代数系と符号理論 (ICT.C209) 授業関連情報

担当教員 笠井 健太 (所属：工学院 情報通信系、南 3 号館 4 階 418 号室)

教員の Email: kenta@ict.eng.isct.ac.jp

配布資料・演習問題・予想試験問題 https://kasaikenta.github.io/
配付資料に誤りがあった場合に更新されるので、最新版をチェックしてください。[1]

成績評価 中間試験と期末試験の結果が成績の大部分を支配します。

参考書
代数系と符号理論、植松、オーム社
符号理論、平澤, https://bit.ly/3YxGsYt
符号理論入門、平澤, 西島、培風館
代数系と符号理論入門、坂庭好一、渋谷智治、コロナ社
符号理論，今井，コロナ社

[1]授業で講義資料を参照するまでは、各節には去年の講義のものがそのまま掲載されています。今年度の資料は、昨年度のものを修正して、その授業の開始までに掲載されます。

集合と写像の基本概念と記法は、必要になったときに説明していきます。必要に応じて下記を利用してください。

参考書：情報基礎数学，佐藤泰介ら著，オーム社，2014，ISBN 978-4-274-21610-7

参考科目：XCO.B101 情報理工学基礎 1(Science Tokyo 情報理工学院の科目です)

この資料の中の@マークは、全１２回講義の各回の区切りの目安を表しています。

定義 0.1. 文脈から誤解が生じない場合には、以下のように表記を乱用することがある。

1. 変数 x の範囲を限定せずに命題 $P(x)$ を参照する場合には、命題 $P(x)$ が文脈上意味のある範囲で x の範囲が限定されているものとする。

2. 設定が不明な場合には、文脈上もっとも尤もらしい解釈で理解すること。

3. 設定に不備や矛盾がある場合には、文脈上もっとも尤もらしい修正を施して理解すること。

4. $\#A$ により集合 A の要素数 $|A|$ を表す。誤って $\sharp A$ と書くこともある。

5. 集合 A, B に対して、$A \neq B, A \subset B$ であるとき、$B - A$ で B から A に含まれる要素を除いた集合を表す。

6. 確率 $\Pr(X = x|Y = y)$ を $P_{X|Y}(x|y)$ などと書く。さらに文脈から確率変数が明らかな場合には、$p(x|y)$ などと書く。

7. $x_1, \ldots, x_n$ を x_1^n または x^n と書くことがある。

8. "$y := x$" は "x を y と書くこととする" を意味する。

9. 読点 "、" とコンマ ", " を混在して使用する。

10. 句点 “。” とピリオド “. ” を混在して使用する。

11. y が x から決定されることを強調するときには、$y(x)$ と書く。

12. 数ベクトル $\mathbf{x} = \vec{x} = (x_1, \dots, x_n)$ がベクトルであることを強調したくないときには、単に $x = (x_1, \dots, x_n)$ と書くことがある。

13. 数ベクトル $\vec{x} = (x_1, \dots, x_n)$ を、$x_1 \cdots x_n$ と書くことがある。例：(0,0,0)=000

14. 証明において、“A を仮定する” と述べた場合には、背理法の使用とその仮定 A を宣言している。

15. “任意の” を省略することがある。例：(任意の)$x \in \mathbb{R}$ に対して $e^{\sqrt{-1}x} = \cos x + \sqrt{-1}\sin x$ が成り立つ。

16. “A, B” で “A と B” または “A および B” を表す。“A, B” で “A または B” を表すことはない。

17. 文脈から明らかな場合には、写像の表記に現れる $\mapsto$ と $\to$ を区別しないで使用する。例：$f : x \to f(x)$

18. 文脈から明らかな場合には、$A \subset B$ を $A \leq B$ と書くことがある。,

19. 自然数の集合 $\mathbb{N} := \{1, 2, 3, \dots\}$

20. 整数の集合 $\mathbb{Z} := \{0, \pm 1, \pm 2, \dots\}$

21. 実数の集合を $\mathbb{R}$、有理数の集合を $\mathbb{Q}$、複素数の集合を $\mathbb{C}$ と書く。

22. 数列：$n \in \mathbb{N}$ に対して $x_n \in X$ となる $(x_1, x_2, \dots,)$ を X 上の点列または X 点列といい、$(x_n)_{n=1}^{\infty}$ または $\{x_n\}_{n=1}^{\infty}$ または (x_n) または $\{x_n\}$ と書く。

23. 命題 A が真であるとき 1、偽であるとき 0 となる関数を $\mathbb{1}[A]$ と書く。

□

1 冗長性とは何か

符号理論が扱う中心的課題は「情報の信頼性」である．すなわち，送信者が伝えた情報を受信者が誤りなく再現できるようにすることである．雑音や劣化により誤りが生じても，冗長性を加えた符号化や誤り訂正によって正しい情報を回復する．[2] 符号理論の核心にあるのは「冗長性 (redundancy)」である．冗長性とは，本来伝えたい情報に加えて余分な情報を付け加えることを指す．一見ムダに思えるが，これによって誤り

[2] これに対し，暗号理論が扱う中心的課題は「情報の秘匿性」である．これは，通信路を盗聴されても内容を理解されないようにすることであり，符号理論の信頼性とは本質的に異なる．符号化は「正しく届くこと」を保証するのに対し，暗号化は「内容が漏れないこと」を保証する．

を検出したり訂正したりできる．まずは日常生活における身近な例を見てみよう．

- **日付と曜日**:「2025 年 9 月 28 日（日曜日）」と書けば，日付と曜日のどちらかが間違っていても気づける．
- **クレジットカード番号**: 16 桁のうち最後の 1 桁はチェックディジット（Luhn アルゴリズム）であり，入力誤りを検出できる．
- **会話の繰り返し**:「右右右右右右！」のように，人間も自然に冗長性を加えて聞き漏らしによる情報損失を防いでいる．

これらの例から分かるように，冗長性は単に「情報を増やす」だけではなく，誤りを検出・訂正して信頼性を高めるために必須の仕組みである．

定義 1.1 (符号理論の扱う技術)**.** 符号理論は，情報が物理媒体に載って伝送・記録されるときに避けられないノイズや劣化を克服するための技術を扱う．

- 応用例（通信）：情報は電波や光ファイバといった媒体を通じて伝送される．電波は大気・建物による減衰やマルチパス干渉を受け，光ファイバは散乱・吸収によって信号が劣化する．物理層では，変調信号に冗長性を加えて送信し，受信側で誤り訂正を行うことで信頼性を確保

する．具体例として，衛星通信の RS 符号，携帯電話の畳み込み符号や Turbo 符号，そして 5G で採用された LDPC 符号や Polar 符号がある．これにより，雑音の多い空間伝送媒体でも安定した通信が可能となる．

