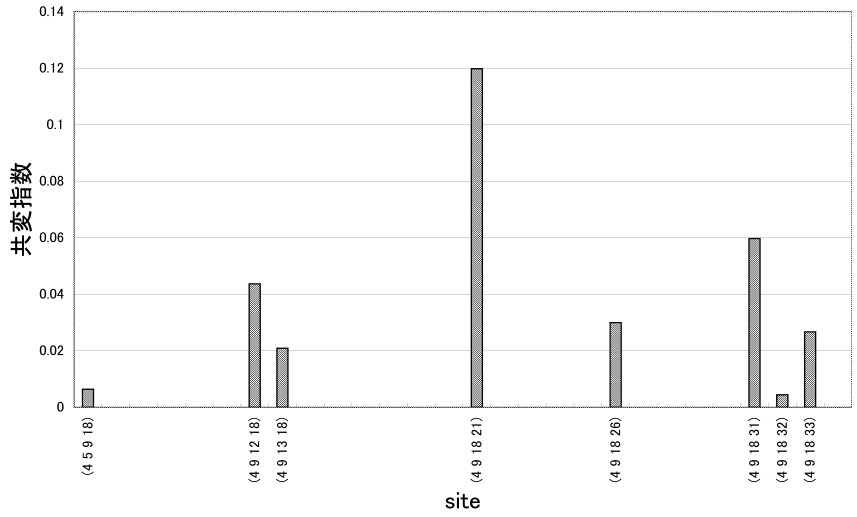


図 11　GPGQ 型：共変指数 $K(4, 9, 18, i)$

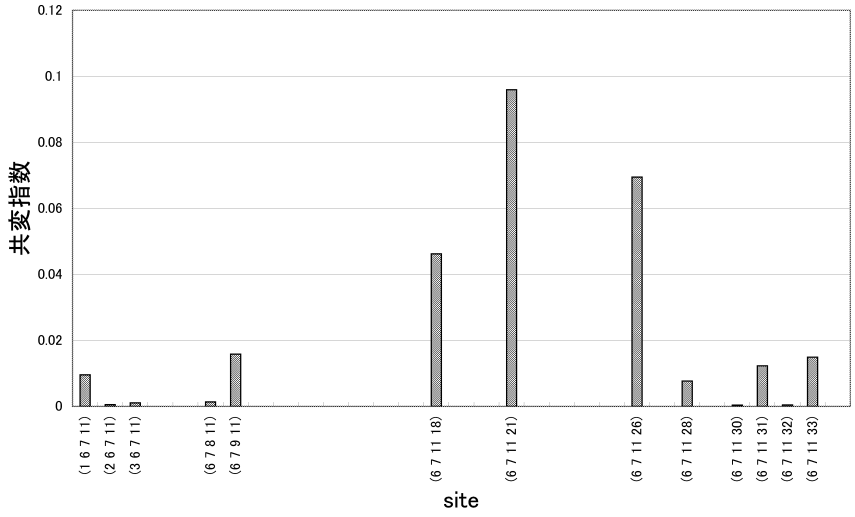


図 12 GPGQ 型：共変指数 $K(6,7,11,i)$

5.5　結論

5 章では，V3 loop 内のアミノ酸配列の位置に何らかの相互依存が存在し，V3 loop の機能もしくは構造に関与するという仮定のもとに，多次元相互情報量と新たに共変指数を導入することで，位置間に働くネットワークの解明を試みた．今回得られた数値データでは，V3 loop 内にいくつかのネットワークが存在することを予想させるものとなったが，さらに生物学，農学，薬学，医学面からの研究の進展を待って，その真偽を明らかにしたい．また，生体内の酵素などのタンパク質は，互いに依存しあいその働きが制御されている事はすでに知られ，新薬の開発等に活かされている．今回導入した手法をアミノ酸配列の変異の激しいウィルス等に応用することで，その研究に役に立つことを期待したい．

参考文献

2章

[1] C. Ding and V. Pless, Cyclotomy and duadic codes of prime lengths, Proceedings of 1998 IEEE, Inter. Sym. on IT, p.234, 1998.

[2] C. Ding and V. Pless, Cyclotomy and duadic codes of prime lengths, IEEE Trans. Inform. Theory, **45**, pp.453-466, 1999.

[3] T. Hiramatsu, Theory of automorphic forms of weight 1, Adv. Studies in Pure Math., **13**, pp.503-584, 1988.

[4] W. C. Huffman and V. Pless, Fundamentals of Error-Correcting Codes, Cambridge Univ.Press 2003.

