実験数学３

平成２２年 (２０１０年) 前期

渡部隆夫

Contents

1 可換環と体 **2**

2 素体と体の標数 **6**

3 体上のベクトル空間と行列 **9**

4 有限体 **12**

5 線形符号とエラー訂正 **15**

6 双対コードと検査行列 **19**

7 MDS コードと一般 Reed–Solomon コード **22**

8 巡回コード **26**

計算機演習項目

- 有限体上の多項式の既約分解, 有限体の原始元の計算
- 線形コードの最小距離, weight enumerator の計算
- 一般 Reed–Solomon コードの構成
- 巡回コードの構成, その最小距離の計算

参考図書

A. Betten, etal, Error-Correcting Linear Codes, Springer, 2006.
内田興二, 有限体と符号理論, サイエンス社, 2000.

1　可換環と体

定義　集合 A 上に和と積

$$A \times A \longrightarrow A : (a, b) \mapsto a + b, \quad a \cdot b$$

が定義されており, 以下をみたすときに A を**可換環**という.

(R1) 和と積は, 結合法則, 交換法則, 分配法則をみたす.

- $(a + b) + c = a + (b + c), \quad (a \cdot b) \cdot c = a \cdot (b \cdot c)$
- $a + b = b + a, \quad a \cdot b = b \cdot a$
- $(a + b) \cdot c = a \cdot c + b \cdot c$

(R2) $^{\exists}o \in A \quad ^{\exists}e \in A \quad \text{s.t.} \quad a + o = a, \quad a \cdot e = a \quad (^{\forall}a \in A)$

(R3) $^{\forall}a \in A \quad ^{\exists}a' \in A \quad \text{s.t.} \quad a + a' = o$

o を和の単位元 e を積の単位元といい, 通常 o を 0, e を 1 と表す. (R3) の a' を $-a$ と表す.

例 1 次は可換環になる. $\mathbf{Z}$:整数全体, $\mathbf{Q}$:有理数全体, $\mathbf{R}$:実数全体, $\mathbf{C}$:複素数全体

例 2 A を可換環として, X を不定元とするとき

$$f(X) = a_m X^m + \cdots + a_1 X + a_0 \,, \qquad (a_i \in A)$$

を A 係数多項式という. $a_m \neq 0$ のとき, $m = \deg f(X)$ を $f(X)$ の次数という. 形式的に $\deg 0 = -1$ とおく.

$$A[X] := A \text{ 係数多項式全体}$$

は, 多項式の和と積で可換環になる. これを A 上の **1 変数多項式環**という.

定義　A を可換環とする. $0 \neq a \in A$ に対し, $a \cdot x = 1$ をみたす元 $x \in A$ が存在するとき, a を**単元** といい, $x = a^{-1}$ を a の逆元という. A の単元全体の集合を $A^{\times}$ と表す.

例 3 $\mathbf{Z}^{\times} = \{\pm 1\}$ である. $\mathbf{Q}^{\times} = \mathbf{Q} \setminus \{0\}$, $\mathbf{R}^{\times} = \mathbf{R} \setminus \{0\}$, $\mathbf{C}^{\times} = \mathbf{C} \setminus \{0\}$ である.

定義　可換環 A が $A^{\times} = A \setminus \{0\}$ をみたすとき, A を**体**という.

例 4 例 3 から $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$ は体であるが, $\mathbf{Z}$ は体ではない.

命題 1 A を体とする.

1. $ab = 0$ ならば $a = 0$ または $b = 0$ である.
2. 任意の 1 次方程式 $aX + b = 0$ $(a \neq 0)$ は A で唯一つの根をもつ.

証明　容易

以下 $\mathbf{Z}$ と体上の多項式環を調べる.

(I) Z

記号と定義

- $a \in \mathbf{Z}$ に対し,
$$(a) = a\mathbf{Z} := \{an \ : \ n \in \mathbf{Z}\} : \ a \text{ の倍数全体}$$
とおく. とくに $(0) = \{0\}$, $(1) = (-1) = \mathbf{Z}$.
- $0 \neq a, b \in \mathbf{Z}$ に対し, a が b を割り切ることを $a \mid b$ と表す. 明らかに
$$a \mid b \iff b \in (a) \iff (b) \subset (a)$$
- 部分集合 $A \subset \mathbf{Z}$ が次の 2 条件をみたすとき, A を**イデアル**という.
  1. $\alpha, \beta \in A \implies \alpha + \beta \in A$
  2. $\alpha \in A \implies \alpha n \in A$, $(^{\forall} n \in \mathbf{Z})$ (とくに $0 \in A$, $-\alpha \in A$ である.)

命題 2 (a) はイデアルである. 逆に $A \subset \mathbf{Z}$ がイデアルならば, $^{\exists} g \in \mathbf{Z}$ で $A = (g)$ となる.

証明 前半は明らか. $A = \{0\}$ ならば $A = (0)$ でよい. $A \neq \{0\}$ のとき
$$g = \min\{0 < \alpha \in A\}$$
が存在する. $g \in A$ だから, $gn \in A$ $(^{\forall} n \in \mathbf{Z})$. よって $(g) \subset A$. 逆に $0 \neq {}^{\forall}\alpha \in A$ に対し, $g \leq |\alpha|$ だから, 剰余の定理より
$$\alpha = gr + q, \qquad r \in \mathbf{Z}, \ \ 0 \leq q < g$$
となる. ここで $q = \alpha - gr = \alpha + (-gr) \in H$ だから, $0 \neq q$ ならば g の最小性に矛盾. よって $q = 0$ で $\alpha = gr \in (g)$. したがって $H \subset (g)$.

命題 3 $0 \neq a, b \in \mathbf{Z}$ をとり, $m = \gcd(a, b)$ を a と b の最大公約数とする.
$$H = \{ax + by \ : \ x, y \in \mathbf{Z}\}$$
とおけば, $H = (m)$ である.

証明 $m > 1$ の場合: H は $\mathbf{Z}$ のイデアルである. $(0) \neq H$ だから, $0 < {}^{\exists} g \in \mathbf{Z}$, $H = (g)$ となる. $a, b \in H = (g)$ より $g \mid a$ かつ $g \mid b$. よって $g \mid m$ から $g = 1$ で, $H = (1) = \mathbf{Z}$.
$m > 1$ の場合: $a' = a/m, b' = b/m$ とおけば, $\gcd(a', b') = 1$. よって
$$H' = \{a'x + b'y \ : \ x, y \in \mathbf{Z}\} = \mathbf{Z}$$
したがって
$$H = \{ax + by \ : \ x, y \in \mathbf{Z}\} = \{m(a'x + b'y) \ : \ x, y \in \mathbf{Z}\} = m\mathbf{Z} = (m)$$

命題 4 $0 \neq a, b \in \mathbf{Z}$ に対し
$$(1) \ \gcd(a, b) = 1 \iff (2) \ \{ax + by \ : \ x, y \in \mathbf{Z}\} = \mathbf{Z}$$
$$\iff (3) \ ^{\exists} c, d \in \mathbf{Z} \quad \text{s.t.} \quad ac + bd = 1$$

証明 $(1) \implies (2)$ は命題 3. $(2) \implies (3)$ は自明. $(3) \implies (1)$ を示す. (3) より
$$1 = ac + bd \in H = \{ax + by \ : \ x, y \in \mathbf{Z}\} = (m), \quad (m = \gcd(a, b))$$
だから, $m \mid 1$, 即ち $m = 1$ である.

(II) 体上の多項式環

$F[X]$ を体 F 上の 1 変数多項式環とする. F のゼロを 0, $F[X]$ のゼロを $0(X)$ と表す. $f(X)g(X) = 0(X)$ ならば $f(X) = 0(X)$ または $g(X) = 0(X)$ である.

定理 1 (剰余定理) $f(X), g(X) \in F[X]$ に対し,

$$^{\exists}q(X), r(X) \in F[X] \quad \text{s.t.} \quad f(X) = q(X)g(X) + r(X), \qquad \deg r(X) < \deg g(X)$$

この $q(X), r(X)$ は一意である.

証明 $\deg f(X) = m$, $\deg g(X) = n$ として

$$f(X) = a_m X^m + \cdots + a_0, \qquad g(X) = b_n X^n + \cdots + b_0$$

とする.
$m < n$ ならば, $q(X) = 0(X)$, $r(X) = f(X)$ とすればよい.
$m \geqq n$ とする.

$$h_1(X) = f(X) - a_m b_n^{-1} X^{m-n} g(X) \in F[X]$$

とすると

$$h_1(X) = a'_{m-1} X^{m-1} + \cdots + a'_0$$

次に

$$h_2(X) = h_1(X) - a'_{m-1} b_n^{-1} X^{m-n-1} g(X) \in F[X]$$

とおけば,

$$h_2(X) = a''_{m-2} X^{m-2} + \cdots + a''_0$$

以下, これを繰り返していくと

$$r(X) = h_{m-n+1}(X) \in F[X], \quad \deg r(X) < n$$

で,

$$q(X) = a_m b_n^{-1} X^{m-n} + a'_{m-1} b_n^{-1} X^{m-n-1} + \cdots \in F[X]$$

とすれば, $f(X) - q(X)g(X) = r(X)$ となる. 一意性も容易.

命題 5 $f(X) \in F[X]$, $\alpha \in F$ に対し

$$f(X) = (X - \alpha)q(X) + f(\alpha) \qquad (^{\exists}q(X) \in F[X])$$

とくに

$$f(\alpha) = 0 \iff f(X) = (X - \alpha)q(X)$$

(このとき α を $f(X)$ の根という.)

証明 定理 1 で, $g(X) = (X - \alpha)$ とすればよい.

定義 $f(X) \in F[X]$ が,

$$f(X) = g_1(X)g_2(X), \qquad (^{\exists}g_i(X) \in F[X], \deg g_i[X] \geqq 1)$$

と分解するとき, F 上可約であるという. 可約でないとき, 既約という.

記号と定義

- $f(X) \in F[X]$ に対し

$$(f(X)) := \{f(X)h(X) \ : \ h(X) \in F[X]\}$$

とおく. $0(X) \neq g(X) \in (f(X))$ であるとき, $f(X)$ は $g(X)$ を割り切るといい, $f(X) \mid g(X)$ と表す.

- 部分集合 $A \subset F[X]$ が次の 2 条件をみたすとき, イデアルという.

1. $\varphi(X), \psi(X) \in A \implies \varphi(X) + \psi(X) \in A$
2. $\varphi(X) \in A \implies \varphi(X)h(X) \in A \ (^{\forall}h(X) \in F[X])$

$F[X]$ は $\mathbf{Z}$ と同様の性質をもつ.

命題 6 $^{\forall}f(X) \in F[X]$ に対し, $(f(X))$ はイデアルである. 逆に $A \subset F[X]$ がイデアルならば, $^{\exists}f(X) \in F[X]$ s.t. $A = (f(X))$. この $f(X)$ は F の元による定数倍を除いて一意である.

証明 $A = \{0(X)\}$ ならば $A = (0(X))$ となる, $A \neq \{0(X)\}$ のとき,

$$n = \min\{\deg \varphi(X) \ : \ 0(X) \neq \varphi(X) \in A\} \geq 0$$

が存在する. $f(X) \in A$ を $\deg f(X) = n$ ととる. $^{\forall}h(X) \in F[X]$ に対し, $f(X)h(X) \in A$ であるから, $(f(X)) \subset A$. 逆に, $^{\forall}\varphi(X) \in A$ に対し, 剰余の定理から

$$\varphi(X) = f(X)q(X) + r(X), \qquad (q(X), r(X) \in F[X], \ \deg r(X) < \deg f(X) = n)$$

このとき, $r(X) = \varphi(X) + f(X)(-q(X)) \in A$ で, $\deg r(X) < n$ だから, n の最小性より $r(X) = 0(X)$. よって, $\varphi(X) = f(X)q(X) \in (f(X))$.
もし, $A = (f(X)) = (f'(X))$ ならば, $f(X) \mid f'(X)$ かつ $f'(X) \mid f(X)$ であるから, $f'(X) = cf(X)$ $(^{\exists}c \in F^{\times})$ となる.

命題 7 $0(X) \neq f(X), g(X) \in F[X]$ とし, $m(X) = \gcd(f(X), g(X))$ を $f(X)$ と $g(X)$ の最大公約因子とする.

$$H = \{f(X)\varphi(X) + g(X)\psi(X) \ : \ \varphi(X), \psi(X) \in F[X]\}$$

とおけば, H はイデアルであり $H = (m(X))$ となる. 更に

$$\begin{aligned} m(X) = 1 \quad (\text{定数}) &\iff H = F[X] \\ &\iff {}^{\exists}\varphi(X), \psi(X) \in F[X] \quad \text{s.t.} \quad f(X)\varphi(X) + g(X)\psi(X) = 1 \end{aligned}$$

証明 証明は 命題 3,4 と同じ.

2　素体と体の標数

$g \in \mathbf{Z}$ を固定する. $a, b \in \mathbf{Z}$ に対し, $a - b \in (g)$ となることを

$$a \equiv b \mod g$$

と表し, a と b は g を法として合同であるという. これは次をみたす.

- $a \equiv a \mod g$
- $a \equiv b \mod g \implies b \equiv a \mod g$
- $a \equiv b \mod g$ かつ $b \equiv c \mod g \implies a \equiv c \mod g$

即ち, $\equiv \mod g$ は $\mathbf{Z}$ に同値関係を定める.

a に同値な元全体の集合を $\overline{a}$ で表す.

$$\overline{a} := \{b \in \mathbf{Z} \ : \ a \equiv b \mod g\} = \{a + gn \ : \ n \in \mathbf{Z}\}$$

明らかに

$$\overline{a} = \overline{b} \iff a \equiv b \mod g$$

同値類全体の集合を

$$\mathbf{Z}/(g) = \{\overline{a} \ : \ a \in \mathbf{Z}\}$$

とおく. $a \in \mathbf{Z}$ に対し

$$a = gr + q, \qquad r \in \mathbf{Z}, \ 0 \leq r < g$$

とすると, $a - q = gr \in (g)$ だから $a \equiv q \mod g$. よって, ${}^{\forall}a$ は, $0, 1, \cdots, g-1$ の一つと同値. したがって $\mathbf{Z}/(g) = \{\overline{0}, \overline{1}, \overline{2}, \cdots, \overline{g-1}\}$.

命題 8 $\mathbf{Z}/(g)$ に和と積を次で定義する.

$$\text{和: } \overline{a} + \overline{b} = \overline{a+b}, \qquad \text{積: } \overline{a} \cdot \overline{b} = \overline{ab}$$

これらの定義は well-defined で, この和と積により $\mathbf{Z}/(g)$ は可換環になる.

証明　和と積が well-defined であることは,

$$\overline{a} = \overline{c}, \quad \overline{b} = \overline{d} \implies \overline{a+b} = \overline{c+d}, \quad \overline{ab} = \overline{cd}$$

を示せばよい. $c = a + gm$, $d = b + gn$ だから

$$\overline{c+d} = \overline{a+b+g(m+n)} = \overline{a+b}, \quad \overline{cd} = \overline{ab+g(an+bm+gmn)} = \overline{ab}$$

でいえた.
可換環になることは (R1), (R2), (R3) を見ればよい. (R1) は容易. (R2) は, $o = \overline{0}$, $e = \overline{1}$ で成立. (R3) は $-\overline{a} = \overline{-a}$ で成立.

例 5 $\mathbf{Z}/(4) = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$ の和と積は

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$		$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$			$\overline{0}$	$\overline{1}$
$\overline{3}$				$\overline{2}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$		$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$			$\overline{0}$	$\overline{2}$
$\overline{3}$				$\overline{1}$

$\mathbf{Z}/(4)$ の単数は $(\mathbf{Z}/(4))^\times = \{\overline{1}, \overline{3}\}$ である.

補題 1 $a \in \mathbf{Z}$ に対し

$$\overline{a} \in (\mathbf{Z}/(g))^\times \iff \gcd(a, g) = 1$$

証明

$$\begin{aligned}
\overline{a} \in (\mathbf{Z}/(g)^\times &\iff {}^\exists\overline{x} \in \mathbf{Z}/(g) \quad \text{s.t.} \quad \overline{ax} = \overline{1} \quad \text{i.e.,} \quad \overline{ax} = \overline{1} \\
&\iff ax \equiv 1 \mod g \\
&\iff {}^\exists y \in \mathbf{Z} \quad \text{s.t.} \quad ax = 1 - gy \\
&\iff {}^\exists x, y \in \mathbf{Z} \quad \text{s.t.} \quad ax + gy = 1 \\
&\iff \gcd(a, g) = 1 \quad (\text{命題 4 より})
\end{aligned}$$

命題 9 $\mathbf{Z}/(g)$ が体 $\iff$ g は素数

証明 ($\Longleftarrow$) g が素数ならば, 補題 1 より $\overline{1}, \cdots, \overline{g-1} \in (\mathbf{Z}/(g))^\times$. よって $(\mathbf{Z}/(g))^\times = \mathbf{Z}/(g) \setminus \{\overline{0}\}$ だから $\mathbf{Z}/(g)$ は体である.
($\Longrightarrow$) 対偶を示す. g が合成数で, p を g の素因数とすれば, $\overline{p} \notin (\mathbf{Z}/(g))^\times$ だから, $\overline{0} \neq \overline{p}$ は逆元をもたない. よって $\mathbf{Z}/(g)$ は体にならない.

定義 p が素数のとき, 体 $\mathbf{Z}/(p)$ を $\mathbf{F}_p$ と表し, **標数 p の素体**という.

F を任意の体とする. $a \in F$ と $n \in \mathbf{Z}$ に対し, a の n 倍を

$$na := \begin{cases} a + \cdots + a & (n > 0) \\ 0_F & (n = 0) \\ (-a) + \cdots + (-a) & (n < 0) \end{cases}$$

と定める. 明らかに次が成り立つ.

- $n(a + b) = na + nb, \quad n(a \cdot b) = (na) \cdot b = a \cdot (nb)$
- $(m + n)a = ma + na, \quad (mn)a = m(na) = n(ma)$
- $(-n)a = n(-a)$

$\mathbf{Z}$ の部分集合 $\mathbf{Z}_F$ を次で定める.

$$\mathbf{Z}_F := \{n \in \mathbf{Z} \ : \ n1_F = 0_F\}$$

$0 \in \mathbf{Z}_F$ であるが, $\mathbf{Z}_F$ は 0 以外の元を含むことがある.

例 6 $F = \mathbf{F}_p$ のとき,

$$n\overline{a} = \overline{na} \qquad ({}^\forall n \in \mathbf{Z},\ \overline{a} \in \mathbf{F}_p)$$

とくに

$$p\overline{1} = \overline{p} = \overline{0}$$

となるから, $p \in \mathbf{Z}_{\mathbf{F}_p}$ である.

命題 10 $\mathbf{Z}_F \neq \{0\}$ ならば, ある素数 p が存在して, $\mathbf{Z}_F = (p) = p\mathbf{Z}$ となる.

証明 $\mathbf{Z}_F$ はイデアルである. 即ち

1. $\alpha, \beta \in \mathbf{Z}_F \implies \alpha + \beta \in \mathbf{Z}_F$
2. $\alpha \in \mathbf{Z}_F \implies \alpha n \in \mathbf{Z}_F$ $({}^\forall n \in \mathbf{Z})$

が成り立つ. 命題 3 から $\mathbf{Z}_F \neq \{0\}$ ならば $\mathbf{Z}_F = (g)$ となる $0 < g \in \mathbf{Z}$ が存在する. g は $\mathbf{Z}_F$ に含まれる最小の正の整数である. g が素数でなければ, $g = mn$ と分解できる. このとき

$$0_F = g1_F = (mn)1_F = m(n1_F) = m(1_F \cdot n1_F) = (m1_F) \cdot (n1_F)$$

となるから, 命題 1 より $m1_F = 0_F$ または $n1_F = 0_F$ となり, g の最小性に矛盾. よって g は素数である.