- 応用例（記録）：情報は半導体メモリセル，磁気ディスク，光ディスクなどの物理媒体に保存される．DRAM や SRAM のセルは熱雑音や放射線でビット反転を起こし，磁気・光ディスクは傷や経年劣化で読み取りエラーが生じる．ECC メモリではハミング符号や BCH 符号を用いて物理素子レベルでの誤りを訂正する．SSD ではフラッシュセルの電荷劣化に対抗するため LDPC 符号が，CD・DVD では RS 符号が使われ，傷や汚れを補償する．このように，記録媒体の不完全さを前提として符号理論が導入されている．

- 応用例（コンピュータ）：情報は計算機の内部で論理回路を通じて処理される．プロセッサ内部のレジスタや演算器も物理素子であり，微小なノイズや放射線によるソフトエラーでビット反転が生じることがある．このため，演算中のデータにも冗長性が付加される．例として，

  – 命令やデータバスのパリティチェック，
  – 高信頼サーバで用いられる ECC レジスタ，
  – スーパーコンピュータやデータセンター向け GPU に搭載される ECC メモリ（NVIDIA A100/H100

などの HPC GPU では HBM メモリやキャッシュに SECDED ECC を導入し，単一ビット誤り訂正と二重ビット誤り検出を行う NVIDIA Hopper Whitepaper），

– 航空宇宙用途などで使われる三重化回路（TMR: Triple Modular Redundancy）

特に GPU は AI 学習や科学シミュレーションに広く利用されており，数十 GB 規模の大容量メモリを扱うためソフトエラーの影響を受けやすい．そのため HPC 向け GPU（例：NVIDIA A100/H100）は ECC メモリを標準搭載し，行リマッピングやページオフライニングによって訂正不能エラーの影響を限定化している．一方，ゲーミング用途 GPU では性能やコストを優先して ECC が省略されることが多い．

- 応用例（量子コンピュータ）：ノイズが多い物理量子ビットから，量子誤り訂正によって論理量子ビットを構成する．現在の量子コンピュータは様々な物理プラットフォームで研究開発が進められている：

  – 超伝導量子ビット（マイクロ波共振器で結合しゲート操作を行う），

  – イオントラップ量子ビット（レーザー冷却したイオンの内部準位を利用），

– 半導体量子ドット（電子スピン状態を用いる），
– 光量子ビット（光子の偏光や時間ビンを利用）

などが代表例である．いずれの実装においても，環境との相互作用によるデコヒーレンスにより，位相反転エラーやビット反転エラーが高頻度で生じるため，そのままでは大規模計算に利用できない．多数の不完全な物理量子ビットを符号化することで，安定した論理量子ビットを構成することが可能となる．

関連講義との関連

- 講義「通信理論」で学習したこと：通信路容量、通信路符号化定理、ランダム符号化
- 本講義で勉強すること：現実的な符号化法（通信路容量には達成しません）
- 大学院の講義「情報通信理論」で勉強すること：現実的な符号化法で通信路容量を達成する方法

□

2　線形とは限らない２元符号 @01

この節では，符号理論の基本的な問題設定を導入し，最も単純な場合として**線形とは限らない２元符号**を考える．符号理論の目的は，通信路における誤りの影響をできるだけ小さくしながら，限られた通信回数でできるだけ多くの情報を確実に伝送することである．

まず，符号器・復号器・通信路の三要素からなる**符号理論の基本設定**を定義し，メッセージ空間・符号空間・通信路モデルの関係を明確にする．次に，符号の良さを測る指標として**符号化率（code rate）**を導入し，いくつかの具体例によって符号の構成とそのパラメータを理解する．

この節の目標は，符号がどのように設計され，何をもって良い符号とみなすかを把握することである．

定義 2.1 (符号理論の扱う問題の設定)**.** 符号理論では以下の問題の設定を扱う

1. 送信者は受信者にメッセージ $m \in \mathcal{M} = \{0, \ldots, M-1\}$ を誤り無く伝えたい。$M = 2^k$ の場合、メッセージは長さ k のベクトルで[3]表わされる。

   例：$M = 2^3 = 8$,

   $$\begin{aligned} m &= 0 = (000), \\ m &= 1 = (001), \\ m &= 2 = (010), \\ &\vdots \\ m &= 7 = (111) \end{aligned}$$

   メッセージ m は、文脈によって、情報ベクトルまた単に情報、またはユーザデータと呼ばれることがある。

2. 送信者は、k ビットのメッセージ $m \in \mathcal{M}$ を符号語とよばれる長さ n の 2 元ベクトル

   $$c = c(m) = (c_1, \ldots, c_n) \in \{0,1\}^n =: \mathbb{F}_2^n$$

[3]ベクトル空間の元をベクトルと呼ぶので、一般に、$x \in X$ をベクトルと呼ぶ場合には X がベクトル空間であることが想定されている。後で分かることだが実際、$\{0,1\}^n$ はベクトル空間をなす。

にある決められた方法で写像する。この写像 $m \mapsto c$ を符号化といい、符号化が実装された装置を符号器という。2元ベクトル c を符号語といい、符号語を集めたもの、つまり符号化の像

$$C(\mathcal{M}) := \{c(m) \mid m \in \mathcal{M}\}$$

を符号空間または単に符号という。符号語の長さ n を符号長といい、$n(C)$ と書く。符号長は通信路の使用回数に一致する。

例：1ビットの情報ビット m を3回繰り返したものを符号語 $c(m)$ とする。

$$c(0) = 000, c(1) = 111$$

例：3ビットの情報ビット系列 m に1の数が偶数個になるように1ビットを付け加えて符号語 c とする。

$$c(000) = 0000, c(001) = 0011, c(010) = 0101,$$
$$c(011) = 0110, c(100) = 1001, c(101) = 1010,$$
$$c(110) = \boxed{1100}, c(111) = \boxed{1111},$$

3. 通信路は、符号語 $x = (x_1, \ldots, x_n) \in \{0,1\}^n$ を入力されると出力

$$y = (y_1, \ldots, y_n) \in \{0,1\}^n$$

をランダムに出力する。ランダムネスは一般に条件付き確率 $P_{Y|X}(y|x)$ によって記述される。符号語は、送信語とも呼ばれる。出力 y は受信語とも呼ばれる。通信路は、入出力の遷移確率 $P_{Y|X}(y|x)$ によって規定されるので、$P_{Y|X}(y|x)$ を通信路と呼ぶことがある。