[5] J. S. Leon, J. M. Masley, and V. Pless, Duadic codes, IEEE Trans.Inform. Theory, **30**, pp.709-714, 1984.

[6] N. Tschebotareff, Die Bestimmung der Dichtigkeit einer Menge von Primzahlen, welche zu einer gegebenen Substitutionsklasse gehören, Math. Ann., **95**, pp.191-228, 1926.

[7] 平松豊一; 数論を学ぶ人のための相互法則入門, 牧野書店,1988.

3章

[8] Taher Abualrub and Robert Oehmke,On the Generators of $\mathbf{Z}_4$ Cyclic Codes of Length 2^e, IEEE Trans.IT.,**49**,pp2126-2133,2003.

[9] V.Pless, Introduction to the Theory of Error-Correcting Codes, 3rd. ed, ser. Wiley-Intersci.Ser. Discrete Math.Optim. New York:Wiley,1998.

[10] 西村滋人 , 平松豊一, 有限剰余環上の誤り訂正符号, 法政大学工学部研究集報, **37**,pp11-16,2001.

[11] 今井秀樹, 符号理論, 電子情報通信学会,1990.

[12] Gilberto Bini and Flaminino Flamini,FINITE COMMUTATIVE RINGS AND THEIR APPLICATIONS, Kluwer Academic Pablishers,2002.

4章

[13] Acampora A., Bloom S.H., Krishnamurthy S., A hybrid approach for universal broadband access using small radio cells interconnected by free-space optical links,IEEE Journal on Selected Areas in Communications,Aug.1998,vol.16,no.6,pp.973-987

[14] Hoffman NG, Schiffer CA, Swanstrom R, Covariation of amino acid positions in HIV-1 protease, VIROLOGY 314 (2)，pp.536-548,SEP.30 2003

[15] 金子尚史，大場和隆，中山道彦，濱井龍明，光空間伝送ネットワーク (III) －メッシュ化による最短経路に関する一検討－，信学ソ，Mar.2002，B-5-307.

[16] 金子尚史，大場和隆，濱井龍明，光空間伝送ネットワーク (II) －メッシュ化によるノードの信頼性向上に関する一検討－，信学ソ，Mar.2002，B-5-306.

[17] Shoji Kaneko, Kazutaka Oba and Tatsuaki Hamai,
Evaluation of free space optical link availability in metropolitan Tokyo area Proceedings of SPIE, vol.4635.

[18] Shoji Kaneko, Tatsuaki Hamai, Kazutaka Oba, Evaluation of a free-space optical mesh network communication system in the Tokyo metropolitan area,Journal of Optical Networking,Vol.1, Iss.11,pp.414-423,Nov. 2002.

[19] 金子尚史，田畑慶太，中山道彦，森日出樹，濱井龍明，大場和隆，光空間伝送アクセスシステム-メッシュ型-光空間伝送アクセスによる大容量化・信頼性向上の提案-，信学ソ，Sep.2001，B-5-222，pp.508.

[20] Korber BT, Farber RM, Wolpert DH, Lapedes AS, Covariation of Mutations in the V3 Loop of Human Immunodeficiency Virus Type 1 Envelope Protein, An Information Theoretic Analysis, Proc Natl Acid Sci USA 1993,90,pp.7176-7180.

[21] K Kumekawaet al.,Influence of Weather Conditions on Data Communication through Optical Wireless LAN,The transactions of the institute of electronics, infomation and communication engineers B,2000,Vol.J83-B,pp.308-313.

[22] M.Oya,“Information Theoretial Treatment of Genes,” Trans. IEICE, E72-5, pp.556-560, May.1989.

[23] 森日出樹，大場和隆，濱井龍明，光空間伝送ネットワーク (IV)-メッシュ型網における経路の切り替え方式の一検討－，信学ソ，.2002，B-5-266.

[24] 中山道彦，森日出樹，金子尚史，大場和隆，濱井龍明，光空間伝送ネットワーク (I)-降水強度と視程との関係－，信学ソ，Mar.2002，B-5-308.

[25] 多田秀樹，関田英太郎，HIV-1 とエントロピー，研究集会「符号と暗号の代数的数理」，数理解析研究所講究録 1420，pp.18-27，2005.

[26] Park PJ and Kohane IS,Identifying three-way interactions among gene expression and chemosensitivity profiles using ternary mutual information,Technical report, Harvard University, Boston,MA.,2001.