定義 $\mathbf{Z}_F = (g)$ ($g = 0$ または素数) のとき, この g を F の**標数**とよび, $\mathrm{ch}(F) = g$ と表す.

例 7 $\mathrm{ch}(\mathbf{Q}) = \mathrm{ch}(\mathbf{R}) = \mathrm{ch}(\mathbf{C}) = 0$. $\mathrm{ch}(\mathbf{F}_p) = p$.

命題 11 $\mathrm{ch}(F) = 0$ ならば $\mathbf{Q} \subset F$ である. $\mathrm{ch}(F) = p > 0$ ならば $\mathbf{F}_p \subset F$ である.

証明 $\mathrm{ch}(F) = 0$ ならば $\mathbf{Z}_F = (0)$. $0 \neq m \in \mathbf{Z}$ ならば $0_F \neq m1_F$ だから $m1_F$ は逆元 $(m1_F)^{-1}$ をもつ. このとき, 対応

$$\mathbf{Q} \ni \frac{n}{m} \longrightarrow (n1_F)(m1_F)^{-1} \in F$$

は単射であり, $\mathbf{Q} \subset F$ となる. p でも同様.

命題 12 $\mathrm{ch}(F) = p > 0$ ならば

1. $pa = 0_F$ $({}^\forall a \in F)$
2. $(a + b)^p = a^p + b^p$ $({}^\forall a, b \in F)$

証明 1. 定義より $p1_F = 0_F$ である. よって $pa = p(1_F \cdot a) = (p1_F) \cdot a = 0_F \cdot a = 0_F$.
2. $(a + b)^p = a^p + pa^{p-1}b + \cdots + pab^{p-1} + b^p = a^p + b^p$.

3　体上のベクトル空間と行列

F を体とする.

定義　集合 V に和とスカラー倍

(和) $V \times V \longrightarrow V : (v, w) \mapsto v + w$　　(スカラー倍) $F \times V \longrightarrow V : (a, v) \mapsto av$

が定義されており, 以下をみたすときに V を F **ベクトル空間**という.

(V1) 和とスカラー倍は, 結合法則, 交換法則, 分配法則をみたす.

- $(u + v) + w = u + (v + w)$, $(ab)v = a(bv)$
- $v + w = w + v$
- $a(v + w) = av + aw$, $(a + b)v = av + bv$

(V2) $^{\exists}o \in V$　s.t.　$v + o = v$　$(^{\forall}v \in V)$　(以下 v' を $-v$ と書く)

(V3) $^{\forall}v \in V$, $^{\exists}v'$　s.t.　$v + v' = o$

(V4) $1_F v = v$,　$0_F v = o$　$(^{\forall}v \in V)$

例 8 $1 \leq n \in \mathbf{Z}$ を固定して

$$F^n := \left\{ \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = {}^t(x_1, \cdots, x_n) \ : \ x_1, \cdots, x_n \in F \right\}$$

とする. 和とスカラー倍を

$${}^t(x_1, \cdots, x_n) + {}^t(y_1, \cdots, y_n) = {}^t(x_1 + y_1, \cdots, x_n + y_n), \quad a\,{}^t(x_1, \cdots, x_n) = {}^t(ax_1, \cdots, ax_n)$$

と定義すれば F^n は F ベクトル空間となる.

例 9 E, F はともに体として, $F \subset E$ であるとする. E の和とスカラー倍を

$$E \times E \longrightarrow E : (v, w) \mapsto v + w \quad \text{体の和}$$
$$F \times E \longrightarrow E : (a, v) \mapsto av \quad \text{体の積}$$

とすれば E は F ベクトル空間となる.

実ベクトル空間と同様に F ベクトル空間でも次が定義される.

- ベクトルの 1 次独立性, 1 次従属性
- 部分空間, 基底, 次元

V が F ベクトル空間で, $v_1, \cdots, v_k \in V$ のとき

$$\langle v_1, \cdots, v_k \rangle_F := \{a_1 v_1 + \cdots + a_k v_k \ : \ a_1, \cdots, a_k \in F\}$$

とおく. これは V の部分空間である.

例 10 $\mathbf{R} \subset \mathbf{C}$ だから, 例 10 により $\mathbf{C}$ は $\mathbf{R}$ ベクトル空間となる. $1, \sqrt{-1}$ は $\mathbf{R}$ 上 1 次独立で, $\mathbf{C} = \langle 1, \sqrt{-1} \rangle_{\mathbf{R}}$ だから, $1, \sqrt{-1}$ は基底である. よって $\dim_{\mathbf{R}} \mathbf{C} = 2$ である.

例 11 $F = \mathbf{F}_2 = \{\overline{0}, \overline{1}\}$ のとき,

$$V = \mathbf{F}_2^3 = \left\{ \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \ : \ x_1, x_2, x_3 \in \mathbf{F}_2 \right\}$$

は 3 次元空間であるが, 元の個数は 8 個である. V の 1 次元部分空間, 2 次元部分空間はともに 7 個しかない.

$1 \leq m, n \in \mathbf{Z}$ を固定して, mn 個の元 $a_{ij} \in F$ $(1 \leq i \leq m,\ 1 \leq j \leq n)$ を長方形に並べたもの

$$\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix}$$

を F に成分をもつ (m, n) 行列という.

実行列と同様に次が定義される.

- 行列のスカラー倍, 和, 積
- 行列の基本変形
- ランク
- 正方行列の場合に, 正則行列, 逆行列, 行列式, 余因子行列, 固有多項式

F に成分をもつ (m, n) 行列全体を $M_{m,n}(F)$ と表し, n 次正方行列全体を $M_n(F)$ と表す.

例 12 $F = \mathbf{F}_2 = \{\overline{0}, \overline{1}\}$ のとき

$$M_2(\mathbf{F}_2) = \left\{ \begin{array}{cccccc} \begin{pmatrix} \overline{0} & \overline{0} \\ \overline{0} & \overline{0} \end{pmatrix}, & \begin{pmatrix} \overline{1} & \overline{0} \\ \overline{0} & \overline{0} \end{pmatrix}, & \begin{pmatrix} \overline{0} & \overline{1} \\ \overline{0} & \overline{0} \end{pmatrix}, & \begin{pmatrix} \overline{0} & \overline{0} \\ \overline{1} & \overline{0} \end{pmatrix}, & \begin{pmatrix} \overline{0} & \overline{0} \\ \overline{0} & \overline{1} \end{pmatrix}, & \begin{pmatrix} \overline{1} & \overline{1} \\ \overline{0} & \overline{0} \end{pmatrix} \\ \begin{pmatrix} \overline{0} & \overline{0} \\ \overline{1} & \overline{1} \end{pmatrix}, & \begin{pmatrix} \overline{1} & \overline{0} \\ \overline{1} & \overline{0} \end{pmatrix}, & \begin{pmatrix} \overline{0} & \overline{1} \\ \overline{0} & \overline{1} \end{pmatrix}, & \begin{pmatrix} \overline{1} & \overline{0} \\ \overline{0} & \overline{1} \end{pmatrix}, & \begin{pmatrix} \overline{0} & \overline{1} \\ \overline{1} & \overline{0} \end{pmatrix}, & \begin{pmatrix} \overline{1} & \overline{1} \\ \overline{1} & \overline{0} \end{pmatrix} \\ \begin{pmatrix} \overline{1} & \overline{1} \\ \overline{0} & \overline{1} \end{pmatrix}, & \begin{pmatrix} \overline{1} & \overline{0} \\ \overline{1} & \overline{1} \end{pmatrix}, & \begin{pmatrix} \overline{0} & \overline{1} \\ \overline{1} & \overline{1} \end{pmatrix}, & \begin{pmatrix} \overline{1} & \overline{1} \\ \overline{1} & \overline{1} \end{pmatrix} & & \end{array} \right\}$$

$A = \begin{pmatrix} \overline{1} & \overline{1} \\ \overline{1} & \overline{1} \end{pmatrix}$ の固有多項式は

$$\det(XI - A) = \begin{vmatrix} X - \overline{1} & -\overline{1} \\ -\overline{1} & X - \overline{1} \end{vmatrix} = (X - \overline{1})^2 - \overline{1} = X^2$$

となる.

$A \in M_{m,n}(F)$ は, 線形写像

$$F^n \longrightarrow F^m \ : \ \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \mapsto A \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

を与え, これから部分空間

$$\mathrm{Ker}A := \{v \in F^n \ : \ f_A(v) = o\}, \qquad \mathrm{Im}A := \{f_A(v) \ : \ v \in F^n\}$$

が定まる. 実ベクトル空間と同様に次が成り立つ.

- $\dim_F \mathrm{Ker}A + \dim_F \mathrm{Im}A = n$
- $\dim_F \mathrm{Im}A = \mathrm{rank}A$

定義　F ベクトル空間 F^n において,

1. $v = {}^t(a_1, \cdots, a_n), w = {}^t(b_1, \cdots, b_n)$ に対し

$$(v, w) := {}^tvw = a_1b_1 + a_2b_2 + \cdots + a_nb_n \in F$$

と定める. これを F^n 上の**標準双線形形式**とよぶ.

2. $W \subset F^n$ が部分空間のとき

$$W^\perp := \{v \in W \ : \ (w, v) = 0 \quad ({}^\forall w \in W)\}$$

とおく. $W^\perp$ は部分空間である. これを W の**双対空間**という.

命題 13 $W \subset F^n$ を $\dim W = k$ の部分空間とするとき

1. $\dim W^\perp = n - k$
2. $(W^\perp)^\perp = W$

証明　1. W の基底を $w_1, \cdots, w_k$ として, これらを列にもつ行列を

$$A = (w_1, \cdots, w_k) \in M_{n,k}(F)$$

とする.

$$v \in W^\perp \iff (w_1, v) = \cdots = (w_k, v) = 0 \iff {}^tAv = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

であるから, $W^\perp = \mathrm{Ker}\,{}^tA$. よって $\dim W^\perp = n - \mathrm{rank}\,{}^tA = n - k$.
2. $W \subset (W^\perp)^\perp$ は容易. 次元が等しいので $W = (W^\perp)^\perp$ となる.

注 一般に $W^\perp$ は W の補空間とは限らない. 即ち $W^\perp \cap W \neq \{0\}$ となる場合がある.

例 13 $\mathbf{F}_2^3$ の 2 次元部分空間

$$W = \langle w_1, w_2 \rangle_{\mathbf{F}_2}, \qquad w_1 = {}^t(\overline{1}, \overline{0}, \overline{0}), \quad w_2 = {}^t(\overline{1}, \overline{1}, \overline{1})$$

の双対空間は

$$W^\perp = \langle w_1 + w_2 \rangle_{\mathbf{F}_2} \subset W$$

となる.

4　有限体

定義　体 F と E が, $F \subset E$ をみたすとき, E を F の**拡大体**, F を E の**部分体**という.

定理 2 (代数的閉体の存在) F を体とする. このとき, F の拡大体 Ω ($F \subset \Omega$) で次の条件をみたすものが存在する.

(AC1) ${}^{\forall}f(X) \in F[X]$ ($\deg f(X) \geq 1$) は $\Omega[X]$ において 1 次式の積に分解する.

とくに Ω は ${}^{\forall}f(X) \in F[X]$ の根をすべて含む.

証明は略. (**注** このような Ω は無数にある).

例 14 $F = \mathbf{Q}, \mathbf{R}$ ならば $\Omega = \mathbf{C}$ は (AC1) をみたす.

以下 F を体として, (AC1) をみたす Ω を 1 つ固定する.
$f(X) \in F[X]$ を既約多項式とし, $\alpha \in \Omega$ を $f(X)$ の一つの根とするとき

$$F(\alpha) := \{g(\alpha) \in \Omega \ : \ g(X) \in F[X]\}$$

とおく.

命題 14 $\deg f(X) = n$ とする.

1. $F(\alpha)$ は体で, F の拡大体である.
2. $1, \alpha, \alpha^2, \cdots, \alpha^{n-1}$ は $F(\alpha)$ の F ベクトル空間としての基底になる. とくに, 任意の元 $\lambda \in F(\alpha)$ は

$$\lambda = a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{n-1}\alpha^{n-1} \qquad (a_0, \cdots, a_{n-1} \in F)$$

と一意的に表示される.

証明　1. $F(\alpha)$ が環になることと $F \subset F(\alpha)$ は容易. $0 \neq {}^{\forall}\lambda \in F(\alpha)$ が逆元をもつことを示す. $\lambda = g(\alpha) \neq 0$ と書ける. $f(X)$ は既約だから, $\gcd(f(X), g(X))$ は $f(X)$ または 1 である. $\gcd(f(X), g(X)) = f(X)$ ならば, $f(X) \mid g(X)$ だから, $g(\alpha) = 0$ となり矛盾. よって $\gcd(f(X), g(X)) = 1$. 命題 7 より,

$${}^{\exists}\varphi(X), \psi(X) \in F[X] \quad \text{s.t.} \quad f(X)\varphi(X) + g(X)\psi(X) = 1$$

α を代入すれば, $g(\alpha)\psi(\alpha) = 1$. 即ち $g(\alpha)^{-1} = \psi(\alpha) \in F(\alpha)$ である.
2. $W := \langle 1, \alpha, \cdots, \alpha^{n-1} \rangle_F$ とおく.

$$W = \{r(\alpha) \ : \ r(X) \in F[X], \ \deg r(X) \leq n-1\}$$

である. ${}^{\forall}g(X) \in F[X]$ に対し, $g(\alpha) \in W$ を示す. 剰余定理から

$$g(X) = f(X)q(X) + r(X), \qquad (q(X), r(X) \in F[X], \ \deg r(X) < \deg f(X) = n)$$

と書けるので

$$g(\alpha) = r(\alpha) \in W$$

よって $F(\alpha) = W$ である.
$1, \alpha, \cdots, \alpha^{n-1}$ が 1 次独立であることを示す. これらが 1 次従属と仮定すると

$$a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} = 0$$

となる少なくとも一つは 0 と異なる $a_0, \cdots, a_{n-1} \in F$ が取れる.

$$h(X) = a_0 + a_1 X + \cdots + a_{n-1}X^{n-1} \in F[X]$$

をとれば, $h(\alpha) = 0$ かつ $1 \leq \deg h(X) \leq n-1$. $f(X)$ は既約だから $\gcd(f(X), h(X)) = 1$ で,

$$^{\exists}\varphi(X), \psi(X) \in F[X] \quad \text{s.t.} \quad f(X)\varphi(X) + h(X)\psi(X) = 1$$

α を代入すれば $0 = 1$ となり矛盾.

例 15 $f(X) = X^2 + 2 \in \mathbf{Q}[X]$ は既約, その $\mathbf{C}$ での根 $\sqrt{-2}$ をとる.

$$\mathbf{Q}(\sqrt{-2}) = \{g(\sqrt{-2}) \ : \ g[X] \in \mathbf{Q}[X]\} = \{a + b\sqrt{-2} \ : \ a, b \in \mathbf{Q}\}$$

である. これは体で $\mathbf{Q}$ 上 2 次元ベクトル空間となる.

定義 元の個数が有限である体を**有限体**という.

命題 15 F が有限体ならば, $\mathrm{ch}(F) = p > 0$ である.

証明 命題 11 より, $\mathrm{ch}(F) = 0$ ならば $\mathbf{Q} \subset F$ で $\sharp F = \infty$ となり矛盾.

命題 16 F が有限体で $\mathrm{ch}(F) = p$ ならば, $\sharp F$ は p のべきである.

証明 命題 11 より, $\mathbf{F}_p \subset F$ である. F は $\mathbf{F}_p$ ベクトル空間になる. $\sharp F < \infty$ だから, F は有限次元になる. $\dim_{\mathbf{F}_p} F = n$ とすれば, 基底 $e_1, \cdots, e_n$ が存在して

$$F = \langle e_1, \cdots, e_n \rangle_{\mathbf{F}_p} = \{a_1 e_1 + \cdots + a_n e_n \ : \ a_1, \cdots, a_n \in \mathbf{F}_p\}$$

よって $\sharp F = p^n$ となる.

具体的に p^n 個の元をもつ体を作るためには, $\mathbf{F}_p$ に命題 14 を適用する.

定理 3 $\mathbf{F}_p$ を素体とする.

1. $1 \leq {}^{\forall}n \in \mathbf{Z}$ に対し $\mathbf{F}_p[X]$ には既約 n 次多項式 $f(X)$ が存在する.
2. $f(X)$ の 1 つの根を $\alpha \in \Omega$ とすると, $\mathbf{F}_p(\alpha)$ は p^n 個の元をもつ体である.
3. F が $q = p^n$ 個の元をもつ任意の体ならば, F は多項式 $X^q - X$ の根全体と一致する. とくに $X^q - X$ は F で 1 次式の積に分解する.

証明　1. $\mathbf{F}_p[X]$ の n 次既約多項式で X^n の係数が 1 のものすべての個数を N とすると

$$\frac{1}{n}\left(p^n - \sum_{p_i} p^{n/p_i}\right) \leq N$$

が証明できる. ここで p_i は素数で n のすべての素因数を動く.
2. は命題 14 から明らか.
3. $F^\times = \{a_1, \cdots, a_{q-1}\}$ とする. $b \in F^\times$ を固定する. このとき, 写像

$$F^\times \longrightarrow F^\times : a_i \mapsto ba_i$$

は単射である. よって $\{a_1, \cdots, a_{q-1}\} = \{ba_1, \cdots, ba_{q-1}\}$. 積をとれば

$$a_1 \cdots a_{q-1} = (ba_1) \cdots (ba_{q-1}) = b^{q-1}(a_1 \cdots a_{q-1})$$

よって $b^{q-1} = 1$. したがって, $^\forall b \in F^\times$ は $X^{q-1} - 1$ の根である.

定義　定理 3 より, $q = p^n$ 個の元をもつ有限体は $X^q - X = 0$ の根全体であり本質的にただ一つしかない. これを $\mathbf{F}_q$ と表す.

例 16 $F = \mathbf{F}_2 = \{\overline{0}, \overline{1}\}$ とする.

$$f(X) = X^2 + X + \overline{1} \in \mathbf{F}_2[X]$$

は既約である. もし既約でなければ, これは 1 次式の積に分解するから, $\overline{0}$ または $\overline{1}$ を根にもつが, $f(\overline{0}) = \overline{1}, f(\overline{1}) = \overline{3} = \overline{1}$ で, どちらも根にならないから矛盾する. $f(X)$ の根を α とすれば

$$\mathbf{F}_4 = \mathbf{F}_2(\alpha) = \{\overline{0}, \overline{1}, \alpha, \overline{1} + \alpha\}$$

α の積は, $\alpha^2 = -\alpha - \overline{1} = \alpha + \overline{1}$.

命題 17 $^\exists\alpha \in \mathbf{F}_q^\times$　s.t.　$\alpha^j \neq 1\ (1 \leq j \leq q-2),\ \alpha^{q-1} = 1$. とくに $\mathbf{F}_q^\times = \{1, \alpha, \alpha^2, \cdots, \alpha^{q-2}\}$ となる. この α を $\mathbf{F}_q$ の**原始元**という.