例：符号語 $x = 000$ が入力されると、通信路で 1 ビット以下の誤りが一様ランダムに発生して、出力

$$y = \boxed{000}, \boxed{100}, \boxed{010}, 001$$

が出力される。

例：符号長 $n = 3$ として、符号語 $\vec{c} = 101$ が入力されると、各ビット確率 $p = 0.01$ で独立に反転した出力 $\vec{y}$ が出力される。最も高い確率 $\boxed{0.99^3}$ で出力されるのは、

$$\vec{y} = \boxed{101}$$

である。2 番目に高い確率 $\boxed{0.01 \times 0.99^2}$ で出力されるのは、以下の三つで、

$$\vec{y} = \boxed{001}, \boxed{111}, 100$$

最も低い確率 $\boxed{0.01^3}$ で出力されるのは、

$$\vec{y} = \boxed{010}$$

である。

4. 受信者は、受信語 y から、推定符号語 $\hat{c} = (\hat{c}_1, \ldots, \hat{c}_n) \in C$ を推定する。この写像 $y \mapsto \hat{c}$ を復号化といい、復号化が実装された装置を復号器という。正しく復号できないことを、復号誤りという。

この設定において、次の条件をできるだけ満たして、

1. できるだけ少ない通信路の使用回数 n で
2. できるだけ大きなサイズ M のメッセージを
3. できるだけ少ない復号誤り確率 $\Pr(c \neq \hat{c}(y))$ で

送信者がメッセージを受信者に伝えることができる、

1. 符号空間 C
2. 符号器 $c : m \mapsto c(m)$
3. 復号器 $\hat{c} : y \mapsto \hat{c}(y)$

を設計することが**符号理論の目的**である。 □

定義 2.2 (符号化率)**.** 与えられた符号長 n の符号空間 C に対して、上の望みを測る指標を導入する。多くの情報を扱いたいので、情報ビット系列のビット数 $k = \log_2 |C|$ は大きい方が望ましい。一方、コストがかかるので通信路の使用回数 n は小さい方が望ましい。この要求に対する尺度を、以下で定義する。

$$R = \frac{1}{n} \log_2 |C|$$

この尺度は、符号化率と呼ばれ、大きいほど望ましい。 □

例 2.3. C を以下の行列の行ベクトル $\vec{c}_i$ を符号語として有する符号空間とする。

$$
\begin{array}{l}
11101111111001010000\\
10101110011110001100\\
01110111100011011000\\
10010011110000010111\\
11000110100101010000\\
11010101110001011010\\
10110100110101001110\\
11001110101101001010
\end{array}
$$

符号長は $n(C) = \boxed{20}$、符号語数は $M = \boxed{8}$、符号化率は $R(C) = \boxed{\frac{1}{20}\log_2(8)} = \boxed{3/20}$ となる. □

3 線形とは限らない２元符号のための復号法

この節では，前節で導入した２元符号に対して，**復号（decoding）**の基本的な考え方を学ぶ．まず，２元ベクトル間の距離を定める**ハミング距離**を導入し，符号の性質を特徴づける**最小距離**の概念を定義する．その後，受信語から送信語を推定する各種の復号法を説明する．

特に，確率的観点から最適とされる**最大事後確率復号（MAP 復号）**と，多くの実用的通信路で等価となる**最尤復**

号（ML 復号）を導入し，MAP 復号が復号誤り確率を最小にすることを証明する．さらに，最尤復号が最適となるための条件を示し，後に扱う線形符号や LDPC 符号の復号法の基礎を準備する．

定義 3.1 (ハミング距離、最小距離)**.** $\mathbb{F}_2 := \{0,1\}$ とする。ベクトル x, y に対して異なる成分の数を $d(x,y)$ とする。正確に書くと、

$$d(x,y) = \#\{1 \le i \le n \mid x_i \neq y_i\}$$
$$x = (x_1, \ldots, x_n), y = (y_1, \ldots, y_n) \in \mathbb{F}_2^n$$

である。距離関数 $d(\cdot,\cdot)$ によって $(\mathbb{F}_2^n, d)$ は距離空間となる(あとで証明します)。$d(x,y)$ を x, y の間のハミング距離または単に距離という。
例：$d((101111),(111011)) = \boxed{2}$ □

証明. $(\mathbb{F}_2^n, d)$ が距離空間となるための条件のうち、

非負値性 :	$d(x,y) \ge 0,$
非退化性 :	$x = y \Leftrightarrow d(x,y) = 0,$
対称性 :	$d(x,y) = d(y,x)$

は自明なので、残りの三角不等式

$$d(x,y) + d(y,z) \ge d(x,z)$$

だけを証明する。$\vec{x}, \vec{y}, \vec{z} \in \mathbb{F}^n$ を長さ n のベクトルとする。集合 $D(\vec{x}, \vec{y})$ を以下のように定義することで、以下が成り立つ。

$$
\begin{aligned}
D(\vec{x}, \vec{y}) &= \{1 \leq i \leq n \mid x_i \neq y_i\} \\
d(\vec{x}, \vec{y}) &= |D(\vec{x}, \vec{y})|
\end{aligned}
$$

これより、以下が成り立つ。

$$
\begin{aligned}
d(\vec{x}, \vec{z}) &= |D(\vec{x}, \vec{z})| \\
&\leq |D(\vec{x}, \vec{y}) \cup D(\vec{y}, \vec{z})| && (3.2) \\
&\leq |D(\vec{x}, \vec{y})| + |D(\vec{y}, \vec{z})| && (3.3) \\
&= d(\vec{x}, \vec{y}) + d(\vec{y}, \vec{z})
\end{aligned}
$$

(3.2) は

$$D(\vec{x}, \vec{z}) \subseteq D(\vec{x}, \vec{y}) \cup D(\vec{y}, \vec{z})$$

より明らかであるが、これは、

$$[x_i \neq z_i \text{ならば } (x_i \neq y_i \text{または } y_i \neq z_i)] \tag{3.4}$$

と書き換えられる。これが成り立つのは、(3.4) の対偶

$$\boxed{[(x_i = y_i \text{かつ } y_i = z_i) \text{ ならば } x_i = z_i]}$$

を考えれば明らか。(3.3) では、一般に集合 D_1, D_2 に対して成り立つユニオン限界[4]

$$|D_1 \cup D_2| \leq |D_1| + |D_2|$$

[4] $|A \cup B| = |A| + |B| - |A \cap B| \leq |A| + |B|$

を使用した。 □

符号空間 C に対して、C に属する異なる符号語 $\vec{c}_1$, $\vec{c}_2$ のハミング距離の最小値を最小ハミング距離とまたは単に最小距離と呼び $d_{\min}(C)$ または単に $d(C)$ と書く。正確に書くと、符号 C の最小ハミング距離 $d_{\min}(C)$ は

$$d_{\min}(C) = \min_{\vec{c}_1,\vec{c}_2 \in C : \vec{c}_1 \neq \vec{c}_2} d(\vec{c}_1, \vec{c}_2)$$

となる。

例 3.5. C を以下の行列の行ベクトル $\vec{c}_i$ を符号語として有する符号空間とする。

```
11101111111001010000
10101110011110001100
01110111100011011000
10010011110000010111
11000110100101010000
11010101110001011010
10110100110101001110
11001110101101001010
```