5 章

[27] B.T.M. Korber, R.M.Farber, D.H.Wolpert, A.S.Lapedes, “Covariation of mutation in the V3 loop of human immunodeficiency virus type 1 envelope protein,” An information theoretic analysis, Proc.Natl. Acad.Sci.USA, vol.**90**, pp.7176-7180, August 1993.

[28] B. アルバート他 中村桂子他訳, 細胞の分子生物学第 3 版, 教育社,1995.

[29] M. Oya,“Information Theoretial Treatment of Genes,” Trans. IEICE, E72-5, pp.556-560, May 1989.

[30] 嵩忠雄, 情報と符号の理論入門, 昭晃堂,1989.

[31] 中山晃治, 田辺文雄, 多田秀樹, 関田英太郎, 平松豊一, 西村滋人,“エイズウィルスにおける V3 ループの情報理論的解析,” 第 25 回情報理論とその応用シンポジウム予稿集, pp.763-766, 2002.

[32] 多田秀樹, 関田英太郎,“HIV-1 とエントロピー,”研究集会「符号と暗号の代数的数理」, 数理解析研究所講究録 1420, pp.18-27, 2005.

[33] National Center for Biotechnology Information, http://www4.ncbi.nlm.nih.gov/Entrez/

[34] Parallel Protein Information Analysis System(PAPIA), http://www.cbrc.jp/papia-cgi/mul_queryJ.pl

業績リスト

論文

1. 多田秀樹, 西村滋人, Z/p^2Z 上の長さ p^e の巡回符号の多項式表現, 電子情報通信学会論文誌 和文論文誌 A,(acceptance)
2. 多田秀樹, 西村滋人, 共変指数とそのメッシュ型通信路の解析への応用, 電子情報通信学会論文誌 和文論文誌 A,(acceptance)
3. H.Tada, Shigeto Nishimura, Toyokazu Hiramatsu, Cyclotomy and its application to duadic codes,(to appear)
4. 多田秀樹, 平松豊一, HIV-1 の共変指数による解析, 法政大学工学部研究集報 第 **42** 巻 (2007),(投稿予定)

学会講演, 報告集等

4. 西村滋人, 多田秀樹, 斎藤正顕, A note on decoding of lifting BCH codes over Z/p^mZ, 第 29 回情報理論とその応用シンポジウム (SITA2006) 予稿集, 2006 年 11 月予定.
5. 多田秀樹, 西村滋人, 斎藤正顕, 平松豊一, 情報理論への共変指数の応用について, 第 28 回情報理論とその応用シンポジウム (SITA2005) 予稿集, 709-712, 2005 年 11 月.
6. 多田秀樹, 関田英太郎, HIV-1(V3loop) とエントロピー, 符号と暗号の代数的数理, 数理解析研究所講究録 1420, 18-27, 2005 年 4 月.
7. 多田秀樹, 西村滋人, 斎藤正顕, 平松豊一, Z/p^2Z 上での長さ P^e の巡回符号の構成, 第 27 回情報理論とその応用シンポジウム (SITA2004) 予稿集, 687-690, 2004 年 12 月.
8. T.Mimuro, H.Tada, S.Nishimura, S.Matsuda, T.Hiramatsu, On the Conjecture of Ding and Pless, Proc. of the 2004 International Sym. on Information Theory and its Applications, 172-177, Oct,2004.
9. 松井聖滋, 多田秀樹, 三室智明, 西村滋人, 平松豊一, Duadic 符号と巾剰余, 第 26 回情報理論とその応用シンポジウム (SITA2003) 予稿集, 469-472, 2003 年 12 月.
10. 多田秀樹, 三室智明, 平松豊一, 関田英太郎, 西村滋人, 松田修三, 符号理論を用いた遺伝子の解析, 第 25 回情報理論とその応用シンポジウム (SITA2002) 予稿集, 759-762, 2002 年 12 月.
11. 中山晃治, 田辺文雄, 多田秀樹, 関田英太郎, 平松豊一, 西村滋人, エイズウィ

ルスにおける V3 ループの情報理論的解析，第 25 回情報理論とその応用シンポジウム (SITA2002) 予稿集, 763-766, 2002 年 12 月.

謝辞

法政大学大学院工学研究科 平松豊一教授の本論文をまとめるに至るまでの辛抱強いご指導に深く感謝いたします．また，本論文の審査にあたって頂いた石浜明教授，本間教授 (神奈川工科大学)，尾川教授，浦谷規教授，に感謝します．
そして最後まで様々なアドバイスを頂いた西村滋人氏，関田英太郎氏，三室智明氏，斎藤正顕氏，金子尚史氏にこの場を借りて感謝いたします．