証明　$q-1$ の素因数分解を $q - 1 = p_1^{e_1} \cdots p_r^{e_r}$ とする. $d_i = p_i^{e_i}$ とおく. 写像

$$\sigma_i, : \mathbf{F}_q^\times \longrightarrow \mathbf{F}_q^\times : \sigma_i(a) = a^{(q-1)/d_i}$$

を考える. $\sigma_i(a)^{d_i} = a^{q-1} = 1$ だから $\mathrm{Im}\sigma_i \subset (X^{d_i} - 1$ の根全体$)$

$$\sigma_i(a) = \sigma_i(b) \iff (a/b)^{(q-1)/d_i} = 1 \iff {}^\exists\zeta \in (X^{(q-1)/d_i} - 1 \text{ の根})\quad \text{s.t.}\quad a = b\zeta$$

したがって, $c \in \mathrm{Im}\sigma_i$ ならば $\sharp\sigma_i^{-1}(c) \leq (q-1)/d_i$ である.

$$\mathbf{F}_q^\times = \bigsqcup_{c \in \mathrm{Im}\sigma_i} \sigma_i^{-1}(c), \qquad q - 1 = \sharp(\mathbf{F}_q^\times) \leq (\sharp\mathrm{Im}\sigma_i)\frac{q-1}{d_i}$$

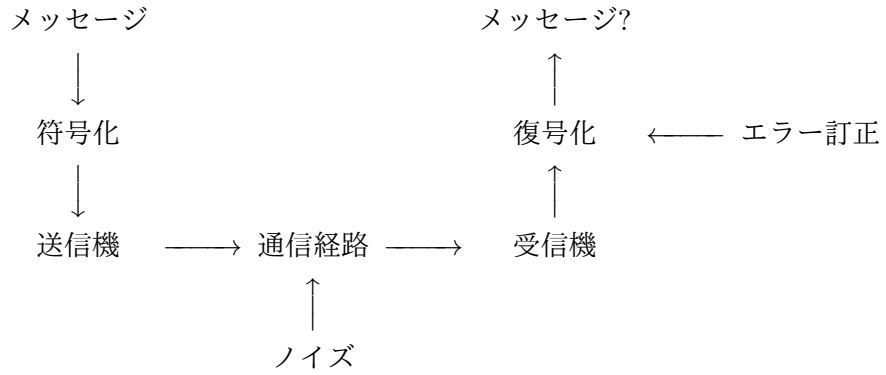
より, $d_i \leq \sharp\mathrm{Im}\sigma_i$. 一方 $\sharp(X^{d_i} - 1$ の根全体$) \leq d_i$ だから, $\mathrm{Im}\sigma_i = (X^{d_i} - 1$ の根全体$)$ となる.

$$\alpha_i \in (X^{d_i} - 1 \text{ の根全体}) \setminus (X^{d_i/p_i} - 1 \text{ の根全体})$$

を一つとる. このとき $\alpha = \alpha_1\alpha_2 \cdots \alpha_r$ は条件をみたす.

5　線形符号とエラー訂正

通信 (communication) には様々な種類がある (メール, インターネット, 電話, テレビ, ナビゲーション, 手紙, 会話). ここでは次の通信形態を考える.



「符号化」「復号化」「エラー訂正」のシステムを考える. このシステムで要求されることは

- 効率性 $\cdots$ 符号化に必要なビット数が少なければ, 通信, 復号の時間と経費が少.
- 正確性 $\cdots$ ノイズが入った場合にどれだけ正確に修正が可能か

この「効率性」と「正確性」は互いに相反するので, バランスが問題となる.

例 17 ある会への出欠をメールで通信する. 符号に $\{0,1\}$ を使い, 1 ビットが正しく受信される確率を $1-\epsilon$ とする. 誤送信される確率が ϵ である.
符号化に

$$\text{「出席」} \longrightarrow 1, \qquad \text{「欠席」} \longrightarrow 0$$

と 1 ビットだけを使うと, 効率はよいがエラーは全く修正されず, 正しく受信される確率は $1-\epsilon$ である. 符号化に 3 ビットを使い

$$\text{「出席」} \longrightarrow (1,1,1) \qquad \text{「欠席」} \longrightarrow (0,0,0)$$

とする. ノイズが入り, 例えば $(1,0,1)$ が受信された場合, これを $(1,1,1)$ とみなす. 即ち $0,1$ の多い方をとる. このとき, 正しく受信される確率は $1-3\epsilon^2+2\epsilon^3$ となり, $\epsilon<1/2$ ならばこちらがより正確である.

符号化に使われる文字 (アルファベット) には一定の有限集合 (英字 a $\sim$ z, 数字 0 , 1 など) を用いる. 文字を n 個並べたものを長さ n の語 (ワード) という. 符号化に使う語全体の集合をワード空間という.

例 18 有限体 $\mathbf{F}_q$ $(q=p^m)$ の元を文字として使い, 長さが一定 $(=n)$ の語だけを使う場合

$$\text{ワード空間} = \{{}^t(a_1,\cdots,a_n) \,:\, a_i \in \mathbf{F}_q\} = \mathbf{F}_q^n$$

である.

例 19 $\mathbf{F}_2=\{0,1\}$ として, ワード空間を $\mathbf{F}_2^2$ とする. 符号化に際して, すべての語に意味をもたせるとエラー訂正ができない. M_1,M_2,M_3,M_4 という 4 つのメッセージがあり,

$$M_1 \longrightarrow \begin{pmatrix}0\\0\end{pmatrix}, \quad M_2 \longrightarrow \begin{pmatrix}0\\1\end{pmatrix}, \quad M_3 \longrightarrow \begin{pmatrix}1\\0\end{pmatrix}, \quad M_4 \longrightarrow \begin{pmatrix}1\\1\end{pmatrix}$$

と符号化する. 1 ビットの誤送信確率を ϵ とすれば, メッセージが正しく復号できる確率は $(1-\epsilon)^2$ で. この場合修正はできない.
他方, ワード空間を $\mathbf{F}_2^5$ にとり,

$$M_1 \longrightarrow \begin{pmatrix}0\\0\\0\\0\\0\end{pmatrix}, \quad M_2 \longrightarrow \begin{pmatrix}0\\0\\1\\1\\1\end{pmatrix}, \quad M_3 \longrightarrow \begin{pmatrix}1\\1\\1\\0\\0\end{pmatrix}, \quad M_4 \longrightarrow \begin{pmatrix}1\\1\\0\\1\\1\end{pmatrix}$$

と符号化する. 互いのベクトルは少なくとも 3 か所が異なる. よって 1 ビットのエラーは修正できる. よって正しく復号できる確率は, $(1-\epsilon)^5 + 5\epsilon(1-\epsilon)^4$ で, $\epsilon \leq 0.35$ ならば, これは前よりもよい.

定義　ワード空間の中で意味を割り当てられた語を符号語 (コードワード) という. コードワード全体の集合をメッセージ空間とよぶ. ワード空間とメッセージ空間のペア

$$C = (\text{ワード空間}, \text{メッセージ空間}) = (V_C, W_C)$$

を符号 (コード) とよぶ.

定義　コード $C = (V_C, W_C)$ が, $V_C = \mathbf{F}_q^n$ かつ $W_C \subset \mathbf{F}_q^n$ が部分空間であるとき, C を**線形コード**という. $\dim_{\mathbf{F}_q} W_C = k$ ならば, これを $\mathbf{F}_q$ 上の (n,k) コードといい, $[n,k]_q$ と略記する. n を C の長さ, k を C の次元, $k/n < 1$ を**符号化率**という.

例 20 上の例に現れた

$$C = (\mathbf{F}_2^5, W), \quad W = \left\{ \begin{pmatrix}0\\0\\0\\0\\0\end{pmatrix}, \quad \begin{pmatrix}0\\0\\1\\1\\1\end{pmatrix}, \quad \begin{pmatrix}1\\1\\1\\0\\0\end{pmatrix}, \quad \begin{pmatrix}1\\1\\0\\1\\1\end{pmatrix} \right\}$$

は $[5,2]_2$ である.

定義　$C = (\mathbf{F}_q^n, W)$ を (n,k) コードとする. W は基底 $w_1, \cdots, w_k$ をもつ. これを列とする行列

$$A_C = (w_1, \cdots, w_k) \in M_{n,k}(\mathbf{F}_q)$$

を C の**生成行列**という.

例 21 前の例では

$$A_C = \begin{pmatrix}0&1\\0&1\\1&1\\1&0\\1&0\end{pmatrix}$$

線形コードの基本用語

定義　$v = {}^t(a_1, \cdots, a_n),\ w = {}^t(b_1, \cdots, b_n) \in \mathbf{F}_q^n$ に対し

1. $|v| := \sharp\{i\ :\ a_i \neq 0\}$ を v の **Hamming weight** という.
2. $d(v, w) = |v - w|$ を v と w の **Hamming 距離**という.

命題 18　d は $\mathbf{F}_q^n$ の距離である. 即ち, 次をみたす.

i　$d(v, w) \geq 0$ で, $d(v, w) = 0 \iff v = w$

ii　$d(v, w) = d(w, v)$

iii　$d(v, w) \leq d(v, u) + d(u, w)$.

更に,

iv　$d(v, w) = d(v + u, w + u)$

v　$d(\lambda v, \lambda w) = d(v, w)$ $({}^\forall\lambda \in \mathbf{F}_q^\times)$

も成り立つ.

証明　証明は容易

定義　$[n, k]_q$ コード $C = (\mathbf{F}_q^n, W)$ に対し,

$$d_C := \min\{d(w_1, w_2)\ :\ w_i \in W,\ w_1 \neq w_2\} = \min\{|w|\ :\ 0 \neq w \in W\}$$

を C の**最小距離**という. 最小距離 d の $[n, k]_q$ コードを $[n, k, d]_q$ コードとよぶ.

命題 19　$C = (\mathbf{F}_q^n, W)$ を $[n, k, d]_q$ コードとし

$$t := \left[\frac{d-1}{2}\right] = \frac{d-1}{2} \text{ 以下の最大の整数}$$

とおく. ${}^\forall w \in W$ に対し, w を中心とする半径 t の球を

$$B(w, t) := \{w + e\ :\ e \in \mathbf{F}_q^n,\ |e| \leq t\}$$

とすれば,

$$B(w, t) \cap W = \{w\}$$

となる.

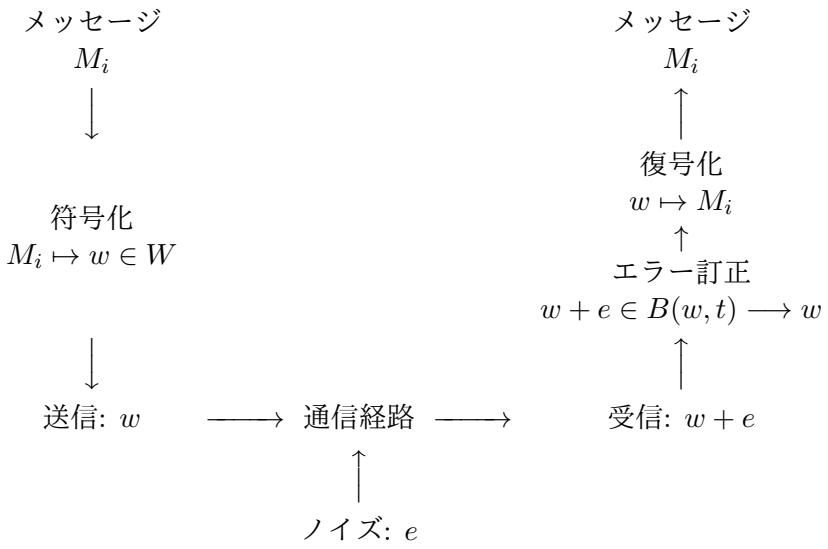
証明　$|e| \leq t$ で, $w + e \in W$ とする. このとき $w \neq w + e$ ならば

$$d = d_c \leq d(w, w + e) = |e| \leq t < d$$

となり矛盾.

ビットエラーの訂正

$C = (\mathbf{F}_q^n, W)$ を $[n,k,d]_q$ コードとして, メッセージ $\{M_i\}$ を C を用いて通信することを考える. このシステムは



と表され, ノイズの範囲が $|e| \leq t$ に収まれば, エラー訂正ができる. これは各 $w = {}^t(a_1, \cdots, a_n)$ の成分のうち, t 個までのエラーは修正できることを意味する. この復号化を **Maximum Likelihood Decoding** という.

$\mathbf{F}_q$ の 1 文字の誤通信が確率 ϵ で起こるとして, 誤りが独立に起こるならば, エラー訂正ができずに誤ったメッセージを受け取る確率は

$$\mathbf{P}_{\text{error}}(C) = \sum_{j=t+1}^{n} {}_nC_j \epsilon^j (1-\epsilon)^{n-j}$$

となる.

例 22 例 20 の $C = (\mathbf{F}_2^5, W)$ は $[5,2,3]_2$ コードであるから, $t = 1$. $\epsilon = 10^{-4}$ とすると, $\mathbf{P}_{\text{error}}(C) = 9.998 \times 10^{-8}$ となる. 他方, $\mathbf{F}_2^{15}$ で $[15,8,5]_2$ コード C' が存在し, これを用いれば $t = 2$, $\mathbf{P}_{\text{error}}(C') = 4.545 \times 10^{-10}$ である.

$[n,k,d]_q$ コードの効率性と正確性の尺度は

- 符号化率 $k/n < 1$ が 1 に近いほど効率がよい.
- $d/n < 1$ が 1 に近いほど, エラー訂正が効果的になり, 正確さが増す.

ということになり, $k/n, d/n$ が共に 1 に近いほど良いコードになる.

注 エラーには, 上で述べた誤送信エラーの他に, ビット消失, バーストエラーなどもあるが, ここでは扱わない.

6　双対コードと検査行列

$\mathbf{F}_q^n$ の標準双線形形式

$$(v,w) = {}^t vw = a_1b_1 + \cdots + a_nb_n$$

をとる. 部分空間 $W \subset \mathbf{F}_q^n$ の双対空間は

$$W^\perp = \{v \in \mathbf{F}_q^n \ : \ (w,v) = 0 \quad ({}^\forall w \in W)\}$$

であった.

定義　コード $C = (\mathbf{F}_q^n, W)$ に対し, $C^\perp := (\mathbf{F}_q^n, W^\perp)$ を C の**双対コード**という. C が $[n,k]_q$ コードならば $C^\perp$ は $[n, n-k]_q$ コードである.

命題 20 $C^\perp = (\mathbf{F}_q^n, W^\perp)$ の生成行列を $A_{C^\perp} \in M_{n,n-k}(\mathbf{F}_q)$ とすると, $v \in \mathbf{F}_q^n$ に対し

$$v \in W \iff {}^t A_{C^\perp} v = 0$$

である. 即ち $W = \mathrm{Ker}\, {}^t A_{C^\perp}$.

証明　$W = (W^\perp)^\perp$ であったから,

$$v \in W \iff (w', v) = 0 \quad ({}^\forall w' \in W^\perp) \iff {}^t A_{C^\perp} v = 0$$

定義　コード C に対し, $H_C := {}^t A_{C^\perp} \in M_{n-k,n}(\mathbf{F}_q)$ を C の**検査行列**という.

双対コードを使ったエラー訂正復号を述べる.

(I) Syndrome Decoding
Maximum Likelihood Decoding で, エラーベクトルを決定する方法である. $C = (\mathbf{F}_q^n, W)$ を $[n,k,d]_q$ コードとして, $t = [(d-1)/2]$ とする.
$H_C v \in \mathbf{F}_q^n$ $(v \in \mathbf{F}_q^n)$ を**シンドロームベクトル**という.

$$B(0,t) = \{e \in \mathbf{F}_q^n \ : \ |e| \le t\} = \{e_1, \cdots, e_\ell\}$$

として, シンドロームベクトルのリスト $\{H_C e_i\}_{1 \le i \le \ell}$ を作っておく.

$$H_C e_i = H_C e_j \implies H_C(e_i - e_j) = 0 \implies e_i - e_j \in W \cap B(0,2t) = \{0\} \implies e_i = e_j$$

に注意する.
送信コードを $w \in W$, その受信コードを z とする. ノイズの範囲が $|z-w| \le t$ であれば, z から w が次のように復元できる. シンドローム $H_C z$ に対し, $H_C z = H_C(z-w)$ で, $z - w \in B(0,t)$ だから, $H_C z$ はリスト $\{H_C e_i\}$ にある. よって $H_C z = H_C e_i$ となる e_i が 1 つ定まる. このとき $w = z - e_i$ である.

(II) Majority Logic Decoding
$\mathbf{F}_2$ 上のコードでのエラー訂正復号である. $C = (\mathbf{F}_2^n, W)$ を $[n,k]_2$ コードとする. $u_1, \cdots, u_r \in W^\perp$ を列にもつ行列を

$$U = (u_1, \cdots, u_r) \in M_{n,r}(\mathbf{F}_q)$$

とする. $W^{\perp}$ の定義から

$$ {}^tUw = \begin{pmatrix} (u_1, w) \\ \vdots \\ (u_r, w) \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \qquad ({}^{\forall} w \in W) $$

である. この意味で U をパリティ検査行列という.

定義 $1 \leq i_0 \leq n$ を固定する. U が,

1. U の第 i_0 行の成分はどれも 0 ではない.
2. ${}^{\forall} i \neq i_0$ に対し, U の第 i 行の成分で 0 でないものは高々1 つである.

をみたすとき, U を**焦点 i_0 のパリティ検査行列**という.

U を焦点 i_0 のパリティ検査行列とする. 送信ワード $w \in W$ の受信ワードを $z = w + e$ として, $|e| \leq [r/2]$ と仮定する. このとき

$$ e_{i_0} = \begin{cases} 0 & (|{}^tUy| \leq r/2 : \text{パリティ検査で 0 の数が半数以上}) \\ 1 & (\text{それ以外：パリティ検査で 1 の数が半数未満}) \end{cases} $$

が成り立つ. よって, すべての i について, 焦点 i のパリティ検査行列 $U_i \in M_{n,k}(\mathbf{F}_q)$ が存在すれば, $|y - w| \leq [r/2]$ のエラーが訂正できる. r の大きさは $r \leq (n-1)/(d_{C^{\perp}} - 1)$ であることが示される.

コードの同型を定義する.

定義 線形写像 $T : \mathbf{F}_q^n \longrightarrow \mathbf{F}_q^n$ が, $|Tv| = |v|$ $({}^{\forall} v \in \mathbf{F}_q^n)$ をみたすとき, **線形等長**(linear isometry) という. 線形等長は全単射である.

命題 21 線形写像 $T : \mathbf{F}_q \longrightarrow \mathbf{F}_q$ を行列と見たとき

$$ T \text{ が線形等長} \iff T \text{ は単項行列} = \left(\begin{array}{l} T \text{ の各行各列に 0 でない成分が} \\ \text{丁度一つだけある} \end{array} \right) $$

証明 $(\Longrightarrow)$ $e_1, \cdots, e_n$ を $\mathbf{F}_q^n$ の標準基底とする. $v \in \mathbf{F}_q^n$ に対し

$$ |v| = 1 \iff {}^{\exists}\lambda \in \mathbf{F}_q^{\times} \ {}^{\exists} i \quad \text{s.t.} \quad v = \lambda e_i $$

である. $|Te_j| = |e_j| = 1$ だから $T\boldsymbol{e}_j = \lambda_j e_{i_j}$ とかける. よって

$$ T = (t_{ij}), \quad t_{ij} = \begin{cases} \lambda_j & (i = i_j) \\ 0 & (i \neq i_j) \end{cases} $$

は条件をみたす. 逆 $(\Longleftarrow)$ は容易.

定義　2つの $[n,k]_q$ コード $C=(\mathbf{F}_q^n, W)$ と $C'=(\mathbf{F}_q^n, W')$ に対し, 線形等長 $T:\mathbf{F}_q^n \longrightarrow \mathbf{F}_q^n$ で $T(W)=W'$ となるものが存在するとき, C と C' は**同型**であるといい, $C\cong C'$ と表す. このとき, 生成行列には $A_{C'}=TA_C$ の関係がある.

命題 22 C を $[n,k]_q$ コードとする. このとき C に同型なコード C' で, 生成行列が

$$A_{C'}=\begin{pmatrix} I_k \\ B \end{pmatrix} \in M_{n,k}(\mathbf{F}_q)$$

となるものがある. この形の生成行列をもつコードを**組織的**(systematic) であるという. このとき, C' の検査行列は $H_{C'}=(-B, I_{n-k})$ となる.

証明　C に同型なコーの生成行列は

$$TA_CS, \qquad (T\in GL_n(\mathbf{F}_q) \text{ は単項行列}, S\in GL_k(\mathbf{F}_q))$$

の形をもつ. T,S を適当に取れば上の形になる.