以下の表はハミング距離 $d(\vec{c}_i, \vec{c}_j)$ を (i, j) 成分に配置している。$*=\boxed{5}$ なので、この表から C の最小距離 $d_{\min}(C) = \boxed{5}$ で有ることが分かる。

```
 0  9  7 10  6  7 11  7
 9  0 12 13 11 14  8  8
 7 12  0 11  7  6 10 10
10 13 11  0 10  7  9 13
 6 11  7 10  0  7  9  *
 7 14  6  7  7  0  6  8
11  8 10  9  9  6  0  8
 7  8 10 13  *  8  8  0
```

□

例 **3.6** (符号語数と最小距離のトレードオフ)**.** 一般に、符号空間の最小距離 $d_{\min}$ と、符号語数 M はトレードオフの関係にある。C を以下のベクトル $\vec{c}_i (i = 1, \ldots, M)$ を符号語として有する符号空間 C は、符号語数 $M = 16$、最小距離 $d_{\min} = 3$ を有する。符号語数 M を増やそうと考えて C に新たに符号語 1011000 を追加しても 1110000 との距離が 3 より小さくなってしまい、最小距離は $d_{\min} = 3$ より小さくなってしまう。

```
0000000 1000110 0100011 1100101
0010101 1010011 0110110 1110000
0001111 1001001 0101100 1101010
0011010 1011100 0111001 1111111
```

3.19 で説明することから、最小距離が大きいとより多くの誤りを訂正することができる。できるだけ良い符号語数と最小距離に関するトレードオフを与える符号空間を構成したい。□

定義 3.7 (事後確率、尤度、事前確率)**.** 推定に関わる一般的な設定において、推定の対象 θ と独立とは限らない観測値 x に対して、$P_{X|\Theta}(x|\theta)$ を尤度、$P_\Theta(\theta)$ を事前確率、$P_{\Theta|X}(\theta|x)$ を事後確率という。符号理論の設定では、推定の対象 θ は符号語 c、観測値 x は受信語 y に対応する。 □

変数と対応する確率変数が文脈から明らかな場合には $\Pr_{\vec{C}|\vec{R}}(\vec{c} \mid \vec{r})$ を $p(\vec{c} \mid \vec{r})$ と書く。

定義 3.8 (最大事後確率復号法、最尤復号)**.** 受信語 $\vec{r}$ に対して、実際の送信語が $\vec{c}$ である確率 $p(\vec{c} \mid \vec{r})$（$\vec{c}$ の事後確率）を最大にする符号語 $\hat{\vec{c}}^{(\mathrm{MAP})}(\vec{r})$ を復号の結果とする復号法を最大事後確率復号法と呼ぶ。正確に書くと

$$\hat{\vec{c}}^{(\mathrm{MAP})}(\vec{r}) = \operatorname*{argmax}_{\vec{c} \in C} p(\vec{c} \mid \vec{r})$$

である。

送信語 $\vec{c}$ が送られた条件で受信語が $\vec{r}$ である確率 $p(\vec{r} \mid \vec{c})$（$\vec{c}$ の尤度）を最大にする符号語 $\vec{c}$ を復号の結果とする復号法を最尤復号法と呼ぶ。正確に書くと

$$\hat{\vec{c}}^{(\mathrm{ML})}(\vec{r}) = \operatorname*{argmax}_{\vec{c} \in C} p(\vec{r} \mid \vec{c})$$

である。 □

命題 3.9 (最大事後確率復号の**最適性**)**.** 一般に、有限値確率変数のペア $(X, Y), X \in \mathcal{X}, Y \in \mathcal{Y}$ に関して、$Y = y$ を観測したもとで、X の推定値 $\hat{x}(y)$ を推定することを考える。このと

き、誤り確率 $\Pr(X \neq \hat{x}(Y))$ を最小にする推定 $\hat{x} : y \mapsto \hat{x}(y)$ は以下で与えられる。

$$\hat{x}(y) = \operatorname*{argmax}_x \Pr(X = x | Y = y)$$

これを、符号理論の設定に適用すると以下を得る。**最大事後確率復号はあらゆる復号法の中で最小の復号誤り確率を与える**ことが分かる。 □

証明. $\Pr(X \neq \hat{x}(Y)) = 1 - \Pr(X = \hat{x}(Y))$ なので、$\Pr(X = \hat{x}(Y))$ を最大にする $\hat{x} : y \mapsto \hat{x}(y)$ を考える。任意の推定 $\hat{x}$ に関して、以下が成り立つ。

$$\begin{aligned}
&\Pr(X = \hat{x}(Y)) \\
&= \sum_{x \in \mathcal{X}, y \in \mathcal{Y}} \mathbb{1}[\hat{x}(y) = x] \Pr(X = x, Y = y)
\end{aligned}$$

ただし、$\mathbb{1}[A]$ は命題 A が真であるとき 1、偽であるとき 0 となる関数である。さらに、

$$\begin{aligned}
&\Pr(X = \hat{x}(Y)) \\
&= \sum_{x \in \mathcal{X}, y \in \mathcal{Y} : \hat{x}(y) = x} \Pr(X = x, Y = y) \\
&= \sum_{y \in \mathcal{Y}} \Pr(X = \hat{x}(y), Y = y) \\
&\leq \sum_{y \in \mathcal{Y}} \max_{x \in \mathcal{X}} \Pr(X = x, Y = y)
\end{aligned}$$

を得る。ここで、

$$\hat{x}(y) = \operatorname*{argmax}_{x \in \mathcal{X}} \Pr(X = x, Y = y)$$

とすると、上の不等号を等号で満たすことが分かる。さらに以下のように変形して、証明が完成する。

$$\begin{aligned}\hat{x}(y) &= \operatorname*{argmax}_{x \in \mathcal{X}} \Pr(X = x, Y = y) \\ &= \operatorname*{argmax}_{x \in \mathcal{X}} \Pr(X = x | Y = y) \Pr(Y = y) \\ &= \operatorname*{argmax}_{x \in \mathcal{X}} \Pr(X = x | Y = y)\end{aligned}$$

最後の等号では argmax の結果に $P_Y(y)$ が影響しないことを用いた。 □

@02

命題 3.10 (最尤復号が最適になる十分条件)**.** 事前確率が一様である、言い換えると送信語が符号の中から一様な確率で選ばれる場合には、最大事後確率復号と最尤復号は同じ復号結果を与える。