定義　$[n,k]_q$ コード $C=(\mathbf{F}_q^n, W)$ に対し, 2変数多項式

$$G_C(X,Y)=\sum_{w\in W} X^{|w|}Y^{n-|w|} \in \mathbf{Z}[X,Y]$$

を C の **weight enumerator** という.

明らかに, $C\cong C' \implies G_C(X,Y)=G_{C'}(X,Y)$. 対偶を取れば $G_C(X,Y)\neq G_{C'}(X,Y) \implies C\ncong C'$. これは2つのコードが同型でないことの判定に使われる.

定理 4 (MacWilliams の恒等式) C が $[n,k]_q$ コードならば

$$G_{C^\perp}(X,Y)=q^{-k}G_C(Y-X, Y+(q-1)X)$$

証明は略.

例 23 $\mathbf{F}_2^4$ で, $W=\langle {}^t(1,1,0,0), {}^t(1,0,0,1)\rangle_{\mathbf{F}_2}$ とすれば, $C=(\mathbf{F}_2^4, W)$ は $[4,2]_2$ コードで, $G_C(X,Y)=3X^2Y^2+Y^4$. $C^\perp$ も $[4,2]_2$ コードであるが

$$G_{C^\perp}(X,Y)=\frac{1}{4}\{3(Y-Z)^2(Y+X)^2+(Y+X)^4\}=X^4+X^3Y+Y^3X+Y^4$$

だから, $C\ncong C^\perp$. また $d_{C^\perp}=1$.

7 MDS コードと一般 Reed–Solomon コード

命題 23 $[n,k]_q$ コード $C=(\mathbf{F}_q^n, W)$ の検査行列を $H_C=(\boldsymbol{a}_1,\cdots,\boldsymbol{a}_n)$ $(\boldsymbol{a}_i\in\mathbf{F}_q^{n-k})$ とする. $\boldsymbol{a}_1,\cdots,\boldsymbol{a}_n$ の中で, どの $r-1$ 個も 1 次独立となり, 適当に r 個のベクトルを選べば 1 次従属になる組があるとする. このとき $d_C=r$ である.

証明 $\boldsymbol{a}_{i_1},\cdots,\boldsymbol{a}_{i_r}$ が 1 次従属とすると,

$$0\neq{}^{\exists}\lambda_1,\cdots,\lambda_r\in\mathbf{F}_q \quad \text{s.t.} \quad \lambda_1\boldsymbol{a}_{i_1}+\cdots+\lambda_r\boldsymbol{a}_{i_r}=0$$

ベクトル $v={}^t(c_1,\cdots,c_n)\in\mathbf{F}_q^n$ を

$$c_i=\begin{cases}\lambda_\ell & (i=i_\ell,\ell=1,\cdots,r)\\ 0 & (i\neq i_\ell)\end{cases}$$

ととれば

$$H_Cv=\lambda_1\boldsymbol{a}_{i_1}+\cdots+\lambda_r\boldsymbol{a}_{i_r}=0$$

となるので, $v\in W$ である. これから $d_C\leq|v|=r$ となる.
ベクトル $0\neq w\in W$ を $|w|=d=d_C$ ととる. $w={}^t(\mu_1,\cdots,\mu_n)$ として 0 と異なる成分を $\mu_{j_1},\cdots,\mu_{j_d}$ とする. このとき

$$0=H_Cw=\mu_{j_1}\boldsymbol{a}_{j_1}+\cdots+\mu_{j_d}\boldsymbol{a}_{j_d}$$

だから $\boldsymbol{a}_{j_1},\cdots,\boldsymbol{a}_{j_d}$ は 1 次従属となる. よって $r\leq d=d_C$.

命題 24 (Singleton 限界式) C が $[n,k,d]_q$ コードならば, $d\leq n-k+1$.

証明 $\operatorname{rank}H_C=\operatorname{rank}A_{C^\perp}=\dim C^\perp=n-k$ である. これから H_C の $n-k+1$ 個の列ベクトルで 1 次従属な組がある. よって, 命題 23 の r は $r\leq n-k+1$ である.

定義 C を $[n,k,d]_q$ コードとする. Singleton 限界式で等号が成り立つとき, 即ち $d=n-k+1$ のとき, C を **MDS(Maximum Distance Separable) コード**という.

命題 25 $C=(\mathbf{F}_q^n,W)$ を $[n,k,n-k+1]_q$ MDS コードとする. このとき $C^\perp=(\mathbf{F}_q^n,W^\perp)$ は $[n,n-k,k+1]_q$ MDS コードである.

証明 Singleton の限界式から $d_{C^\perp}\leq k+1$ である. $d_{C^\perp}\leq k$ と仮定して矛盾を出す.

$$A_{C^\perp}=\begin{pmatrix}{}^t\boldsymbol{a}_1\\ \vdots\\ {}^t\boldsymbol{a}_n\end{pmatrix}=(\boldsymbol{b}_1,\cdots,\boldsymbol{b}_{n-k})=(b_{ij}),\qquad(\boldsymbol{a}_i\in\mathbf{F}_q^{n-k},\ \boldsymbol{b}_j\in\mathbf{F}_q^n)$$

とする. 命題 23 より, $\boldsymbol{a}_1,\cdots,\boldsymbol{a}_n$ のどの $n-k$ 個のベクトルの組も 1 次独立になるから, $A_{C^\perp}$ の任意の $n-k$ 小行列式は 0 ではない. $\boldsymbol{b}_1,\cdots,\boldsymbol{b}_{n-k}$ は $W^\perp$ の基底だから,

$$W^\perp\ni w'=\lambda_1\boldsymbol{b}_1+\cdots+\lambda_{n-k}\boldsymbol{b}_{n-k}=\begin{pmatrix}\lambda_1b_{11}+\cdots+\lambda_{n-k}b_{1,n-k}\\ \vdots\\ \lambda_1b_{n1}+\cdots+\lambda_{n-k}b_{n,n-k}\end{pmatrix}$$

と書ける. $^{\exists}w' \neq 0$ s.t. $|w'| = d_{C^\perp} \leq k$. このとき w' の少なくとも $n-k$ 個の成分は 0. 簡単のため, 最初の $n-k$ 座標が 0 とすると

$$\begin{cases} \lambda_1 b_{11} + \cdots + \lambda_{n-k} b_{1,n-k} = 0 \\ \vdots \\ \lambda_1 b_{n-k,1} + \cdots + \lambda_{n-k} b_{n-k,n-k} = 0 \end{cases}$$

$n-k$ 小行列 $(b_{ij})_{1 \leq i,j \leq n-k}$ の行列式は 0 ではないから正則. よって $\lambda_1 = \cdots = \lambda_{n-k} = 0$ で $w' = 0$ となり矛盾. したがって $d_{C^\perp} = k+1$ である.

MDS コードの例を構成する.

$$\mathbf{F}_q[X]_k := \{f(X) \in \mathbf{F}_q[X] \ : \ \deg f(X) \leq k-1\}$$

とおく. これは次元 k の $\mathbf{F}_q$ ベクトル空間である.

定義 $1 \leq k < n < q$ とする. $\mathbf{F}_q$ の部分集合 $\Lambda = \{\lambda_1, \cdots, \lambda_n\}$ と $\xi = {}^t(\xi_1, \cdots, \xi_n) \in \mathbf{F}_q^n$, $|\xi| = n$ を固定して, 線形写像

$$T = T_{\Lambda,\xi}^{(k)} \ : \ \mathbf{F}_q[X]_k \longrightarrow \mathbf{F}_q^n \ : \ T(f(X)) = (\xi_1 f(\lambda_1), \cdots, \xi_n f(\lambda_n))$$

を定義する. T は単射であるから, $\dim \mathrm{Im}T = k$. このとき $C = (\mathbf{F}_q^n, \mathrm{Im}T)$ で定まる $[n,k]_q$ コードを**一般 Reed–Solomon コード**という. $C = \mathrm{GRS}_k(\Lambda, \xi)$ と表す.

命題 26 $\mathrm{GRS}_k(\Lambda, \xi)$ は MDS コードである.

証明 $f(X) \in \mathbf{F}_q[X]_k$ の根は高々 $k-1$ 個である. よって $T(f(X))$ の成分で 0 となるのは高々 $k-1$ 個. 即ち $|T(f(X))| \geq n-k+1$. ゆえに $d_{\mathrm{GRS}_k(\Lambda,\xi)} \geq n-k+1$.

命題 27 Λ, ξ に対し, $^{\exists}\eta \in \mathbf{F}_q^n$, $|\eta| = n$ で, $\mathrm{GRS}_k(\Lambda, \xi)^\perp = \mathrm{GRS}_{n-k}(\Lambda, \eta)$ $(k = 1, \cdots, n-1)$ となる.

証明 $\mathrm{GRS}_{n-1}(\Lambda, \xi) = (\mathbf{F}_q^n, W)$ とする. $\mathrm{GRS}_{n-1}(\Lambda, \xi)$ は $[n, n-1, 2]_q$ MDS コードだから, 命題 24 より $\mathrm{GRS}_{n-1}(\Lambda, \xi)^\perp$ は $[n, 1, n]_q$ MDS コードである. $\dim W^\perp = 1$ で $0 \neq \eta \in W^\perp$ をとれば, $|\eta| = n$. $\eta \in W^\perp$ より

$$0 = (\eta, T(f(X))) = \eta_1 \xi_1 f(\lambda_1) + \cdots + \eta_n \xi_n f(\lambda_n) \qquad ({}^\forall f(X) \in \mathbf{F}_q[X]_{n-1})$$

とくに $^\forall g(X) \in \mathbf{F}_q[X]_{n-k}, {}^\forall h(X) \in \mathbf{F}_q[X]_k$ に対し, $g(X)h(X) \in \mathbf{F}_q[X]_{n-1}$ だから

$$0 = \eta_1 \xi_1 g(\lambda_1) h(\lambda_1) + \cdots + \eta_n \xi_n g(\lambda_1) h(\lambda_1) = (T_{\Lambda,\eta}^{(n-k)}(g(X)), T_{\Lambda,\xi}^{(k)}(h(X)))$$

即ち, $\mathrm{Im}T_{\Lambda,\eta}^{(n-k)} \subset (\mathrm{Im}T_{\Lambda,\xi}^{(k)})^\perp$. 次元が同じなので, $\mathrm{Im}T_{\Lambda,\eta}^{(n-k)} = (\mathrm{Im}T_{\Lambda,\xi}^{(k)})^\perp$.

Reed–Solomon 符号による符号化と生成行列

有限体 $\mathbf{F}_q$ の部分集合 $\Lambda = \{\lambda_1, \cdots, \lambda_n\} \subset \mathbf{F}_q$ を固定する. $\mathbf{1} = {}^t(1, 1, \cdots, 1) \in \mathbf{F}_q^n$ として, Reed–Solomon 符号 $C = \mathrm{GRS}_k(\Lambda, \mathbf{1}) = (\mathbf{F}_q^n, W)$ を考える.

$$T : \mathbf{F}_q[X]_k \longrightarrow \mathbf{F}_q^n \ : \ f(X) \mapsto {}^t(f(\lambda_1), \cdots, f(\lambda_n))$$

とすれば, $W = \mathrm{Im}T$ である. $\mathbf{F}_q[X]_k$ の $\mathbf{F}_q$ ベクトル空間としての基底は $1, X, X^2, \cdots, X^{k-1}$ である. T は単射線形写像であるから, $T(1), T(X), T(X^2), \cdots, T(X^{k-1})$ が W の基底になる. よって, $\mathrm{GRS}_k(\Lambda, \mathbf{1})$ の生成行列は

$$A = (T(1), T(X), \cdots, T(X^{k-1})) = \begin{pmatrix} 1 & \lambda_1 & \cdots & \lambda_1^{k-1} \\ 1 & \lambda_2 & \cdots & \lambda_2^{k-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \lambda_n & \cdots & \lambda_n^{k-1} \end{pmatrix}$$

となる.

k ビットのメッセージ $M = \{c_0, c_1, \cdots, c_{k-1}\}$ が与えられたとき, 多項式

$$f_M(X) = c_0 + c_1 X + \cdots + c_{k-1} X^{k-1}$$

からコードワード

$$w_M = T(f_M(X)) = A \begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_{k-1} \end{pmatrix}$$

ができる.

逆に, コードワード $w = (w_1, \cdots, w_n) \in W$ が与えられたとき, $T(f(X)) = w$ となる $f(X) \in \mathbf{F}_q[X]_k$ の係数は, 連立 1 次方程式

$$A \begin{pmatrix} x_0 \\ x_1 \\ \vdots \\ x_{k-1} \end{pmatrix} = \begin{pmatrix} w_1 \\ w_2 \\ \vdots \\ w_n \end{pmatrix}$$

の唯一つの解として定まるので, メッセージは $\{x_0, x_1, \cdots, x_{k-1}\}$ で復元される.

Reed–Solomon 符号のエラー訂正復号

$C = \mathrm{GRS}_k(\Lambda, \mathbf{1}) = (\mathbf{F}_q^n, W)$ の最小距離は $d_C = n - k + 1$ である. $t = [(d_C - 1)/2] = [(n-k)/2]$ とおく. $w \in W$ を送信語として, 受信語を $z = w + e = {}^t(z_1, \cdots, z_n)$ とする.

命題 28 z に対し, 恒等的に 0 でない 2 変数多項式 $Q(X, Y) = Q_0(X) + Q_1(X)Y \in \mathbf{F}_q[X, Y]$ で次をみたすものが少なくとも 1 つ存在する.

- $Q(\lambda_i, z_i) = 0 \quad (i = 1, \cdots, n)$
- $\deg Q_0(X) \leq n - t - 1, \ \deg Q_1(X) \leq n - k - t$

証明　$\ell = n-t-1$, $m = n-k-t$ とおいて,

$$Q_0(X) = \sum_{i=0}^{\ell} \alpha_i X^i, \qquad Q_1(X) = \sum_{i=0}^{m} \beta_i X^i$$

とおく. 最初の条件は

$$(\sharp) \qquad \begin{pmatrix} 1 & \lambda_1 & \lambda_1^2 & \cdots & \lambda_1^\ell & z_1 & z_1\lambda_1 & z_1\lambda_1^2 & \cdots & z_1\lambda_1^m \\ 1 & \lambda_2 & \lambda_2^2 & \cdots & \lambda_2^\ell & z_2 & z_2\lambda_2 & z_2\lambda_2^2 & \cdots & z_2\lambda_2^m \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \lambda_n & \lambda_n^2 & \cdots & \lambda_n^\ell & z_n & z_n\lambda_n & z_n\lambda_n^2 & \cdots & z_n\lambda_n^m \end{pmatrix} \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_\ell \\ \beta_0 \\ \beta_1 \\ \vdots \\ \beta_m \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

と表される. これを α_i, β_j の連立 1 次方程式とみると, 係数行列 B は $n \times (\ell+1+m+1)$ 行列であり,

$$(\ell+1+m+1) - \mathrm{rank} B \geq (n+1) - n = 1$$

をみたすから, 必ず非自明解をもつ.

命題 29　$w = T(f(X))$ $(f(X) \in \mathbf{F}_q[X]_k)$ とする. $|e| \leq t$ ならば,

$$f(X) = -\frac{Q_0(X)}{Q_1(X)}$$

となる.

証明　$z_i = f(\lambda_i) + e_i$ で, $Q(X,Y)$ の性質から, $Q(\lambda_i, f(\lambda_i)+e_i) = 0$. とくに, $e_i = 0$ のとき λ_i は $Q(X, f(X))$ の根となる. $|e| \leq t$ より $e_i = 0$ となる i は $n-t$ 個以上あるが, $\deg Q(X, f(X)) \leq n-t-1$ なので, 根の個数が次数よりも大きい. よって $Q(X, f(X)) = 0(X)$ である.

この補題から, $f(X)$ が復元でき, z のエラー訂正ができる. また

$$Q(X,Y) = Q_1(X)\left(Y + \frac{Q_0(X)}{Q_1(X)}\right) = Q_1(X)(Y - f(X))$$

となり

$$0 = Q(\lambda_i, f(\lambda_i)+e_i) = Q_1(\lambda_i)e_i$$

から

$$e_i \neq 0 \iff Q_1(\lambda_i) = 0$$

したがって, エラーのある位置 i は $Q_1(\lambda_i) = 0$ となる i であることがわかる.

8　巡回コード

行列 $\sigma \in M_n(\mathbf{F}_q)$ を

$$\sigma := \begin{pmatrix} 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix}, \qquad \sigma \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} a_n \\ a_1 \\ \vdots \\ a_{n-1} \end{pmatrix}$$

とする.

定義　コード $C = (\mathbf{F}_q^n, W)$ が $\sigma(W) = W$ をみたすとき, **巡回コード**という.

巡回コードは多項式で分類できる.
$\mathbf{F}_q[X]$ において, $I \subset \mathbf{F}_q[X]$ がイデアルとは

1. $\varphi(X), \psi(X) \in I \implies \varphi(X) + \psi(X) \in I$
2. $\varphi(X) \in I \implies h(X)\varphi(X) \in I \quad ({}^{\forall}h(X) \in \mathbf{F}_q[X])$

をみたすことであった.

補題 2　$I \subset \mathbf{F}_q[X]$ が 条件 1 をみたすとする. このとき

$$I \text{ がイデアル} \iff \text{「}\varphi(X) \in I \implies (aX+b)\varphi(X) \in I \quad ({}^{\forall}a, b \in \mathbf{F}_q)\text{」}$$

証明　($\Longrightarrow$) は条件 2 より自明. ($\Longleftarrow$) を示す. 仮定より

$$\varphi(X) \in I \implies X\varphi(X) \in I \implies X^m\varphi(X) \in I \implies aX^m\varphi(X) \in I$$

これと条件 1 から条件 2 が従う.

$v = {}^t(a_1, \cdots, a_n) \in \mathbf{F}_q^n$ に対し

$$f_v(X) = a_1 + a_2X + \cdots + a_nX^{n-1} \in \mathbf{F}_q[X]$$

とおく.

補題 3　$v, w \in \mathbf{F}_q^n$, $\lambda, \mu \in \mathbf{F}_q$ に対し

- $f_{\lambda v + \mu w}(X) = \lambda f_v(X) + \mu f_w(X)$
- $Xf_v(X) = f_{\sigma(v)}(X) + a_n(X^n - 1)$

証明　証明は容易.

$\Phi_n(X) = X^n - 1$ とおく.
$C = (\mathbf{F}_q^n, W)$ をコードとするとき, $I_C \subset \mathbf{F}_q[X]$ を

$$I_C := \{f_w(X) + h(X)\Phi_n(X) \ : \ w \in W,\ h(X) \in \mathbf{F}_q[X]\}$$

と定義する. $f_0(X) = 0(X)$ だから, I_C は $h(X)\Phi_n(X)$ の形の多項式をすべて含む. 即ち $(\Phi_n(X)) \subset I_C$. また I_C は条件 1

1. $\varphi(X), \psi(X) \in I_C \implies \varphi(X) + \psi(X) \in I_C$

をみたす.

定理 5 C が巡回コード $\iff I_C$ がイデアル

証明 $(\Longrightarrow)$ 補題 2 より

$$\varphi \in I_C \implies (aX + b)\varphi(X) \in I_C \quad ({}^{\forall}a, b \in \mathbf{F}_q)$$

を示せばよい. $\varphi(X) = f_w(X) + h(X)\Phi_n(X)$ とすると, 補題 3 より

$$\begin{aligned}(aX + b)\varphi(X) &= aXf_w(X) + bf_w(X) + (aX + b)h(X)\Phi_n(X) \\ &= f_{a\sigma(w)+bw}(X) + \{a_n + (aX + b)h(X)\}\Phi_n(X)\end{aligned}$$

となり, C は巡回コードだから $a\sigma(w) + bw \in W$. よって $(aX + b)\varphi(X) \in I_C$ となる.
$(\Longleftarrow)$ I_C がイデアルとする. 定義より

$$W \longleftrightarrow \{f_w(X)\}_{w \in W} = I_C \text{ の中の } \deg \leq n - 1 \text{ の多項式全体}$$

である. イデアルの条件から $f_w(X) \in I_C$ に対し, $Xf_w(X) - a_n\Phi_n(X) \in I_C$ だから

$$Xf_w(X) - a_n\Phi_n(X) = f_{\sigma(w)}(X) \in I_C$$

で, $\deg f_{\sigma(w)}(X) \leq n - 1$ だから, 上の対応により $\sigma(w) \in W$ である. よって $\sigma(W) \subset W$.

定義 $\Phi_n(X)$ に対し, $g(X) \in \mathbf{F}_q[X]$ $(\deg g(X) \geq 1)$ で

$$g(X) \mid \Phi_n(X) \quad \text{かつ} \quad g(X) \text{ の最高次の係数は } 1$$

となる $g(X)$ を $\Phi_n(X)$ の**モニック因子**とよぶ.

補題 4 $g(X)$ が $\Phi_n(X)$ のモニック因子ならば, $(\Phi_n(X)) \subset (g(X))$ である. 逆に $I \subset \mathbf{F}_q[X]$ がイデアルで $I \neq \mathbf{F}_q[X]$ ならば, モニック因子 $g(X)$ で $I = (g(X))$ となるものが唯一つ存在する.

証明 命題 6 より明らか.

定義 C が巡回コードならば, I_C はイデアルかつ $(\Phi_n(X)) \subset I_C$ だから, 補題 4 により $I_C = (g_C(X))$ となる $\Phi_n(X)$ のモニック因子 $g_C(X)$ が唯一つ定まる. これを C の**生成多項式**という. また $h_C(X) = \Phi_n(X)/g_C(X) \in \mathbf{F}_q[X]$ で定まる多項式を C の**検査多項式**という.

逆に $\Phi_n(X)$ のモニック因子 $g(X)$ から, 巡回コード $C_{g(X)}$ が次のように構成される.
イデアル $J = (g(X))$ から

$$J^{n-1} := \{f(X) \in (g(X)) \ : \ \deg f(X) \leq n-1\}$$

とおく. $f(X) \in J^{n-1}$ を

$$f(X) = a_0 + a_1 X + \cdots + a_{n-1}X^{n-1}$$

とするとき, ベクトル $u_f \in \mathbf{F}_q^n$ を

$$u_{f(X)} := {}^t(a_0, a_1, \cdots, a_{n-1})$$

で定義する.

命題 30 $W := \{u_{f(X)} \ : \ f(X) \in J^{n-1}\}$ は部分空間となり, $C_{g(X)} := (\mathbf{F}_q^n, W)$ は巡回コードとなる.

証明 証明は容易.

以上をまとめると

定理 6 対応 $C \mapsto g_C(X)$, $g(X) \mapsto C_{g(X)}$ により, $\mathbf{F}_q$ 上の長さ n の巡回コードと $\Phi_n(X)$ のモニック因子は 1 対 1 に対応する.

命題 31 $C = (\mathbf{F}_q^n, W)$ を巡回コードとして,

$$g_C(X) = g_0 + g_1 X + \cdots + g_m X^m$$

とする.

1. $k = \dim W = n - \deg g_C(X) = \deg h_C(X)$
2. C の 1 つの生成行列 A_C として

$$ {}^t A_C = \begin{pmatrix} g_0 & g_1 & \cdots & g_{m-1} & g_m & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & g_{m-1} & g_m & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \cdots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & g_0 & g_1 & \cdots & g_{m-1} & g_m \end{pmatrix} \in M_{n,k}(\mathbf{F}_q)$$

   が取れる.

3. 双対コード $C^\perp$ も巡回コードで, その生成多項式は $g_{C^\perp}(X) = h_C(0)^{-1}X^k h_C(X^{-1})$ となる.

証明 $g(X) = g_C(X)$ とすれば, $C = C_{g(X)}$ であるから, $C_{g(X)}$ の構成を使って計算すればよい.

例 24 命題 17 より, $\mathbf{F}_q^\times = \{1, \alpha, \cdots, \alpha^{q-2}\}$ となる原始元 α が取れる. 定理 3 から, $\Phi_{q-1}(X) = X^{q-1} - 1$ は

$$\Phi_{q-1}(X) = (X-1)(X-\alpha)\cdots(X-\alpha^{q-2})$$

と因数分解する. よって

$$g(X) = (X-1)(X-\alpha)\cdots(X-\alpha^{m-1})$$

は $\Phi_{q-1}(X)$ のモニック因子であるから, 巡回コード $C_{g(X)}$ ができる. これは $[q-1, q-m-1]_q$ コードである. この $C_{g(X)}$ が **Reed–Solomon コード**である. 簡単な計算で

$$C_{g(X)}^\perp = \mathrm{GRS}_m(\Lambda_0, \xi_0), \qquad \Lambda_0 = \mathbf{F}_q^\times,\ \xi_0 = {}^t(1, 1, \cdots, 1)$$

が解る. これから $C_{g(X)} = \mathrm{GRS}_{q-m-1}(\Lambda_0, \xi_0)$ となる.

実験数学３
A 多項式の操作

A1. $\mathbf{Z}[X]$ の多項式の p を法とする剰余

p を素数として, $\mathbf{F}_p = \mathbf{Z}/(p)$ を標数 p の素体とする. 以下, $\mathbf{F}_p = \{0, 1, 2, \cdots, p-1\}$ と同一視する. 整数係数の多項式

$$f(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 \in \mathbf{Z}[X]$$

に対し,

$$f(X) \mod p = \overline{a}_n X^n + \overline{a}_{n-1} X^{n-1} + \cdots + \overline{a}_1 X + \overline{a}_0 \in \mathbf{F}_p[X]$$

と定める. **Mathematica** では **PolynomialMod**$[f, p]$ により $f(X) \mod p$ が計算できる.

PolynomialMod[$-113 * X\text{^}4 + 71 * X\text{^}3 + 92 * X\text{^}2 - 26, 3$**]**

$1 + 2X^2 + 2X^3 + X^4$

A2. $\mathbf{Z}[X]$ と $\mathbf{F}_p[X]$ の多項式の既約分解

$\mathbf{Z}[X]$ の多項式の既約分解をするには, **Factor** を使う.

Factor[$X\text{^}12 - 1$**]**

$(-1 + X)(1 + X)\left(1 + X^2\right)\left(1 - X + X^2\right)\left(1 + X + X^2\right)\left(1 - X^2 + X^4\right)$

$\mathbf{F}_p[X]$ での多項式の既約分解には, **Factor** のオプション **Modulus** $\rightarrow p$ を用いる.

Factor[$X\text{^}12 - 1$**, Modulus** $\rightarrow 3$**]**

$(1 + X)^3 (2 + X)^3 \left(1 + X^2\right)^3$

Factor[$X\text{^}12 - 1$**, Modulus** $\rightarrow 5$**]**

$(1+X)(2+X)(3+X)(4+X)\left(1 + X + X^2\right)\left(4 + 2X + X^2\right)\left(4 + 3X + X^2\right)\left(1 + 4X + X^2\right)$

A3. $\mathbf{F}_p[X]$ の n 次多項式のリスト

$\mathbf{F}_p[X]$ の中の次数 n のモニック多項式 (X^n の係数が 1 の多項式) 全体の集合を構成する. n 次多項式の係数は $\mathbf{F}_p^{n+1}$ の要素とみなせる. 即ち

$$a_0 + a_1 X + \cdots + a_n X^n \longleftrightarrow {}^t(a_0, a_1, \cdots, a_n)$$

モニックならば $a_n = 1$ である. よって, まず次元の一つ小さい $\mathbf{F}_p^n$ のリストを作り, その各ベクトルの最後に成分 1 を付け加えたベクトルのリストを作る. このリストのベクトルから対応する多項式を構成すれば, n 次モニック多項式全体が得られる.

例 1 $\mathbf{F}_2[X]$ の 4 次モニック多項式のリストを作る. まず $\mathbf{F}_2^4$ を **Tuples** で与える. **Tuples[list,** k**]** は **list** の要素を成分とする k 次元ベクトル全体のリストを生成する.

F2L4 = Tuples[$\{0, 1\}, 4$**]**

$\{\{0,0,0,0\},\{0,0,0,1\},\{0,0,1,0\},\{0,0,1,1\},\{0,1,0,0\},\{0,1,0,1\},\{0,1,1,0\},\{0,1,1,1\},$
$\{1,0,0,0\},\{1,0,0,1\},\{1,0,1,0\},\{1,0,1,1\},\{1,1,0,0\},\{1,1,0,1\},\{1,1,1,0\},\{1,1,1,1\}\}$

各ベクトルの最後に 1 を付け加える.

F2M5 = Append[#, 1]&/@F2L4

$\{\{0,0,0,0,1\},\{0,0,0,1,1\},\{0,0,1,0,1\},\{0,0,1,1,1\},\{0,1,0,0,1\},\{0,1,0,1,1\},\{0,1,1,0,1\},$
$\{0,1,1,1,1\},\{1,0,0,0,1\},\{1,0,0,1,1\},\{1,0,1,0,1\},\{1,0,1,1,1\},\{1,1,0,0,1\},$
$\{1,1,0,1,1\},\{1,1,1,0,1\},\{1,1,1,1,1\}\}$

このリストのベクトルから 4 次多項式を構成する.

F2P4 = Sum[#[[i]] * X^(i − 1), {i, 1, 5}]&/@F2M5

$\{X^4, X^3+X^4, X^2+X^4, X^2+X^3+X^4, X+X^4, X+X^3+X^4, X+X^2+X^4,$
$X+X^2+X^3+X^4, 1+X^4, 1+X^3+X^4, 1+X^2+X^4, 1+X^2+X^3+X^4, 1+X+X^4,$
$1+X+X^3+X^4, 1+X+X^2+X^4, 1+X+X^2+X^3+X^4\}$

Length[F2P4]

16

問題 1 上で構成した, $\mathbf{F}_2$ 上の 4 次モニック多項式のリスト **F2P4** から既約な多項式だけを取り出したい. そのプログラムを考えよ.

Select[F2P4,
Discriminant[#, X, Modulus → 2]!=0 &&Length[FactorList[#, Modulus → 2]] < 3&]

$\{1+X^3+X^4, 1+X+X^4, 1+X+X^2+X^3+X^4\}$

問題 2 $\mathbf{F}_p$ 上の n 次既約モニック多項式の個数を求める関数 **PN[p,n]** のプログラムを与えよ. $p = 3$ の場合に, $(n,$ **PN[3,n]**$)$ を $n = 1, \cdots, 10$ で計算し, 結果をプロットせよ.

```
PN[p_, n_]:=
Length[
Select[Sum[#[[i]] * X^{i − 1}, {i, 1, n + 1}]&/@
(Append[#, 1]&/@Tuples[Table[i, {i, 0, p − 1}], n]),
Discriminant[#, X, Modulus → p] ≠ 0&&
Length[FactorList[#, Modulus → p]] < 3&]]
Table[{i, PN[3, i]}, {i, 1, 10}]
```

$\{\{1,3\},\{2,3\},\{3,8\},\{4,18\},\{5,48\},\{6,116\},\{7,312\},\{8,810\},\{9,2184\},\{10,5880\}\}$

ListPlot[Table[{i, PN[3, i]}, {i, 1, 10}], Joined → True]

研究課題 I p を素数, $1 \leq n \in \mathbf{Z}$ とするとき, $\mathbf{F}_p$ 上の既約モニック n 次多項式の個数を与える公式を見つけよ.

$$\frac{1}{n}\sum_{d|n}\mu(d)p^{n/d}, \qquad \mu(d) = \begin{cases} (-1)^k & (d \text{ is square free and a product of } k\text{-primes}) \\ 0 & (d \text{ is not square free}) \end{cases}$$

B 有限体の操作

B1. 有限体の要素の表記方法

p を素数として, p のべき $q = p^n$ を固定する. このとき q 個の元をもつ有限体 $\mathbf{F}_q$ が存在する. 以下では, $\mathbf{F}_q$ の要素がどのように表示されるかについて説明する.

(I) ベクトルまたは多項式表示

$m(X)$ を $\mathbf{F}_p[X]$ の n 次既約多項式でモニック (X^n の係数が 1) とする. $m(X)$ の 1 つの根を α とすれば, $\mathbf{F}_q = \mathbf{F}_p(\alpha)$ であった (命題 14). 任意の要素 $a \in \mathbf{F}_q$ は

$$a = a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{n-1}\alpha^{n-1}, \qquad (a_0, \cdots, a_{n-1} \in \mathbf{F}_p = \{0, 1, \cdots, p-1\})$$

と一意に表される. このとき, 要素 a を

$$a = \{a_0, a_1, \cdots, a_{n-1}\} \in \mathbf{F}_p^n$$

とベクトルで表示する. または

$$\{a_0, a_1, \cdots, a_{n-1}\} \longleftrightarrow g_a(X) = a_0 + a_1X + \cdots + a_{n-1}X^{n-1} \in \mathbf{F}_p[X]$$

のように多項式を対応させて, 多項式の形で表示する. $a = g_a(\alpha)$ である. この表記方法は $m(X)$ から一意に定まる. これは多項式環の言葉で言い直せば, イデアル $(m(X))$ による剰余環 $\mathbf{F}_p[X]/(m(X))$ と $\mathbf{F}_q$ の間の同型対応

$$\mathbf{F}_p[X]/(m(X)) \longrightarrow \mathbf{F}_q \ : \ g(X) \mod m(X) \mapsto g(\alpha)$$

に他ならない.

ベクトル表示では, 和の計算は成分ごとに行えばよいが, 積の計算は簡単ではない. $a, b \in \mathbf{F}_q$ に対応する多項式 $g_a(X)$ と $g_b(X)$ の積を $m(X)$ で割り

$$g_a(X)g_b(X) = q(X)m(X) + r(X), \qquad (q(X), r(X) \in \mathbf{F}_p[X])$$

とする. $X = \alpha$ とすれば, $ab = g_a(\alpha)g_b(\alpha) = r(\alpha)$ であるから, $r(X)$ が積 ab に対応する多項式, 即ち $r(X) = g_{ab}(X)$ となる.

(II) 原始元のべき表示

$\mathbf{F}_q$ の原始元 β を固定する. 即ち, $\mathbf{F}_q = \{0, 1, \beta, \beta^2, \cdots, \beta^{q-2}\}$ である. よって, 任意の $a \neq 0$ は, β の適当なべきで $a = \beta^k$ と表される. この表示方法では, $\mathbf{F}_q$ の積の計算は簡単になるが, 和の計算は難しくなる. 一般に $m(X)$ の根 α は原始元になるとは限らないので, 最初に固定する原始元 β は, 何らかの方法で見つけておく必要がある.

B2. Mathmatica の有限体パッケージ

Mathematica で有限体を扱うには, まず有限体パッケージ **FiniteFields** を読み込む.

```
<< FiniteFields`
```

$\mathbf{F}_q$ $(q = p^n)$ は $\mathbf{GF}[p, n]$ で与えられる. 例えば $q = 3^4$ の体は

```
GF[3,4]
```

GF[3, {2, 1, 0, 0, 1}]

となる. ここでリスト $\{2,1,0,0,1\}$ は体の記述に使用される既約モニック多項式が, $m(X) = 2 + X + X^4 \in \mathbf{F}_3[X]$ で与えられていることを意味する. デフォルトでは **Mathemtaica** が自動的に $m(X)$ を設定するが, **GF[*p*, 既約多項式の係数のリスト]** の形式で明示的に指定することも可能である. $m(X)$ は **FieldIrreducible** で確認できる.

FieldIrreducible[GF[3, 4], *X*]
$2 + X + X^4$

体の標数は **Characteristic**, 要素の個数は **FieldSize** で確認できる.

Characteristic[GF[3, 4]]
3
FieldSize[GF[3, 4]]
81

体の要素は $m(X)$ を法とする多項式またはベクトルで表記できるが, その入力は n が大きくなると簡便ではない. 体の要素を適当な順番に並べて, $a[0], a[1], a[2], a[3], \cdots$ の形に表示する方法がある. そのために **SetFieldFormat** を用いる.

SetFieldFormat[GF[3, 4], FormatType → FunctionOfCode[*a*]]

これにより, $\mathbf{F}_{81}$ の要素を $a[i]$ の形で記述できる. 各 $a[i]$ が実際にどの要素を現しているのかを見るには **FullForm** を使う. 例えば 73 番目の要素 $a[73]$ は

FullForm[*a*[73]]
$\mathrm{GF}[3, \mathrm{List}[2, 1, 0, 0, 1]][\mathrm{List}[1, 0, 2, 2]]$

となる. これは $m(X) = 2 + X + X^4$ としたときのベクトル表示が $\{1, 0, 2, 2\}$ の要素, 多項式表示では $g_{a[73]}(X) = 1 + 2X^2 + 2X^3$ であることを意味する. 同様に最初の 3 個は $\mathbf{F}_3$ の要素 $a[0] = 0, a[1] = 1, a[2] = \{2, 0, 0, 0\}$ になることも確認できる. $a[i]$ の形で和と積が計算できる. $a[6]$ と $a[13]$ の和と積を計算してみる. これらは

FullForm[*a*[6]]
$\mathrm{GF}[3, \mathrm{List}[2, 1, 0, 0, 1]][\mathrm{List}[0, 2, 0, 0]]$
FullForm[*a*[13]]
$\mathrm{GF}[3, \mathrm{List}[2, 1, 0, 0, 1]][\mathrm{List}[1, 1, 1, 0]]$

から $a[6] = \{0, 2, 0, 0\}, a[13] = \{1, 1, 1, 0\}$ である.

***a*[6] + *a*[13]**
$a[10]$
FullForm[*a*[10]]
$\mathrm{GF}[3, \mathrm{List}[2, 1, 0, 0, 1]][\mathrm{List}[1, 0, 1, 0]]$

となり, $a[6] + a[13] = a[10] = \{1, 0, 1, 0\}$ となる. 即ち $\{0, 2, 0, 0\} + \{1, 1, 1, 0\} = \{1, 0, 1, 0\}$ である ($3 = 0$ に注意). 積は

a[6] * a[13]
$a[78]$
FullForm[a[78]]
$\mathrm{GF}[3, \mathrm{List}[2, 1, 0, 0, 1]][\mathrm{List}[0, 2, 2, 2]]$

となる.

体の要素の原始元べき乗表記をするためには, **PowerListQ** を **True** にしておく.

PowerListQ[GF[3, 4]] = True

$a[3] = \{0, 1, 0, 0\}$ が原始元で, $\mathbf{F}_{81}^{\times} = \{1 = a[3]^0, a[3]^1, a[3]^2, \cdots, a[3]^{79}\}$ となる. このリストが **PowerList** で得られる.

PowerList[GF[3, 4]]
$\{\{1, 0, 0, 0\}, \{0, 1, 0, 0\}, \{0, 0, 1, 0\}, \{0, 0, 0, 1\}, \{1, 2, 0, 0\}, \{0, 1, 2, 0\}, \{0, 0, 1, 2\}, \cdots\}$

各 $a[i]$ が $a[3]$ の何乗かを確認するためには, **FieldInd** を使う. 例えば $a[51]$ では

FieldInd[a[51]]
35

となるので, $a[51] = a[3]^{35}$ である.

B3. 原始元の計算

有限体 $\mathbf{F}_q$ の原始元をすべて求めるアルゴリズムを考える. β を 1 つの原始元とすれば, $\mathbf{F}_q^{\times} = \{1, \beta, \beta^2, \cdots, \beta^{q-2}\}$ である. 群論の簡単な議論から, β^k が原始元であるためには, k が $q-1$ と互いに素になることが必要十分である. よって $\gcd(k, q-1) = 1$ となるすべての $1 \le k \le q-2$ について, β^k をリストアップすればよい.
$\mathbf{F}_{81}$ の原始元をすべて求めるには次のようにすればよい. $1 \le k \le 79$ で, 80 と素になるもののリストを作りそれを L とおく.