ユーザーデータは情報源符号化によって一様分布になるように圧縮することができるので、事前確率が一様分布であることを仮定することは妥当である。 □

証明. 任意の事前分布 $P_X(x)$ に対して、以下が成り立つ。

$$\begin{aligned}\hat{x}^{(\mathrm{MAP})}(y) &= \operatorname*{argmax}_{x\in C} P_{X|Y}(x|y) \\ &= \operatorname*{argmax}_{x\in C} P_{Y|X}(y|x)P_X(x)/P_Y(y) \\ &= \operatorname*{argmax}_{x\in C} P_{Y|X}(y|x)P_X(x)\end{aligned}$$

第 2 等号では条件付き確率の定義を、第 3 等号では argmax の結果に $P_Y(y)$ が影響しないことを用いた。ここで、一様な事前確率 $P_X(x) = 1/|C|$ を代入すると、

$$\begin{aligned}\hat{x}^{(\mathrm{MAP})}(y) &= \operatorname*{argmax}_{x\in C} P_{Y|X}(y|x)/|C| \\ &= \operatorname*{argmax}_{x\in C} P_{Y|X}(y|x) \\ &= \hat{x}^{(\mathrm{ML})}(y)\end{aligned}$$

となり、証明が完成する。 □

次にハミング距離を用いた復号法を定義する。これが最尤復号法と一致することを 3.14 で示す。

定義 3.11 (最小距離復号、minimum distance decoding)**.** 受信語 $\vec{r}$ とのハミング距離が最小になる[5]符号語 $\vec{c}$ を復号結果と

[5]受信語 $\vec{r}$ とのハミング距離が最小になる符号語が複数ある場合にはその中の一つをランダムに選ぶ

する復号法を最小距離復号法と呼びその復号結果を $\hat{\vec{c}}^{(\mathrm{MD})}(\vec{r})$ と書く。正確に書くと、

$$\hat{\vec{c}}^{(\mathrm{MD})}(\vec{r}) = \operatorname*{argmin}_{\vec{c}\in C} d(\vec{c},\vec{r})$$

である。他の教科書では復号半径 $\left\lfloor \frac{d(C)-1}{2} \right\rfloor$ の限界距離復号 (参照 3.17) を最小距離復号と呼ぶことがあるが、これは上の定義とは異なるので注意しよう。 □

定義 3.12 (無記憶通信路、2 元対称通信路)**.** 送信語 $\vec{c} = (c_1, \ldots, c_n)$, 受信語 $\vec{r} = (r_1, \ldots, r_n)$ とする。このとき、各入力と出力の尤度の積に分解できる、すなわち

$$p(\vec{r} \mid \vec{c}) = p(r_1 \mid c_1) \cdots p(r_n \mid c_n)$$

であるとき、その通信路 $p(\vec{r} \mid \vec{c})$ は無記憶通信路であるという。i 番目の送受信関係が過去の送受信に依存しないことから無記憶と呼ばれる．これ以降、断らなければ通信路は無記憶であるとする。

$r_i, c_i \in \mathbb{F}_2$ に対して、以下の遷移確率によって定義される無記憶通信路を 2 元対称通信路と言い、p を反転確率またはクロスオーバー確率という。

$$p(r_i|c_i) = \begin{cases} p, & (r_i \neq c_i) \\ 1-p, & (r_i = c_i) \end{cases}$$

□

例 3.13. 反転確率 p の 2 元対称通信路に $X = 111100$ を入力して $Y = 000000$ が出力される確率は、

$$p(Y = 000000|X = 111100) = \boxed{p^4(1-p)^2}$$

となる。 □

定理 3.14. 反転誤り確率 $p < 1/2$ の 2 元対称通信路で通信を行うことを考える。このとき、最小距離復号は最尤復号と等しいこと、つまり、以下が成り立つ。

$$\hat{\vec{c}}^{(\mathrm{MD})}(\vec{r}) = \hat{\vec{c}}^{(\mathrm{ML})}(\vec{r})$$

これにより、2 元対称通信路で通信を行う場合に、最尤復号を実現するには最小距離復号をすれば十分であることが分かる。 □

証明. まず、符号長 n の符号 C を反転確率 $p < 1/2$ の 2 元対称通信路で用いたときの符号語 $\vec{c}$ を送信して $\vec{r}$ を受信する尤度は、

$$\begin{aligned} p(\vec{r} \mid \vec{c}) &= p^{d(\vec{c},\vec{r})}(1-p)^{n-d(\vec{c},\vec{r})} \\ &= \left(\frac{p}{1-p}\right)^{d(\vec{c},\vec{r})}(1-p)^n \end{aligned} \tag{3.15}$$

である。従って受信語 $\vec{r}$ を最尤復号した結果は、C の中で $\vec{r}$ と異なるビット数が最小の符号語 $\vec{c}$ となる。$p < 1/2$ より $p/(1-p) < 1$ なので、(3.15) の左辺を最大にする $\vec{c}$ は $d(\vec{c}, \vec{r})$ を最小にする。 □

教員用メモ：次の定理は言及するだけ。詳細は説明しない。

定理 3.16 (通信路符号化定理)**.** 最大事後確率復号の復号誤り率を以下で定義する。

$$P_e^{(\mathrm{MAP})}(C_n) = \Pr(X \neq \hat{x}^{(\mathrm{MAP})}(Y)$$

$R < \max_{P_X} I(X;Y)$ に対して、

$$\lim_{n\to\infty} P_e^{(\mathrm{MAP})}(C_n) = 0$$
$$R(C_n) = R$$

となる符号列 $\{C_n\}$ が存在する。

$R > \max_{P_X} I(X;Y)$ に対して、

$$\lim_{n\to\infty} P_e^{(\mathrm{MAP})}(C_n) = 0$$
$$R(C_n) = R$$

となる符号列 $\{C_n\}$ は存在しない。

すなわち、$\max_{P_X} I(X;Y)$ は誤り確率を 0 にできる符号化率の最大値である。$\max_{P_X} I(X;Y)$ は通信路容量[6]と呼ばれる。□

証明. 通信理論の授業で証明しているはずなので、それを参照してください。 □

[6] $I(X;Y)$ は P_X に関して上に凸な関数になるので、安全に max を使用できる。

定義 3.17 (限界距離復号法)**. 最小距離復号は一般に実装が困難である。以下で定義される限界距離復号法は、実装が比較的容易である。**符号 C を用いて通信を行い受信語 $\vec{r}$ を受信した。$\vec{r}$ から距離 t の範囲に符号語が唯一存在すれば、言い換えると $d(\vec{c},\vec{r}) \leq t$ となる符号語 $\vec{c}$ は複数存在しないならば、それを復号語 $\hat{\vec{c}}_t^{(\mathrm{BD})}(\vec{r})$ とし、見つからなければ復号誤りである error を宣言して復号を中止する。正確に述べると、

$$\hat{\vec{c}}_t^{(\mathrm{BD})}(\vec{r}) = \begin{cases} \vec{c} \in C, & d(\vec{c},\vec{r}) \leq t \text{ となる符号語 } \vec{c} \text{ が} \\ & \text{唯一存在する} \\ \text{error}, & \text{そんな符号語 } \vec{c} \text{ は存在しない} \end{cases}$$