L = Select[Table[k, {k, 1, FieldSize[GF[3, 4]] − 2}], GCD[#, FieldSize[GF[3, 4]] − 1] == 1&]
$\{1, 3, 7, 9, 11, 13, 17, 19, 21, 23, 27, 29, 31, 33, 37, 39, 41, 43, 47, 49,$
$51, 53, 57, 59, 61, 63, 67, 69, 71, 73, 77, 79\}$

L の要素 k に対し, $a[3]^k$ のリストを作る.

Function[k, FieldExp[GF[3, 4], k]]/@L
$\{a[3], a[27], a[32], a[39], a[46], a[8], a[11], a[25], a[68], a[31], a[48], a[53], a[71], a[58], a[80], a[56],$
$a[6], a[54], a[61], a[78], a[65], a[4], a[19], a[14], a[52], a[62], a[69], a[67], a[49], a[35], a[40], a[28]\}$

B4. 有限体上の行列の操作

$\mathbf{F}_q$ に成分をもつ行列の演算は **Mathematica** の通常のコマンドで計算可能である. $\mathbf{F}_{81}$ に成分をもつ行列 A を次で定義する.

A = {{a[3], a[37], a[21], a[74], a[52]},{a[40], a[41], a[79], a[6], a[15]},{a[22], a[68], a[40], a[33], a[2]}, {a[19], a[30], a[12], a[80], a[48]},{a[58], a[61], a[25], a[7], a[76]}}

$\{\{a[3], a[37], a[21], a[74], a[52]\}, \{a[40], a[41], a[79], a[6], a[15]\}, \{a[22], a[68], a[40], a[33], a[2]\}, \{a[19], a[30], a[12], a[80], a[48]\}, \{a[58], a[61], a[25], a[7], a[76]\}\}$

MatrixForm[A]

$$\begin{pmatrix} a[3] & a[37] & a[21] & a[74] & a[52] \\ a[40] & a[41] & a[79] & a[6] & a[15] \\ a[22] & a[68] & a[40] & a[33] & a[2] \\ a[19] & a[30] & a[12] & a[80] & a[48] \\ a[58] & a[61] & a[25] & a[7] & a[76] \end{pmatrix}$$

A の行列式と逆行列, およびランクを計算する.

Det[A]

$a[68]$

Inverse[A]//MatrixForm

$$\begin{pmatrix} a[60] & a[24] & a[15] & a[64] & a[25] \\ a[68] & a[28] & a[80] & a[24] & a[80] \\ a[18] & a[76] & a[46] & a[77] & a[43] \\ a[34] & a[1] & a[36] & a[67] & a[53] \\ a[80] & a[52] & a[67] & a[38] & a[56] \end{pmatrix}$$

MatrixRank[A]

5

B5. 有限体上の多項式環の操作についての注意

$\mathbf{F}_q$ を係数とする多項式環 $\mathbf{F}_q[X]$ の和, 積, 商, 剰余は通常の **Mathematica** のコマンドで計算可能であるが, 因数分解は q が素数の場合を除いてうまく機能しない. 次の例は $\mathbf{F}_{81}[X]$ の多項式 f と g の積, 及び g を f で割ったときの商と余りである.

f = a[1] * X^3 + a[20] * X + a[64]

$X^3 a[1] + a[64] + X a[20]$

g = a[6] * X^4 + a[15] * X^2 + a[50]

$X^4 a[6] + X^2 a[15] + a[50]$

Expand[f * g]

$X^5 a[36] + X^7 a[6] + a[42] + X^3 a[64] + X^4 a[58] + X a[29] + X^2 a[80]$

PolynomialQuotient[g, f, X]

$X a[6]$

PolynomialRemainder[g, f, X]

$X^2 a[66] + a[50] + X a[35]$

実験数学３
C 線形符号の最小距離

C1. 部分空間の構成

$\mathbf{F}_q$ を有限体として, ベクトル空間 $\mathbf{F}_q^n$ の k 次元部分空間を W とする. W の要素は q^k 個ある. W は有限集合なので, **Mathematica** のリストとして表示することが可能である. W の基底を $w_1, \cdots, w_k$ として, それを列ベクトルとする $n \times k$ 行列を $A = (w_1, \cdots, w_k)$ とする. A を線形写像

$$A : \mathbf{F}_q^k \longrightarrow \mathbf{F}_q^n \ : \ v \mapsto Av$$

と見れば, W はその像 $W = \mathrm{Im}A = A\mathbf{F}_q^k$ である. よって $\mathbf{F}_q^k$ をリスト表示しておき, それと A の積をとれば, W のリストが得られる.

例 1 $\mathbf{F}_4^5$ の３次元部分空間を記述する. $m(X) = X^2+X+1 \in \mathbf{F}_2[X]$ の根を α とすれば, $\mathbf{F}_4 = \mathbf{F}_2(\alpha) = \{0, 1, \alpha, 1+\alpha\}$ である. **FiniteFields** を使って $\mathbf{F}_4$ を定め, $\mathbf{F}_4 = \{a[0], a[1], a[2], a[3]\}$ と表す. $\alpha = a[2], 1+\alpha = a[3]$ である.

```
<< FiniteFields`
SetFieldFormat[GF[2, 2], FormatType → FunctionOfCode[a]]
FieldIrreducible[GF[2, 2], X]
```

$1 + X + X^2$

```
Table[FullForm[a[i]], {i, 0, 3}]
```

$\{0, \mathrm{GF}[2, \mathrm{List}[1, 1, 1]][\mathrm{List}[1, 0]], \mathrm{GF}[2, \mathrm{List}[1, 1, 1]][\mathrm{List}[0, 1]], \mathrm{GF}[2, \mathrm{List}[1, 1, 1]][\mathrm{List}[1, 1]]\}$

３次元空間 $\mathbf{F}_4^3$ の構成には **Tuples** を用いる.

```
L = Tuples[{a[0], a[1], a[2], a[3]}, 3];
```

L を表示すると長くなるので, セミコロン ; で表示しないようにしている. L の要素の個数は **Length** で確認できる.

```
Length[L]
```

64

W の基底を列とする行列 A を与える. ここでは

$$A = \begin{pmatrix} \alpha & 1 & 0 \\ \alpha & \alpha & 1 \\ \alpha & \alpha & \alpha \\ 0 & \alpha & \alpha \\ 1 & 0 & \alpha \end{pmatrix}$$

ととる.

```
A = {{a[2], a[1], 0}, {a[2], a[2], a[1]}, {a[2], a[2], a[2]}, {0, a[2], a[2]}, {a[1], 0, a[2]}}
```

$\{\{a[2], a[1], 0\}, \{a[2], a[2], a[1]\}, \{a[2], a[2], a[2]\}, \{0, a[2], a[2]\}, \{a[1], 0, a[2]\}\}$

```
MatrixForm[A]
```

$$\begin{pmatrix} a[2] & a[1] & 0 \\ a[2] & a[2] & a[1] \\ a[2] & a[2] & a[2] \\ 0 & a[2] & a[2] \\ a[1] & 0 & a[2] \end{pmatrix}$$

A と L の要素の積をとり, W を与える. これは **Map** を使う. **#** は L の要素を意味するパラメータであり, **&/@ *L*** で **#** が L の要素全体を動くことを意味する.

***W* = (*A*.#)&/@*L*;**

結果は表示しないようにしている.

例 2 $q = p$ が素数で, $\mathbf{F}_p$ が素体ならば, 有限体パッケージを使わない構成も可能である. $\mathbf{F}_3^6$ の中の 4 次元部分空間を構成する. $\mathbf{F}_3 = \{0, 1, 2\}$ として, $\mathbf{F}_3^4$ を **Tuples** で与える.

***L* = Tuples[{0, 1, 2}, 4];**
Length[*L*]
81

6×4 行列 A を次で与える.

***A* = {{0, 2, 1, 1}, {1, 0, 1, 1}, {2, 1, 0, 1}, {0, 2, 1, 0}, {1, 0, 2, 0}, {2, 1, 0, 0}}**
{{0, 2, 1, 1}, {1, 0, 1, 1}, {2, 1, 0, 1}, {0, 2, 1, 0}, {1, 0, 2, 0}, {2, 1, 0, 0}}
MatrixForm[*A*]

$$\begin{pmatrix} 0 & 2 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 2 & 1 & 0 & 1 \\ 0 & 2 & 1 & 0 \\ 1 & 0 & 2 & 0 \\ 2 & 1 & 0 & 0 \end{pmatrix}$$

例 1 と同様に **Map** で A と L の要素の積を計算し, **Mod** を用いて $\mod 3$ をとる.

W* = Mod[(*A*.#), 3]&/@*L
{{0, 0, 0, 0, 0, 0}, {1, 1, 1, 0, 0, 0}, {2, 2, 2, 0, 0, 0}, {1, 1, 0, 1, 2, 0}, {2, 2, 1, 1, 2, 0}, ⋯}

C2. 線形符号の最小距離の計算

線形符号 $C = (\mathbf{F}_q^n, W)$ が与えられたときに, その最小距離 d_C を計算する. 現在のところ, 一般の線形符号に対し最小距離を計算する多項式時間のアルゴリズムは存在せず, これは NP 問題と考えられている.

C の生成行列を A とする. A が与えられれば, W は C1 に述べた方法で記述できる. そこで

$$d_C = \min\{|w| \ : \ 0 \neq w \in W\}$$

を定義どおりに計算する. **Mathematica** には Hamming 距離 **HammingDistance** があるので, Hamming weight は $|w|$ = **HammingDistance[*w*, *o*]** で計算できる. ただし **o** は w と同じサイズのゼロベクトルである.

例 3 例 1 で構成した W について, 符号 $C = (\mathbf{F}_4^5, W)$ の最小距離を求める. まずゼロベクトルを **Table** で与える.

o = Table[0, {5}]
$\{0, 0, 0, 0, 0\}$

W からゼロベクトルを除く. これは **Complement** でできる.

Complement[W, {o}]
$\{\{0, 0, a[2], a[3], a[2]\}, \{0, 0, a[1], a[2], a[1]\}, \{0, 0, a[3], a[1], a[3]\}, \{0, a[2], 0, a[2], 0\},$
$\{0, a[2], a[2], a[1], a[2]\}, \{0, a[2], a[1], 0, a[1]\}, \cdots\}$

Map を使って各ベクトルの Hamming weight を計算する.

HammingDistance[#, o]&/@Complement[W, {o}]
$\{3, 3, 3, 2, 4, 3, 4, 2, 4, 4, 3, 2, 3, 4, 4, 3, 4, 4, 2, 4, 4, 5, 4, 3,$
$5, 5, 4, 4, 5, 4, 4, 3, 2, 4, 4, 4, 4, 5, 4, 4, 4, 4, 5, 3, 4, 5, 5, 3, 4, 2, 4, 3, 5, 4, 5, 4, 4, 4, 5, 4, 5, 4, 4\}$

その最小値を求める.

Min[%]
2

よって $d_C = 2$ である.

問題 C1 $\mathbf{F}_2$ 上で生成行列が次の A で与えられる $[15, 5]_2$ コード C の最小距離を求めよ.

$$A = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

A = Transpose[{{1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0},
{1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0},
{0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0},

```
{0,0,0,1,0,1,0,0,1,1,0,1,1,1,0},
{0,0,0,0,1,0,1,0,0,1,1,1,1,1,1}};
L = Tuples[{0,1},5];
Length[L]
```
32
```
W = Mod[(A.#),2]&/@L;
o = Table[0,{15}]
```
$\{0,0,0,0,0,0,0,0,0,0,0,0,0,0,0\}$
```
Min[HammingDistance[#,o]&/@Complement[W,{o}]]
```
5

問題 C2 p を素数とする. 問題 C1 で体を $\mathbf{F}_2$ から $\mathbf{F}_p$ に変えて, 同じ行列 A を生成行列とする $[15,5]_p$ コード C_p の最小距離を求めるプログラム **MD[p]** を作れ. また, それを用いて $p=3,5,7,11,13,17,19$ での最小距離を求めよ.

```
MD[p_]:=
Min[HammingDistance[#,Table[0,{15}]]&/@
Complement[Mod[(A.#),p]&/@Tuples[Table[i,{i,0,p-1}],5],
{Table[0,{15}]}]]
MD[3]
```
6
```
MD[5]
```
7
```
MD[7]
```
7
```
MD[11]
```
7
```
MD[13]
```
7
```
MD[17]
```
7
```
MD[19]
```
7

問題 C3 問題 C1 で体を $\mathbf{F}_2$ から $\mathbf{F}_9$ に変えて, 同じ行列 A で与えられる $[15,5]_9$ コード C_9 の最小距離を求めよ.

```
<< FiniteFields`
SetFieldFormat[GF[3,2],FormatType → FunctionOfCode[b]]
L9 = Tuples[{b[0],b[1],b[2],b[3],b[4],b[5],b[6],b[7],b[8]},5];
W9 = (A.#)&/@L9;
Min[HammingDistance[#,o]&/@Complement[W9,{o}]]
```
6

実験数学３
D 検査行列と weight enumerator
D1. 検査行列の計算

コード $C=(\mathbf{F}_q^n, W)$ の生成行列を A とする. W の双対空間は

$$W^{\perp}=\{v\in\mathbf{F}_q^n\ :\ {}^t w\cdot v=0\quad ({}^{\forall}w\in W)\}=\mathrm{Ker}\,{}^tA$$

で与えられる. そこで $\mathrm{Ker}\,{}^tA$ の基底 $u_1,\cdots,u_{n-k}$ を求めれば, $H_C={}^t(u_1,\cdots,u_{n-k})$ が C の検査行列となる.

Mathematica では, 線形写像の核の基底は **NullSpace** で求まる.

例 1 §C 例 3 のコード $C=(\mathbf{F}_4^5, W)$ の検査行列を求める. 行列 A の転置行列を **Transpose** で求める.

<< FiniteFields`

SetFieldFormat[GF[2, 2], FormatType → FunctionOfCode[a]]

A = {{a[2], a[1], 0}, {a[2], a[2], a[1]}, {a[2], a[2], a[2]}, {0, a[2], a[2]}, {a[1], 0, a[2]}}

$\{\{a[2],a[1],0\},\{a[2],a[2],a[1]\},\{a[2],a[2],a[2]\},\{0,a[2],a[2]\},\{a[1],0,a[2]\}\}$

MatrixForm[A]

$$\begin{pmatrix} a[2] & a[1] & 0 \\ a[2] & a[2] & a[1] \\ a[2] & a[2] & a[2] \\ 0 & a[2] & a[2] \\ a[1] & 0 & a[2] \end{pmatrix}$$

Transpose[A]

$\{\{a[2],a[2],a[2],0,a[1]\},\{a[1],a[2],a[2],a[2],0\},\{0,a[1],a[2],a[2],a[2]\}\}$

MatrixForm[Transpose[A]]

$$\begin{pmatrix} a[2] & a[2] & a[2] & 0 & a[1] \\ a[1] & a[2] & a[2] & a[2] & 0 \\ 0 & a[1] & a[2] & a[2] & a[2] \end{pmatrix}$$

核の基底はリストで与えられるので, それがそのまま検査行列であるとみなせる.

NullSpace[Transpose[A]]

$\{\{a[2],0,a[1],0,1\},\{a[3],a[1],a[2],1,0\}\}$

H = %//MatrixForm

$$\begin{pmatrix} a[2] & 0 & a[1] & 0 & 1 \\ a[3] & a[1] & a[2] & 1 & 0 \end{pmatrix}$$

ここで $1=a[1]$ である.

例 2 符号 $C=(\mathbf{F}_2^{16}, W)$ の検査行列が

$$H=\begin{pmatrix} 1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0 \\ 0&1&1&0&0&1&1&0&0&1&1&0&0&1&1&0 \\ 0&0&0&1&1&1&1&0&0&0&0&1&1&1&1&0 \\ 0&0&0&0&0&0&0&1&1&1&1&1&1&1&1&0 \\ 1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1 \end{pmatrix}$$

で与えられているときに, 最小距離 d_C を求める. 行列の成分の入力には, **PadRight**, **PadLeft**, **Table** などを使う. 例えば

PadRight[{1, 0}, 16, {1, 0}]
$\{1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0\}$
PadRight[{0, 1, 1, 0}, 16, {0, 1, 1, 0}]
$\{0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0\}$
Join[Table[0, {3}], Table[1, {4}], Table[0, {4}], Table[1, {4}], {0}]
$\{0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0\}$

となる. これらをまとめると,

***H* = {PadRight[{1, 0}, 16, {1, 0}],**
PadRight[{0, 1, 1, 0}, 16, {0, 1, 1, 0}],
Join[Table[0, {3}], Table[1, {4}], Table[0, {4}], Table[1, {4}], {0}],
Join[Table[0, {7}], Table[1, {8}], {0}],
Table[1, {16}]};
MatrixForm[*H*]

$$\begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

$W = \mathrm{Ker}H$ だから, W の生成行列 A は H の核の基底を列ベクトルとする行列となる. mod 2 で考えるために, **NullSpace** のオプション **Modulus** を使う.

NullSpace[*H*, Modulus → 2];
***A* = Transpose[%];**
MatrixForm[*A*]

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

$\dim_{\mathbf{F}_2} W = 11$ である. W を $W = A\mathbf{F}_2^{11}$ で記述する.

```
L = Tuples[{0, 1}, 11];
Length[L]
```
2048
```
W = Mod[A.#, 2]&/@L;
```

$\mathbf{F}_2^{16}$ のゼロベクトル $\boldsymbol{o}$ を与える.

```
o = Table[0, {16}]
```
$\{0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0\}$

§C 例 3 と同様に, d_C を計算する.

```
Min[HammingDistance[#, o]&/@Complement[W, {o}]]
```
4

よって $d_C = 4$ となる. C は $[16, 11, 4]_2$ コードである.

問題 D1 例 2 で与えられた符号 C の weight enumerator を求めよ.
```
HM = HammingDistance[#, o]&/@W;
Total[X^(#) * Y^(16 - #)&/@HM]
```
$X^{16} + 140X^{12}Y^4 + 448X^{10}Y^6 + 870X^8Y^8 + 448X^6Y^{10} + 140X^4Y^{12} + Y^{16}$

問題 D2 15×5 行列 A を

$$A = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

で与える. これは問題 C1 と同じ行列である. p を素数として, $\mathbf{F}_p$ 上生成行列 A をもつ $[15, 5]_p$ 符号を C_p とする. C_p の weight enumerator を与えるプログラム **WE[*p*]** を作り, **WE[2], WE[3], WE[5], WE[7]** を求めよ.

```
A = Transpose[{{1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0},
{1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0},
{0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0},
{0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0},
{0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1}}];
WE[p_]:=
Total[X^(#) * Y^(15 - #)&/@
(HammingDistance[#, Table[0, {15}]]&/@
(Mod[(A.#), p]&/@Tuples[Table[i, {i, 0, p - 1}], 5]))]
WE[2]
```

$X^{13}Y^2 + 6X^9Y^6 + 11X^8Y^7 + 8X^7Y^8 + 4X^6Y^9 + X^5Y^{10} + Y^{15}$

WE[3]

$4X^{14}Y + 12X^{13}Y^2 + 36X^{12}Y^3 + 50X^{11}Y^4 + 46X^{10}Y^5 + 42X^9Y^6 + 36X^8Y^7 + 14X^7Y^8 + 2X^6Y^9 + Y^{15}$

WE[5]

$96X^{15}+400X^{14}Y+696X^{13}Y^2+912X^{12}Y^3+580X^{11}Y^4+248X^{10}Y^5+100X^9Y^6+64X^8Y^7+28X^7Y^8 + Y^{15}$

WE[7]

$1506X^{15} + 4278X^{14}Y + 4968X^{13}Y^2 + 3648X^{12}Y^3 + 1656X^{11}Y^4 + 462X^{10}Y^5 + 150X^9Y^6 + 96X^8Y^7 + 42X^7Y^8 + Y^{15}$

WE[11]

$37030X^{15}+59810X^{14}Y+42040X^{13}Y^2+15320X^{12}Y^3+5280X^{11}Y^4+1090X^{10}Y^5+250X^9Y^6+160X^8Y^7 + 70X^7Y^8 + Y^{15}$

実験数学３
E Reed–Solomon コード

E1. Reed–Solomon コードのエラー訂正復号アルゴリズム

$\mathbf{F}_q$ の部分集合 $\Lambda = \{\lambda_1, \cdots, \lambda_n\} \subset \mathbf{F}_q$ を固定する. $\mathbf{1} = {}^t(1, 1, \cdots, 1) \in \mathbf{F}_q^n$ として, Reed–Solomon 符号 $C = \mathrm{GRS}_k(\Lambda, \mathbf{1}) = (\mathbf{F}_q^n, W)$ を考える. C の最小距離は $d_C = n - k + 1$ である. $w \in W$ を送信コードワードとして, 受信語を $z = w + e = {}^t(z_1, \cdots, z_n)$ とする. 命題 28 と命題 29 から, エラー訂正復号が次の手順で実行できる.

1. $t = [(d_C - 1)/2] = [(n-k)/2]$, $\ell = n - t - 1$, $m = n - k - t$ とおく.
2. $\Lambda = \{\lambda_1, \cdots, \lambda_n\}$ と受信語 z から, 次の連立 1 次方程式 (♯) の非自明解 $\alpha_0, \cdots, \alpha_\ell, \beta_0, \cdots, \beta_m$ を求める.

$$(\sharp) \qquad \begin{pmatrix} 1 & \lambda_1 & \lambda_1^2 & \cdots & \lambda_1^\ell & z_1 & z_1\lambda_1 & z_1\lambda_1^2 & \cdots & z_1\lambda_1^m \\ 1 & \lambda_2 & \lambda_2^2 & \cdots & \lambda_2^\ell & z_2 & z_2\lambda_2 & z_2\lambda_2^2 & \cdots & z_2\lambda_2^m \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \lambda_n & \lambda_n^2 & \cdots & \lambda_n^\ell & z_n & z_n\lambda_n & z_n\lambda_n^2 & \cdots & z_n\lambda_n^m \end{pmatrix} \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_\ell \\ \beta_0 \\ \beta_1 \\ \vdots \\ \beta_m \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

3. 非自明解から多項式 $Q_0(X), Q_1(X)$ を

$$Q_0(X) = \sum_{i=0}^{\ell} \alpha_i X^i, \qquad Q_1(X) = \sum_{i=0}^{m} \beta_i X^i$$

で定める.

4. $f(X) = -Q_0(X)/Q_1(X)$ とおく.
5. $f(X) \in \mathbf{F}_q[X]$ ならば, $w = T(f(X))$ で復号する. エラーのある位置 i は $Q_1(\lambda_i) = 0$ となる i である.
6. $f(X) \notin \mathbf{F}_q[X]$ ならば受信エラーを返す.

例 **1** $p = 19$ とする. $\mathbf{F}_{19}$ の原始元は **PrimitiveRoot** で求まる.

***p* = 19**
19
PrimitiveRoot[*p*]
2

$\Lambda = \mathbf{F}_{19}^\times = \{1, 2, \cdots, 2^{17}\}$ として, Reed–Solomon コード $\mathrm{GRS}_{10}(\Lambda, \mathbf{1})$ を考える. これは $[18, 10, 9]_{19}$ コードで. $t = [(9-1)/2] = 4$ ビットのエラーが訂正できる. 受信語

$$z = w + e = {}^t(3, 0, 1, 4, 4, 0, 9, 12, 1, 14, 17, 2, 13, 1, 16, 8, 12, 16)$$

の復号を考える. $n=18, k=10, l=n-t-1, m=n-k-t$ を与える.

$n = p - 1$

18

$k = 10$

10

$t =$ IntegerPart[$(p-k)/2$]

4

$l = n - t - 1$

13

$m = n - k - t$

4

Λ のリストを与える. $2^i \mod p$ を計算するには **PowerMod[$2, i, p$]** を用いる.

Lambda = Table[PowerMod[$2, i, p$], {$i, 0, p-2$}]

$\{1, 2, 4, 8, 16, 13, 7, 14, 9, 18, 17, 15, 11, 3, 6, 12, 5, 10\}$

受信語 z を与える.

$z = \{3, 0, 1, 4, 4, 0, 9, 12, 1, 14, 17, 2, 13, 1, 16, 8, 12, 16\}$

$\{3, 0, 1, 4, 4, 0, 9, 12, 1, 14, 17, 2, 13, 1, 16, 8, 12, 16\}$

(♯) の連立 1 次方程式の係数行列を与え, それを B とおく. B の各行は, ふたつの数列 $\{1, \lambda_i, \lambda_i^2, \cdots, \lambda_i^\ell\}$ と $\{z_i, z_i\lambda_i, z_i\lambda_i^2, \cdots, z_i\lambda_i^m\}$ を繋げたものになる. リストの結合を **Join** で行う.

$B =$ Join[Table[Mod[Lambda[[i]]^j, p], {$i, 1,$ Length[Lambda]}, {$j, 0, l$}],
Table[Mod[z[[i]] * Lambda[[i]]^j, p], {$i, 1,$ Length[Lambda]}, {$j, 0, m$}], 2];
MatrixForm[B]

$$\begin{pmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 3 & 3 & 3 & 3 & 3 \\
1 & 2 & 4 & 8 & 16 & 13 & 7 & 14 & 9 & 18 & 17 & 15 & 11 & 3 & 0 & 0 & 0 & 0 & 0 \\
1 & 4 & 16 & 7 & 9 & 17 & 11 & 6 & 5 & 1 & 4 & 16 & 7 & 9 & 1 & 4 & 16 & 7 & 9 \\
1 & 8 & 7 & 18 & 11 & 12 & 1 & 8 & 7 & 18 & 11 & 12 & 1 & 8 & 4 & 13 & 9 & 15 & 6 \\
1 & 16 & 9 & 11 & 5 & 4 & 7 & 17 & 6 & 1 & 16 & 9 & 11 & 5 & 4 & 7 & 17 & 6 & 1 \\
1 & 13 & 17 & 12 & 4 & 14 & 11 & 10 & 16 & 18 & 6 & 2 & 7 & 15 & 0 & 0 & 0 & 0 & 0 \\
1 & 7 & 11 & 1 & 7 & 11 & 1 & 7 & 11 & 1 & 7 & 11 & 1 & 7 & 9 & 6 & 4 & 9 & 6 \\
1 & 14 & 6 & 8 & 17 & 10 & 7 & 3 & 4 & 18 & 5 & 13 & 11 & 2 & 12 & 16 & 15 & 1 & 14 \\
1 & 9 & 5 & 7 & 6 & 16 & 11 & 4 & 17 & 1 & 9 & 5 & 7 & 6 & 1 & 9 & 5 & 7 & 6 \\
1 & 18 & 1 & 18 & 1 & 18 & 1 & 18 & 1 & 18 & 1 & 18 & 1 & 18 & 14 & 5 & 14 & 5 & 14 \\
1 & 17 & 4 & 11 & 16 & 6 & 7 & 5 & 9 & 1 & 17 & 4 & 11 & 16 & 17 & 4 & 11 & 16 & 6 \\
1 & 15 & 16 & 12 & 9 & 2 & 11 & 13 & 5 & 18 & 4 & 3 & 7 & 10 & 2 & 11 & 13 & 5 & 18 \\
1 & 11 & 7 & 1 & 11 & 7 & 1 & 11 & 7 & 1 & 11 & 7 & 1 & 11 & 13 & 10 & 15 & 13 & 10 \\
1 & 3 & 9 & 8 & 5 & 15 & 7 & 2 & 6 & 18 & 16 & 10 & 11 & 14 & 1 & 3 & 9 & 8 & 5 \\
1 & 6 & 17 & 7 & 4 & 5 & 11 & 9 & 16 & 1 & 6 & 17 & 7 & 4 & 16 & 1 & 6 & 17 & 7 \\
1 & 12 & 11 & 18 & 7 & 8 & 1 & 12 & 11 & 18 & 7 & 8 & 1 & 12 & 8 & 1 & 12 & 11 & 18 \\
1 & 5 & 6 & 11 & 17 & 9 & 7 & 16 & 4 & 1 & 5 & 6 & 11 & 17 & 12 & 3 & 15 & 18 & 14 \\
1 & 10 & 5 & 12 & 6 & 3 & 11 & 15 & 17 & 18 & 9 & 14 & 7 & 13 & 16 & 8 & 4 & 2 & 1
\end{pmatrix}$$

連立 1 次方程式の解を **NullSpace** で求める. これは $\mathrm{Ker}B$ の基底を与えるので, 基底の中の 1 つめのベクトルだけを取り出す.

Q = NullSpace[B, Modulus → p][[1]]
$\{0, 6, 8, 15, 5, 9, 13, 8, 3, 0, 1, 0, 0, 0, 13, 11, 3, 0, 1\}$

この解から, 多項式 $Q_0(X)$ と $Q_1(X)$ を構成する. 最初の $\ell + 1$ 個の成分が $Q_0(X)$ の係数で, 残りが $Q_1(X)$ の係数となる.

Q0 = Sum[Q[[i]] * X^(i − 1), {i, 1, l + 1}]
$6X + 8X^2 + 15X^3 + 5X^4 + 9X^5 + 13X^6 + 8X^7 + 3X^8 + X^{10}$
Q1 = Sum[Q[[i + l + 1]] * X^(i − 1), {i, 1, m + 1}]
$13 + 11X + 3X^2 + X^4$

$f(X) = -Q_0(X)/Q_1(X)$ を計算する.

f = PolynomialQuotient[−Q0, Q1, X, Modulus → p]
$X + 3X^3 + 18X^6$

$w = T(f)$ がエラー訂正された復号語となる.

w = Mod[Table[f/.X → Lambda[[i]], {i, 1, Length[Lambda]}], p]
$\{3, 0, 14, 4, 4, 0, 9, 12, 0, 14, 5, 2, 13, 1, 16, 8, 12, 16\}$

z と比較して, 3 箇所のエラーがあったことがわかる.

ついでに, $\mathrm{GRS}_{10}(\Lambda, \mathbf{1})$ の生成行列と検査行列を求め, w が実際に符号ワードになることを確認する. 生成行列 A は §E1 で与えた形となる.

A = Table[PowerMod[Lambda[[i + 1]], j, p], {i, 0, p − 2}, {j, 0, k − 1}];
MatrixForm[A]

$$\begin{pmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 2 & 4 & 8 & 16 & 13 & 7 & 14 & 9 & 18 \\
1 & 4 & 16 & 7 & 9 & 17 & 11 & 6 & 5 & 1 \\
1 & 8 & 7 & 18 & 11 & 12 & 1 & 8 & 7 & 18 \\
1 & 16 & 9 & 11 & 5 & 4 & 7 & 17 & 6 & 1 \\
1 & 13 & 17 & 12 & 4 & 14 & 11 & 10 & 16 & 18 \\
1 & 7 & 11 & 1 & 7 & 11 & 1 & 7 & 11 & 1 \\
1 & 14 & 6 & 8 & 17 & 10 & 7 & 3 & 4 & 18 \\
1 & 9 & 5 & 7 & 6 & 16 & 11 & 4 & 17 & 1 \\
1 & 18 & 1 & 18 & 1 & 18 & 1 & 18 & 1 & 18 \\
1 & 17 & 4 & 11 & 16 & 6 & 7 & 5 & 9 & 1 \\
1 & 15 & 16 & 12 & 9 & 2 & 11 & 13 & 5 & 18 \\
1 & 11 & 7 & 1 & 11 & 7 & 1 & 11 & 7 & 1 \\
1 & 3 & 9 & 8 & 5 & 15 & 7 & 2 & 6 & 18 \\
1 & 6 & 17 & 7 & 4 & 5 & 11 & 9 & 16 & 1 \\
1 & 12 & 11 & 18 & 7 & 8 & 1 & 12 & 11 & 18 \\
1 & 5 & 6 & 11 & 17 & 9 & 7 & 16 & 4 & 1 \\
1 & 10 & 5 & 12 & 6 & 3 & 11 & 15 & 17 & 18
\end{pmatrix}$$

検査行列 H は, $\mathrm{Ker}^t A$ の基底を行とする行列である.

H = NullSpace[Transpose[A], Modulus → p]
MatrixForm[H]

$$\begin{pmatrix} 16 & 4 & 2 & 5 & 2 & 14 & 2 & 15 & 16 & 18 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 14 & 14 & 11 & 17 & 1 & 6 & 2 & 4 & 9 & 16 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 18 & 12 & 8 & 7 & 16 & 15 & 14 & 8 & 1 & 14 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 9 & 12 & 9 & 2 & 17 & 9 & 10 & 16 & 11 & 18 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 11 & 3 & 10 & 10 & 17 & 17 & 9 & 7 & 9 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 14 & 18 & 8 & 5 & 15 & 3 & 7 & 11 & 12 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 3 & 9 & 15 & 2 & 13 & 1 & 2 & 11 & 5 & 14 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 18 & 3 & 15 & 17 & 14 & 17 & 5 & 17 & 4 & 3 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

$W = \mathrm{Ker}H$ である.

Mod[H.w, p]
$\{\{0\},\{0\},\{0\},\{0\},\{0\},\{0\},\{0\},\{0\}\}$

から $w \in W$ である.

問題 E1

$p = 29$ とする. 2 は $\mathbf{F}_{29}$ の原始元である. $\Lambda = \{2^0, 2^1, \cdots, 2^{27}\}$ として, $C = \mathrm{GRS}_{15}(\Lambda, \mathbf{1})$ によるコード化を考える. これは $[28, 15, 14]_{29}$ コードであるから, 15 文字のメッセージが符号化できる. アルファベットと $\mathbf{F}_{29}$ の要素の対応を

$$a \leftrightarrow 1, \quad b \leftrightarrow 2, \quad \cdots, \quad z \leftrightarrow 26, \quad -(\text{ハイフン}) \leftrightarrow 27, \quad ? \leftrightarrow 28, \quad .(\text{ピリオド}) \leftrightarrow 0$$

で与える.

Alphabet = Characters[".abcdefghijklmnopqrstuvwxyz-?"]

$\{., a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r, s, t, u, v, w, x, y, z, -, ?\}$

数字からアルファベットへの変換と逆の変換のリストを準備しておく.

NtoA = Table[$i \to$ Alphabet[[$i+1$]], {i, 0, 28}];
AtoN = Table[Alphabet[[$i+1$]] $\to i$, {i, 0, 28}];

osaka を数字に変換する.

Characters["osaka"]/.AtoN

$\{15, 19, 1, 11, 1\}$

数列 $\{20, 15, 25, 15, 14, 1, 11, 1\}$ を文字に変換する.

StringJoin[{20, 15, 25, 15, 14, 1, 11, 1}/.NtoA]

toyonaka

1 5 文字のメッセージ M を上の対応で数値化し C でコード化して, その受信語が

$$z = \{10, 13, 1, 8, 0, 14, 12, 13, 26, 27, 7, 17, 28, 15, 9, 7, 21, 19, 26, 17, 0, 28, 8, 6, 10, 24, 19, 4\}$$

で得られた. これから元のメッセージ M を復元せよ.

StringJoin[z/.NtoA]

-eans-sdlctchn-

***p* = 29**

29

PrimitiveRoot[p]

2

***n* = *p* − 1**

28

***k* = 15**

15

***t* = IntegerPart[(*n* − *k*)/2]**

6

***l* = *n* − *t* − 1**

21

$m = n - k - t$

7

$\mathbf{Lambda = Table[PowerMod[2, i, p], \{i, 0, p - 2\}]}$

$\{1, 2, 4, 8, 16, 3, 6, 12, 24, 19, 9, 18, 7, 14, 28, 27, 25, 21, 13, 26, 23, 17, 5, 10, 20, 11, 22, 15\}$

$\mathbf{Length[Lambda]}$

28

$\mathbf{A = Table[PowerMod[Lambda[[i + 1]], j, p], \{i, 0, p - 2\}, \{j, 0, k - 1\}];}$

$\mathbf{MatrixForm[A]}$

$$\begin{pmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 2 & 4 & 8 & 16 & 3 & 6 & 12 & 24 & 19 & 9 & 18 & 7 & 14 & 28 \\
1 & 4 & 16 & 6 & 24 & 9 & 7 & 28 & 25 & 13 & 23 & 5 & 20 & 22 & 1 \\
1 & 8 & 6 & 19 & 7 & 27 & 13 & 17 & 20 & 15 & 4 & 3 & 24 & 18 & 28 \\
1 & 16 & 24 & 7 & 25 & 23 & 20 & 1 & 16 & 24 & 7 & 25 & 23 & 20 & 1 \\
1 & 3 & 9 & 27 & 23 & 11 & 4 & 12 & 7 & 21 & 5 & 15 & 16 & 19 & 28 \\
1 & 6 & 7 & 13 & 20 & 4 & 24 & 28 & 23 & 22 & 16 & 9 & 25 & 5 & 1 \\
1 & 12 & 28 & 17 & 1 & 12 & 28 & 17 & 1 & 12 & 28 & 17 & 1 & 12 & 28 \\
1 & 24 & 25 & 20 & 16 & 7 & 23 & 1 & 24 & 25 & 20 & 16 & 7 & 23 & 1 \\
1 & 19 & 13 & 15 & 24 & 21 & 22 & 12 & 25 & 11 & 6 & 27 & 20 & 3 & 28 \\
1 & 9 & 23 & 4 & 7 & 5 & 16 & 28 & 20 & 6 & 25 & 22 & 24 & 13 & 1 \\
1 & 18 & 5 & 3 & 25 & 15 & 9 & 17 & 16 & 27 & 22 & 19 & 23 & 8 & 28 \\
1 & 7 & 20 & 24 & 23 & 16 & 25 & 1 & 7 & 20 & 24 & 23 & 16 & 25 & 1 \\
1 & 14 & 22 & 18 & 20 & 19 & 5 & 12 & 23 & 3 & 13 & 8 & 25 & 2 & 28 \\
1 & 28 & 1 & 28 & 1 & 28 & 1 & 28 & 1 & 28 & 1 & 28 & 1 & 28 & 1 \\
1 & 27 & 4 & 21 & 16 & 26 & 6 & 17 & 24 & 10 & 9 & 11 & 7 & 15 & 28 \\
1 & 25 & 16 & 23 & 24 & 20 & 7 & 1 & 25 & 16 & 23 & 24 & 20 & 7 & 1 \\
1 & 21 & 6 & 10 & 7 & 2 & 13 & 12 & 20 & 14 & 4 & 26 & 24 & 11 & 28 \\
1 & 13 & 24 & 22 & 25 & 6 & 20 & 28 & 16 & 5 & 7 & 4 & 23 & 9 & 1 \\
1 & 26 & 9 & 2 & 23 & 18 & 4 & 17 & 7 & 8 & 5 & 14 & 16 & 10 & 28 \\
1 & 23 & 7 & 16 & 20 & 25 & 24 & 1 & 23 & 7 & 16 & 20 & 25 & 24 & 1 \\
1 & 17 & 28 & 12 & 1 & 17 & 28 & 12 & 1 & 17 & 28 & 12 & 1 & 17 & 28 \\
1 & 5 & 25 & 9 & 16 & 22 & 23 & 28 & 24 & 4 & 20 & 13 & 7 & 6 & 1 \\
1 & 10 & 13 & 14 & 24 & 8 & 22 & 17 & 25 & 18 & 6 & 2 & 20 & 26 & 28 \\
1 & 20 & 23 & 25 & 7 & 24 & 16 & 1 & 20 & 23 & 25 & 7 & 24 & 16 & 1 \\
1 & 11 & 5 & 26 & 25 & 14 & 9 & 12 & 16 & 2 & 22 & 10 & 23 & 21 & 28 \\
1 & 22 & 20 & 5 & 23 & 13 & 25 & 28 & 7 & 9 & 24 & 6 & 16 & 4 & 1 \\
1 & 15 & 22 & 11 & 20 & 10 & 5 & 17 & 23 & 26 & 13 & 21 & 25 & 27 & 28
\end{pmatrix}$$