である。この復号法を復号半径 t の限界距離復号法という。□

補題 3.18. 非負整数 $d \geq 1, t \geq 0$ に対して、以下は同値である。

1. $t \leq \lfloor \frac{d-1}{2} \rfloor$
2. $t < d/2$
3. $2t + 1 \leq d$

証明. d を偶奇で場合分けすると、以下を得ることから明らか。

$$\left\lfloor \frac{d-1}{2} \right\rfloor = \begin{cases} d_o & (d = 2d_o + 1) \\ d_e & (d = 2d_e + 2) \end{cases}$$

$$d/2 = \begin{cases} d_o + 1/2 & (d = 2d_o + 1) \\ d_e + 1 & (d = 2d_e + 2) \end{cases}$$

□

命題 3.19 (誤り訂正能力)**.** 最小距離 d の符号 C と非負整数 t を考える。以下が成り立つ。

1. $t \leq \lfloor \frac{d-1}{2} \rfloor$ ならば、半径 t の限界距離復号は、任意の符号語 $c \in C$ を送信した場合に、t 個以下の任意の誤りを訂正することができる。

2. $t \geq \lfloor \frac{d-1}{2} \rfloor + 1$ ならば、半径 t の限界距離復号は、ある符号語 $c \in C$ を送信した場合に、ある t 個以下の誤りを訂正することができない。

以上により、$\lfloor \frac{d-1}{2} \rfloor$ は符号 C に対する限界距離復号法の**誤り訂正能力の指標を与えている**ことが分かる。$\lfloor \frac{d-1}{2} \rfloor$ は C の誤り訂正能力と呼ばれ $t(C)$ と書く。さらに、訂正能力は最小距離 d に応じて大きくなるので、**訂正能力を大きくするためには最小距離を大きくすることが十分であることが分かる。** □

証明. まず、$\lfloor \frac{d-1}{2} \rfloor$ 個以下の誤りを訂正できるを示そう。3.18 より、$t \leq \lfloor \frac{d-1}{2} \rfloor$ は $t < d/2$ と同値である。直感的に説明すると、各符号語から $d/2$ より小さい半径にある受信語の集合に交わりはないので、$d/2$ より少ない数の誤りは訂正できると言うことができる。これは、教室内の人が少なくとも 1 m以上離れて着席していたら、教室内の任意の点から描いた半径 50cm 未満の円に 2 人以上の人は入れないことに対応している。

厳密に証明しよう。異なる 2 つの符号語 $\vec{c}_1, \vec{c}_2$ の $d/2$ より小さい半径に共通して含まれる受信語 $\vec{r}$ が存在したと仮定すると、

$$\begin{aligned} d &\leq d(\vec{c}_1, \vec{c}_2) \ (d \text{ は } C \text{ の最小距離}) \\ &\leq d(\vec{c}_1, \vec{r}) + d(\vec{r}, \vec{c}_2) \ (\text{三角不等式を使用した}) \\ &< \frac{d}{2} + \frac{d}{2} = d \end{aligned}$$

で $d < d$ となり矛盾が導ける。

次に、半径 t の限界距離復号は、$t \geq \left\lfloor \frac{d-1}{2} \right\rfloor + 1$ 言い換えると $t \geq d/2$ なる t に対して、t 個以下の誤りを訂正できないことがあることを示す。最小距離 d を与える符号語ペアを $\vec{c}_1$ と $\vec{c}_2$ と書く。言い換えると、

$$d(\vec{c}_1, \vec{c}_2) = d$$

である。符号語 $\vec{c}_1$ を送信し、$\vec{c}_1$ の中で $\vec{c}_2$ と異なる d 個の要素のうち t 個が $\vec{c}_2$ の要素に変わった受信語 $\vec{r}$ を受信したとする。

例えば、以下のような状況である。

$$\vec{c}_1 = (00000\ 0000\ 0000000)$$
$$\vec{c}_2 = (\overbrace{11111\ 1111}^{d}0000000)$$
$$\vec{r} = (\overbrace{11111}^{t}\overbrace{0000}^{d-t}0000000)$$

$d(\vec{r},\vec{c}_1) = t$, $d(\vec{r},\vec{c}_2) = d - t \overset{(2t\geq d)}{\leq} t$ となるので、$\vec{r}$ は $\vec{c}_1, \vec{c}_2$ からともに t 以内の距離に位置している。これは、$\vec{r}$ から半径 t 以内にすくなくとも 2 つの符号語 $\vec{c}_1, \vec{c}_2$ が存在することを意味するので、復号エラーとなる。 □

例 3.20. 3.5 の符号 C の最小距離は $d_{\min}(C) = 5$ であったから、限界距離復号により、$\boxed{2}$ 個以下の任意の誤りは訂正することができる。例えば、受信語 $\vec{r} = 01000110101101001010$ に対して、復号半径 $t = 2$ とすれば、

$$\hat{\vec{c}}_t^{(\mathrm{BD})}(\vec{r}) = \boxed{11001110101101001010}$$

となる。一方、3 個以上の誤りを訂正しようと考えて復号半径 $t = 3$ としても、最小距離 $d_{\min}(C) = 5$ を与える符号語ペア $\vec{c}_1, \vec{c}_2$ を選ぶ。

$$\vec{c}_1 = \boxed{11001110101101001010}$$
$$\vec{c}_2 = \boxed{11000110100101010000}$$

$\vec{c}_1$ を送ったときに 3 個の誤りが生じて

$$\vec{r} = \boxed{1100011010110101001 0}$$

を受信したとき、$\vec{r}$ を中心とする半径 $t = 3$ のハミング球 $B(\vec{r}, 3)$ の中に $\vec{c}_1, \vec{c}_2$ が存在するので、復号半径 $t = 3$ の限界距離復号器では、復号エラーとなってしまう。 □

例 3.21 (最小距離復号と限界距離復号)**.** 次の長さ 12 の 4 つの行ベクトルからなる符号 C を考えよう。

```
111011111110
010100001010
111001111000
110001110111
```

各符号語ペアのハミング距離は次のようになるので、$d_{\min}(C) = 3, t(C) = 1$ である。

```
0  8  3  4
8  0  7  8
3  7  0  5
4  8  5  0
```

受信語 $\vec{r} = 010101111101$ を受信した。このとき、

$$\hat{\vec{c}}_1^{(\mathrm{BD})}(\vec{r}) = \boxed{\text{error}}$$
$$\hat{\vec{c}}^{(\mathrm{MD})}(\vec{r}) = \boxed{110001110111}$$