$\mathbf{Mod[A.w, p]}$

$\{10, 13, 10, 5, 0, 14, 12, 13, 26, 27, 7, 17, 28, 15, 9, 7, 26, 17, 26, 17, 0, 28, 8, 6, 24, 24, 19, 0\}$

$\mathbf{z = \{10, 13, 1, 8, 0, 14, 12, 13, 26, 27, 7, 17, 28, 15, 9, 7, 21, 19, 26, 17, 0, 28, 8, 6, 10, 24, 19, 4\}}$

$\{10, 13, 1, 8, 0, 14, 12, 13, 26, 27, 7, 17, 28, 15, 9, 7, 21, 19, 26, 17, 0, 28, 8, 6, 10, 24, 19, 4\}$

$\mathbf{B = Join[Table[Mod[Lambda[[i]]\text{^}j, p], \{i, 1, Length[Lambda]\}, \{j, 0, l\}],}$
$\mathbf{Table[Mod[z[[i]] * Lambda[[i]]\text{^}j, p], \{i, 1, Length[Lambda]\}, \{j, 0, m\}], 2];}$

$\mathbf{MatrixForm[B]}$

$\mathbf{Q = NullSpace[B, Modulus \to p][[1]]}$

$\{7, 0, 25, 28, 28, 3, 16, 15, 1, 23, 21, 20, 28, 27, 15, 19, 9, 7, 0, 5, 15, 2, 18, 27, 14, 1, 2, 10, 0, 1\}$

$\mathbf{Q1 = Sum[}Q\mathbf{[[}i\mathbf{]] * }X\mathbf{\text{^}(}i - 1\mathbf{), \{}i, 1, l + 1\mathbf{\}]}$

$7 + 25X^2 + 28X^3 + 28X^4 + 3X^5 + 16X^6 + 15X^7 + X^8 + 23X^9 + 21X^{10} + 20X^{11} + 28X^{12} + 27X^{13} + 15X^{14} + 19X^{15} + 9X^{16} + 7X^{17} + 5X^{19} + 15X^{20} + 2X^{21}$

$\mathbf{Q2 = Sum[}Q\mathbf{[[}i + l + 1\mathbf{]] * }X\mathbf{\text{^}(}i - 1\mathbf{), \{}i, 1, m + 1\mathbf{\}]}$

$18 + 27X + 14X^2 + X^3 + 2X^4 + 10X^5 + X^7$

$f = \mathbf{\ PolynomialQuotient[-Q1, Q2, }X\mathbf{, Modulus \to }p\mathbf{]}$

$27 + 3X + 15X^2 + 14X^3 + 19X^4 + 20X^5 + 5X^6 + 12X^7 + 12X^8 + X^9 + 20X^{10} + 9X^{11} + 15X^{12} + 14X^{13} + 27X^{14}$

$\mathbf{Mod[Table[}f\mathbf{/.}X \to \mathbf{Lambda[[}i\mathbf{]], \{}i, 1, \mathbf{Length[Lambda]\}], }p\mathbf{]}$

$\{10, 13, 10, 5, 0, 14, 12, 13, 26, 27, 7, 17, 28, 15, 9, 7, 26, 17, 26, 17, 0, 28, 8, 6, 24, 24, 19, 0\}$

$w = \mathbf{CoefficientList[}f, X\mathbf{]}$

$\{27, 3, 15, 14, 19, 20, 5, 12, 12, 1, 20, 9, 15, 14, 27\}$

$\mathbf{StringJoin[}w\mathbf{/.NtoA]}$

-constellation-

実験数学３
F 巡回コード
F1. 巡回符号によるメッセージのコード化
$\mathbf{F}_q[X]$ における $\Phi_n(X) = X^n - 1$ のモニック因子 $g(X)$ を固定する. $g(X)$ から生成されるイデアルを

$$J = \{m(X)g(X) \mid m(X) \in \mathbf{F}_q[X]\}$$

とし

$$J^{n-1} = \{f(X) \in J \mid \deg f(X) \leq n-1\}$$

とおく. 多項式とベクトルの対応

$$f(X) = a_0 + a_1X + \cdots + a_{n-1}X^{n-1} \longleftrightarrow u_{f(X)} = {}^t(a_0, a_1, \cdots, a_{n-1}) \in \mathbf{F}_q^n$$

により,

$$W = \{u_{f(X)} \mid f(X) \in J^{n-1}\}$$

とすれば, $C_{g(X)} = (\mathbf{F}_q^n, W)$ は巡回コードを与える. $k = \dim W = n - \deg g(X)$ である. $M = \{c_0, c_1, \cdots, c_{k-1}\}$ を k ビットのメッセージとするとき,

$$m(X) = c_0 + c_1X + \cdots + c_{k-1}X^{k-1} \in \mathbf{F}_q[X]$$

とすれば, $m(X)g(X) \in J^{n-1}$ である. このとき $u_{m(X)g(X)}$ が M のコード化となる.

例 1 $\Phi_{15}(X) = X^{15} - 1$ を $\mathbf{F}_2[X]$ で既約分解すると

Factor[X^15 − 1, Modulus → 2]

$$(1+X)\left(1+X+X^2\right)\left(1+X+X^4\right)\left(1+X^3+X^4\right)\left(1+X+X^2+X^3+X^4\right)$$

モニック因子 $g(X) = X^4 + X + 1$ から, 巡回コード $C_{g(X)} = (\mathbf{F}_2^{15}, W)$ ができる. これは $[15, 11]_2$ コードである. 1 1 ビットのメッセージ $\{1,1,0,1,0,0,0,1,0,0,0\} \longleftrightarrow 1 + X + X^3 + X^7$ をコード化する.

g = X^4 + X + 1

$$1 + X + X^4$$

m = 1 + X + X^3 + X^7

$$1 + X + X^3 + X^7$$

m ∗ g

$$\left(1+X+X^4\right)\left(1+X+X^3+X^7\right)$$

多項式の係数は **CoefficientList** で取り出せる.

Mod[CoefficientList[m ∗ g, X], 2]

$$\{1,0,1,1,0,1,0,0,1,0,0,1\}$$

これでは長さ 1 5 にならないので, **PadRight** で長さ 1 5 になるように 0 を付け加える.

PadRight[Mod[CoefficientList[m ∗ g, X], 2], 15]

$$\{1,0,1,1,0,1,0,0,1,0,0,1,0,0,0\}$$

F2. 巡回コードの検査行列

巡回コード $C_{g(X)} = (\mathbf{F}_q^n, W)$ の双対コード $C_{g(X)}^{\perp} = (\mathbf{F}_q^n, W^{\perp})$ も巡回コードとなる. $C_{g(X)}^{\perp}$ の生成多項式は

$$h(X) = -g(0)X^k \frac{\Phi_n(X^{-1})}{g(X^{-1})}$$

となる. ただし $k = \dim W = n - \deg g(X)$ である. $\deg h(X) = k$ となるので

$$h(X) = h_0 + h_1 X + \cdots + h_k X^k$$

と書ける. このとき, $C_{g(X)}$ の検査行列は

$$H_C = \begin{pmatrix} h_0 & h_1 & \cdots & h_{k-1} & h_k & 0 & \cdots & 0 \\ 0 & h_0 & h_1 & \cdots & h_{k-1} & h_k & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \cdots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & h_0 & h_1 & \cdots & h_{k-1} & h_k \end{pmatrix} \in M_{n-k,n}(\mathbf{F}_q)$$

で与えられる.

多項式 $f(X)$ に対応するベクトル $u_{f(X)} \in \mathbf{F}_q^n$ が W に含まれるかどうかは,

$$u_{f(X)} \in W \iff g(X) \mid f(X) \iff \Phi_n(X) \mid f(X)h(X)$$

から多項式だけで判定できる.

例 2 例 1 の巡回コード $C_{g(X)}$ の検査行列を求める.

g[X_] = X^4 + X + 1

$1 + X + X^4$

h = Cancel[−g[0] * X^(11) * (X^(−15) − 1)/g[X^(−1)], Modulus → 2]

$1 + X^3 + X^4 + X^6 + X^8 + X^9 + X^{10} + X^{11}$

CoefficientList[h, X]

$\{1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1\}$

a = PadRight[CoefficientList[h, X], 15]

$\{1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0\}$

RotateRight[a]

$\{0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0\}$

H = Table[RotateRight[a, i], {i, 0, 3}]

$\{\{1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0\}, \{0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0\},$
$\{0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0\}, \{0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1\}\}$

MatrixForm[H]

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

F3. 巡回コードの最小距離

C2 で述べたように, コードの最小距離の計算は簡単ではない. これは巡回コードの場合でも同じである.

例 3 $\mathbf{F}_2$ 上で $X^{15}-1$ の 8 次モニック因子から構成されるすべての巡回コードの最少距離を求める. $X^{15}-1$ の因数分解は

```
Factor[X^(15) - 1, Modulus → 2]
```
$$(1+X)\left(1+X+X^2\right)\left(1+X+X^4\right)\left(1+X^3+X^4\right)\left(1+X+X^2+X^3+X^4\right)$$

4 次の因子だけを取り出し, そのリストを M とおく.

```
M = Select[Flatten[FactorList[X^(15) - 1, Modulus → 2]], Exponent[#, X] == 4&]
```
$$\left\{1+X+X^4, 1+X^3+X^4, 1+X+X^2+X^3+X^4\right\}$$

M から異なるふたつを選びその積をとってできるリストを P とおく. これが $X^{15}-1$ の 8 次モニック因子すべてのリストを与える.

```
P =  M[[#[[1]]]] * M[[#[[2]]]]&/@Subsets[{1, 2, 3}, {2}]
```
$$\{\left(1+X+X^4\right)\left(1+X^3+X^4\right),$$
$$\left(1+X+X^4\right)\left(1+X+X^2+X^3+X^4\right),$$
$$\left(1+X^3+X^4\right)\left(1+X+X^2+X^3+X^4\right)\}$$

以下, それぞれの最少距離を求める.

```
L = Tuples[{0, 1}, 7];
P[[1]]
```
$$\left(1+X+X^4\right)\left(1+X^3+X^4\right)$$
```
Min[HammingDistance[PadRight[
Mod[CoefficientList[Sum[#[[j]] * X^(j - 1), {j, 1, 7}] * P[[1]], X], 2],
15], Table[0, {15}]]&/@Complement[L, {L[[1]]}]]
```
```
3
```
```
P[[2]]
```
$$\left(1+X+X^4\right)\left(1+X+X^2+X^3+X^4\right)$$
```
Min[HammingDistance[PadRight[
Mod[CoefficientList[Sum[#[[j]] * X^(j - 1), {j, 1, 7}] * P[[2]], X], 2],
15], Table[0, {15}]]&/@Complement[L, {L[[1]]}]]
```
```
5
```
```
P[[3]]
```
$$\left(1+X^3+X^4\right)\left(1+X+X^2+X^3+X^4\right)$$
```
Min[HammingDistance[PadRight[
Mod[CoefficientList[Sum[#[[j]] * X^(j - 1), {j, 1, 7}] * P[[3]], X], 2],
15], Table[0, {15}]]&/@Complement[L, {L[[1]]}]]
```
```
5
```

問題 F1 $\mathbf{F}_2$ 上 $X^{31}-1$ の 15 次モニック因子から構成される $[31,16]_2$ コードの最少距離を以下の順に従って求めよ.

(1) $X^{31}-1$ の 5 次既約因子全体からなるリスト M を構成せよ.

(2) M から異なる 3 個を選びその積をとってできるリスト P を構成せよ.

(3) P の各要素に対し, 対応する巡回コードの最少距離を計算するプログラムを作れ.

(4) $[31,16]_2$ 巡回コードの中で, 最大の最少距離を持つコードの生成多項式をすべて書き下せ.

```
Factor[X^(31) - 1, Modulus → 2]
```

$$(1+X)\left(1+X^2+X^5\right)\left(1+X^3+X^5\right)\left(1+X+X^2+X^3+X^5\right)$$
$$\left(1+X+X^2+X^4+X^5\right)\left(1+X+X^3+X^4+X^5\right)\left(1+X^2+X^3+X^4+X^5\right)$$

```
M = Select[Flatten[FactorList[X^(31) - 1, Modulus → 2]],Exponent[#, X] == 5&]
```

$$\{1+X^2+X^5, 1+X^3+X^5, 1+X+X^2+X^3+X^5, 1+X+X^2+X^4+X^5,$$
$$1+X+X^3+X^4+X^5, 1+X^2+X^3+X^4+X^5\}$$

```
P = M[[#[[1]]]] * M[[#[[2]]]] * M[[#[[3]]]]&/@Subsets[{1, 2, 3, 4, 5, 6}, {3}]
```

$$\{\left(1+X^2+X^5\right)\left(1+X^3+X^5\right)\left(1+X+X^2+X^3+X^5\right),$$
$$\left(1+X^2+X^5\right)\left(1+X^3+X^5\right)\left(1+X+X^2+X^4+X^5\right),$$
$$\left(1+X^2+X^5\right)\left(1+X^3+X^5\right)\left(1+X+X^3+X^4+X^5\right),$$
$$\left(1+X^2+X^5\right)\left(1+X^3+X^5\right)\left(1+X^2+X^3+X^4+X^5\right),$$
$$\left(1+X^2+X^5\right)\left(1+X+X^2+X^3+X^5\right)\left(1+X+X^2+X^4+X^5\right),$$
$$\left(1+X^2+X^5\right)\left(1+X+X^2+X^3+X^5\right)\left(1+X+X^3+X^4+X^5\right),$$
$$\left(1+X^2+X^5\right)\left(1+X+X^2+X^3+X^5\right)\left(1+X^2+X^3+X^4+X^5\right),$$
$$\left(1+X^2+X^5\right)\left(1+X+X^2+X^4+X^5\right)\left(1+X+X^3+X^4+X^5\right),$$
$$\left(1+X^2+X^5\right)\left(1+X+X^2+X^4+X^5\right)\left(1+X^2+X^3+X^4+X^5\right),$$
$$\left(1+X^2+X^5\right)\left(1+X+X^3+X^4+X^5\right)\left(1+X^2+X^3+X^4+X^5\right),$$
$$\left(1+X^3+X^5\right)\left(1+X+X^2+X^3+X^5\right)\left(1+X+X^2+X^4+X^5\right),$$
$$\left(1+X^3+X^5\right)\left(1+X+X^2+X^3+X^5\right)\left(1+X+X^3+X^4+X^5\right),$$
$$\left(1+X^3+X^5\right)\left(1+X+X^2+X^3+X^5\right)\left(1+X^2+X^3+X^4+X^5\right),$$
$$\left(1+X^3+X^5\right)\left(1+X+X^2+X^4+X^5\right)\left(1+X+X^3+X^4+X^5\right),$$
$$\left(1+X^3+X^5\right)\left(1+X+X^2+X^4+X^5\right)\left(1+X^2+X^3+X^4+X^5\right),$$
$$\left(1+X^3+X^5\right)\left(1+X+X^3+X^4+X^5\right)\left(1+X^2+X^3+X^4+X^5\right),$$
$$\left(1+X+X^2+X^3+X^5\right)\left(1+X+X^2+X^4+X^5\right)\left(1+X+X^3+X^4+X^5\right),$$
$$\left(1+X+X^2+X^3+X^5\right)\left(1+X+X^2+X^4+X^5\right)\left(1+X^2+X^3+X^4+X^5\right),$$
$$\left(1+X+X^2+X^3+X^5\right)\left(1+X+X^3+X^4+X^5\right)\left(1+X^2+X^3+X^4+X^5\right),$$
$$\left(1+X+X^2+X^4+X^5\right)\left(1+X+X^3+X^4+X^5\right)\left(1+X^2+X^3+X^4+X^5\right)\}$$

```
Length[P]
```

20

```
L = Tuples[{0, 1}, 16];
Length[L]
```

65536

```
o = Table[0, {31}];
Table[Min[HammingDistance[PadRight[
Mod[CoefficientList[Sum[#[[j]] * X^(j - 1), {j, 1, 16}] * P[[k]], X],
2], 31], o]&/@Complement[L, {L[[1]]}]], {k, 1, 20}]
```

$$\{5,6,6,5,7,7,6,5,7,7,7,7,6,5,7,7,6,5,5,6\}$$

F4. 巡回コードの最小距離の BCH 限界

Ω を $\mathbf{F}_q$ の代数的閉体とする. $\zeta \in \Omega$ が $\Phi_n(\zeta) = 0$, $\Phi_m(\zeta) \neq 0$ $(1 \leq {}^{\forall}m < n)$ をみたすとき, この ζ を 1 の原始 n 乗根という.

定理 $g(X)$ を $\Phi_n(X)$ のモニック因子として, $C_{g(X)} = (\mathbf{F}_q^n, W)$ を巡回コードとする. 1 の原始 n 乗根 $\zeta \in \Omega$ と定数 ℓ, δ が存在して

$$g(\zeta^{\ell}) = g(\zeta^{\ell+1}) = \cdots = g(\zeta^{\ell+\delta-2}) = 0$$

が成り立つとき, $C_{g(X)}$ の最小距離は $d_{C_{g(X)}} \geq \delta$ をみたす.

証明 任意の $f(X) \in J^{n-1}$ は $g(X)$ で割り切れるので, 仮定から

$$f(\zeta^{\ell}) = f(\zeta^{\ell+1}) = \cdots = f(\zeta^{\ell+\delta-2}) = 0$$

となる. これは

$$\begin{pmatrix} 1 & \zeta^{\ell} & \zeta^{2\ell} & \cdots & \zeta^{(n-1)\ell} \\ 1 & \zeta^{\ell+1} & \zeta^{2(\ell+1)} & \cdots & \zeta^{(n-1)(\ell+1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \zeta^{\ell+\delta-2} & \zeta^{2(\ell+\delta-2)} & \cdots & \zeta^{(n-1)(\ell+\delta-2)} \end{pmatrix} u_{f(X)} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

と同値である. $C_{g(X)}$ の最小距離を d として, $d \leq \delta - 1$ と仮定すると矛盾が出ることをいう. $|u_{f(X)}| = d$ となる $f(X)$ を固定し, $u_{f(X)}$ の成分で 0 と異なるものを $a_{i_1}, \cdots, a_{i_d}$ とおく. 上の係数行列で, 最初の d 行と i_1 列, i_2 列, ..., i_d 列からなる $d \times d$ 部分行列を考えれば,

$$\begin{pmatrix} \zeta^{i_1\ell} & \zeta^{i_2\ell} & \cdots & \zeta^{i_d\ell} \\ \zeta^{i_1(\ell+1)} & \zeta^{i_2(\ell+1)} & \cdots & \zeta^{i_d(\ell+1)} \\ \vdots & \vdots & \ddots & \vdots \\ \zeta^{i_1(\ell+d-1} & \zeta^{i_2(\ell+d-1)} & \cdots & \zeta^{i_d(\ell+d-1)} \end{pmatrix} \begin{pmatrix} a_{i_1} \\ a_{i_2} \\ \vdots \\ a_{i_d} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

となる. これから, 行列

$$D = \begin{pmatrix} \zeta^{i_1\ell} & \zeta^{i_2\ell} & \cdots & \zeta^{i_d\ell} \\ \zeta^{i_1(\ell+1)} & \zeta^{i_2(\ell+1)} & \cdots & \zeta^{i_d(\ell+1)} \\ \vdots & \vdots & \ddots & \vdots \\ \zeta^{i_1(\ell+d-1} & \zeta^{i_2(\ell+d-1)} & \cdots & \zeta^{i_d(\ell+d-1)} \end{pmatrix}$$

は ${}^t(a_{i_1}, \cdots, a_{i_d}) \neq 0$ を $\mathrm{Ker}D$ に含むから正則行列ではない. 他方, D の行列式 $\det D$ は, Vandermonde の行列式となり, $\det D \neq 0$ となるので矛盾である. よって $d \geq \delta$ でなければならない.