となる。この例は、$t = 1$ の限界距離復号では復号誤りとなるが、最小距離復号では正しく復号できる例となっている。 □

4　線形とは限らない符号に関する最小距離に関する限界式

本節では，線形であるかどうかに関わらず，符号の性能を特徴づける**最小距離**に関する基本的な限界式を導く．符号長 n と最小距離 d が与えられたとき，可能な符号語数 M がどの程度まで増やせるかという問いは，符号設計の最も根本的な問題のひとつである．

まず，符号語の分布を幾何学的に捉えるために**ハミング球 (Hamming sphere)** の概念を導入し，空間 $\mathbb{F}_2^n$ における符号語の配置を考察する．この考え方から，符号語が互いに干渉しないための必要条件として**球充填限界 (ハミング限界)** を導き，一方で符号語が空間を完全に覆うための十分条件として**球被覆限界** を得る．さらに，これらの結果をもとに **Varshamov–Gilbert (VG) 限界** を導入し，線形とは限らない符号が存在するための十分条件を与える．

この節の目標は，ハミング距離の幾何学的直感に基づいて，「どのような (n, M, d) の組が実現可能か」を明確に理解することである．

定義 4.1 (限界式)**.** 一般に、興味あるパラメータ群に関する不等式を限界式という。 □

定義 4.2. 符号 C は、以下の条件を満たすとき、(n, M, d) 符号であるという。

1. 符号長が n である。

2. 符号語数が M である。

3. 最小距離が d である。

与えられた符号長に対して、できるだけ大きな符号語数 M と、できるだけ大きな最小距離 d を有する、(n, M, d) 符号を構成することに興味がある。 □

定義 4.3 (ハミング球)**.** ベクトル $\vec{c} \in \mathbb{F}_2^n$ まわりのハミング距離 d 以内のビット系列の集合を $\vec{c}$ を中心とする半径 d のハミング球と言い、$B(\vec{c}, d)$ と書く。正確に書くと、以下の通りである。

$$B(\vec{c}, d) = \{\vec{x} \in \mathbb{F}_2^n \mid d(\vec{x}, \vec{c}) \leq d\}$$

このとき、$|B(\vec{c}, d)|$ は中心 $\vec{c}$ によらず決定され、以下が成り立つ。

$$V(n, d) := |B(\vec{c}, d)| = \sum_{i=0}^{d} \binom{n}{i} \tag{4.4}$$

特に、半径が 0 と n の場合には、それぞれ $V(n, 0) = \boxed{1}, V(n, n) = \boxed{2^n}$ となる。 □

証明. $\vec{c}$ からハミング距離 i だけ離れているベクトルの集合を $S_i(\vec{c})$ と書く。$S_i(\vec{c})$ の各要素は $\vec{c}$ の n 成分のうち i 個を反転することによって生成され、トータルで $\binom{n}{i}$ 個存在する。よって、$|S_i(\vec{c})| = \binom{n}{i}$ となる。各 $i = 0, \ldots, d$ に対して $S_i(\vec{c})$ は交

わりをもたないことと、合併が $B(\vec{c}, d)$ をなすので、(4.4) を得る。 □

次の性質は、ハミング球の要素数とエントロピー関数を結びつける面白い性質である。本講義ではこれ以降使わないので紹介するだけでとどめる。

命題 4.5. $0 \leq \lambda \leq \frac{1}{2}$ に対して、以下が成り立つ。

$$\lim_{n\to\infty} \frac{1}{n} \log_2 V(n, \lfloor \lambda n \rfloor) = H_2(\lambda)$$

H_2 はエントロピー関数である。 □

証明. 本題からそれるので、証明は割愛します。例えば、J. H. Van Lint, Introduction to Coding Theory, p.21 を参照してください。 □

定義 4.6. 符号長 n と最小距離 d を有する符号のうちで最も符号語数の大きな符号に興味がある。この様な符号は最大であるといい $C^*(n, d)$ と書く。さらにその符号語数を $A(n, d)$ または $A_2(n, d)$ と書く。 □

例 4.7. 4.8 に、$\mathbb{F}_2^3$ と $\mathbb{F}_2^4$ の各点に関して、ハミング距離が 1 の点と隣接するようにグラフを描いた。最小距離が 2 となるできるだけ符号語数が多くなるように符号語を選択して符号を構成してみよう。

$$A_2(n = 3, d = 2) \geq \boxed{4}, A_2(n = 4, d = 2) \geq \boxed{8}$$

□

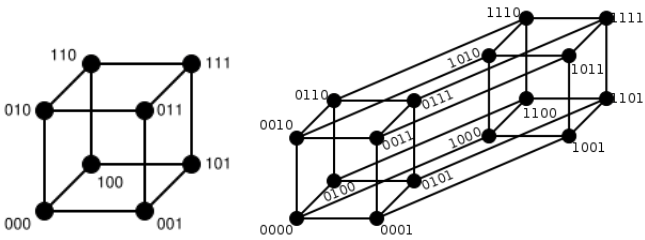


図 4.8: $\mathbb{F}_2^3$ と $\mathbb{F}_2^4$

定理 4.9 (球充填限界、ハミング限界、完全符号)**.** ハミング限界は、線形とは限らない (n, M, d) 符号が存在するための変数組 (n, M, d) に関する必要条件を与える。(n, M, d) 符号 C に対して、以下が成り立つ。

$$M \leq \frac{2^n}{V_2(n,t)} \tag{4.10}$$

ただし、$t = \left\lfloor \frac{d-1}{2} \right\rfloor$ である。最大な符号 $C^*(n,d)$ に関しても、ハミング限界は成立するので、以下が成り立つ。

$$A_2(n,d) \leq \frac{2^n}{V_2(n,t)}, t = \left\lfloor \frac{d-1}{2} \right\rfloor$$

(4.10) を等号で満たす (n, M, d) 符号は完全であると言う。□

証明. C の各符号語からハミング距離 t 以下のベクトル全体は、互いに交わりがない。実際、交わりがあると仮定すると、

3.19 より最小距離が d であることに矛盾する。したがって、ユニオン限界[7]を等式で満たし、

$$\begin{aligned}\#\bigcup_{\vec{c}\in C} B(\vec{c},t) &= \sum_{\vec{c}\in C} \#B(\vec{c},t)\\ &= |C|V_2(n,t)\end{aligned}$$

がなりたつ。左辺の集合は $\mathbb{F}_2^n$ に含まれるまたは $\mathbb{F}_2^2$ と等しいので、

$$2^n \geq |C|V_2(n,t)$$

となり、(4.10) を得る。 □

補題 4.11 (球被覆限界)**.** (n, M, d) 符号 C が最大であるとする。このとき、以下が成り立つ。

$$M \geq \frac{2^n}{V_2(n,d-1)} \tag{4.12}$$

証明. C の各符号語を中心とする半径 $d-1$ のハミング球の合併は $\mathbb{F}_2^n$ 全体を被覆するはずである、つまり

$$\bigcup_{\vec{c}\in C} B(\vec{c},d-1) = \mathbb{F}_2^n$$

となるはずである．実際、そうでないと仮定すると，被覆されていない部分が $\mathbb{F}_2^n$ に存在するはずである。その部分に含まれ

[7] $\#\bigcup_{\vec{c}\in C} B(\vec{c},t) \leq \sum_{\vec{c}\in C} \#B(\vec{c},t)$

るベクトル $\vec{c}'$ を符号語として C に加えた符号を $C' := C \cup \{\vec{c}'\}$ とする。$\vec{c}'$ はどの $\vec{c} \in C$ とも $d(\vec{c}', \vec{c}) \geq d$ となっているので C' の最小距離は d である。C' の符号語数は $|C'| = |C| + 1$ となり，C の最大性に矛盾する．したがって、

$$\begin{aligned} 2^n &= \# \bigcup_{\vec{c} \in C} B(\vec{c}, d-1) \\ &\leq \sum_{\vec{c} \in C} \# B(\vec{c}, d-1) \qquad (4.13) \\ &= |C| V_2(n, d-1) \end{aligned}$$

となり，(4.12) を得る．ここで、不等式 (4.13) はユニオン限界

$$|A \cup B| = |A| + |B| - |A \cap B| \leq |A| + |B|$$

より得られる。 □

定理 4.14 (VG 限界)**.** 以下の条件が成り立つとき、(n, M, d) 符号が存在する。

$$M \leq \frac{2^n}{V_2(n, d-1)} \qquad (4.15)$$

(n, M, d) 符号が存在するための、変数組 (n, M, d) に関する十分条件を与えていることに注意しよう。 □

証明. (4.15) を言い換えると

$$M - 1 < \frac{2^n}{V_2(n, d-1)}$$

である。これが成り立つ $(n, M-1, d)$ 符号に対して、4.11 より $(n, M-1, d)$ 符号 C は最大ではない。したがって、C に最小距離を d に保ったまま符号語を一つ増やすことができる。すなわち、(n, M, d) 符号が存在する。 □

例 **4.16.** (4.15) を等式で満たす (n, M, d) に対して、(n, M, d) 符号は存在する。そのような M は $A_2(n, d)$ を超えないはずである。例をあげると、

$$A_2(n=3, d=2) \geq \frac{8}{\binom{3}{0}+\binom{3}{1}} = \frac{8}{1+3} = 2$$
$$A_2(n=4, d=2) \geq \frac{16}{\binom{4}{0}+\binom{4}{1}} = \frac{16}{1+4} = 3.2$$

となる。4.7 で $A_2(n=3, d=2) \geq 4, A_2(n=4, d=2) \geq 8$ となることがわかっているので、(4.15) が与えた限界式は緊密で無いことが分かる。 □

5　線形符号：有限体をスカラーとする有限次元部分空間 @03

これまでに，線形とは限らない符号の基本構造と限界を学んだ．本節からは，より構造の明確な**線形符号 (linear code)** を扱う．線形符号は，有限体上のベクトル空間の部分空間として定義され，数学的な解析が容易であるだけでなく，実際の通信・記録装置においても極めて重要な役割を果たす．

まず，体や有限体の概念を復習し，特に符号理論で頻繁に用いられる **2 元体** $\mathbb{F}_2$ を定義する．次に，有限体をスカラーとする線形空間（ベクトル空間）の性質を整理し，線形結合・一次独立・基底・次元などの基本概念を導入する．これらの概念が，後に符号の構成や解析にどのように対応するかを理解することが目的である．

この節の目標は，符号を「有限体上の線形空間」として扱うための代数的基礎を整えることである．

定義 5.1 (代数系)**.** 整数の集合 $\mathbb{Z}$ に関して、$a, b \in \mathbb{Z}$ に対して $a+b$ と言う演算 “+” が定義されている。このように、一般に集合 X とその集合上で定義された演算 “ $\circ$ ” または演算の集合に対して、$a, b \in X$ に対して $a \circ b \in X$ となる (閉性が成り立つ) とき組 $(X, \circ)$ を代数系という。
例：$(\mathbb{R}, \{+, -\})$ は代数系である。
例：$(\mathbb{N}, \{+, -\})$ は減算に関して閉じてないので、代数系ではない。 □

定義 5.2 (有限とは限らない体)**.** 四則演算 (加減乗除算) がきちんと[8]定義されている代数系を体という。減算、除算は加算、乗算の逆演算として定義されるので、演算子群から省略されることがある。 □

例 5.3. 体に関する例と反例を挙げる。

1. $(\mathbb{R}, \{+, \times\})$ は体で ある 。
2. $(\mathbb{N}, \{+, \times\})$ は体で ない 。
3. $(\mathbb{Z}, \{+, \times\})$ は体で ない 。
4. $(\mathbb{Q}, \{+, \times\})$ は体で ある 。
5. $(\mathbb{C}, \{+, \times\})$ は体で ある 。
6. (実有理関数全体からなる集合, $\{+, \times\}$) は体で ある 。
7. (2×2 の実行列の集合, $\{+, \times\}$) は体で ない 。

□

定義 5.4 (有限体、要素数が素数の有限体のつくりかた)**.** 有限な体を有限体という。要素数が q である有限体を $\mathbb{F}_q$ と書く。有限体のサイズに興味が無い場合には、$\mathbb{F}_q$ を単に $\mathbb{F}$ と書く。ここでは $\mathbb{F}_p := \{0, 1, \ldots, p-1\}$ 上で定義される四則演算の定

[8] 閉性やゼロ以外による除算可能性や分配則などの性質が成り立つことを意味する。厳密な定義 (https://bit.ly/4hajyh9) はあとで行う。

義を述べる。以下の定義は任意の素数 p に対して有効であるが、この後 $p=2$ の場合に興味が集中するので、$p=2$ に限定してよい。

p を素数として、要素数が p の有限体を $\mathbb{F}_p := \{0, \ldots, p-1\}$ で表記する。その四則演算は以下のように定義すると $\mathbb{F}_p$ は体になる。証明は 26.3 で与える。添字 $\mathbb{Z}$ で整数の四則演算を表し、添字 p で $\mathbb{F}_p$ の四則演算を表す。整数 m, n について $m \bmod n$ を「m を n で割った余り」と定義する。$x, y \in \mathbb{F}_p$ とする。

まず $+_p$ と $\times_p$ を定義しよう。

$$\begin{aligned} x \ +_p \ y &= (x +_{\mathbb{Z}} y) \bmod p, \\ x \ \times_p \ y &= (x \times_{\mathbb{Z}} y) \bmod p \end{aligned}$$

次に、$+_p$ と $\times_p$ の逆演算となる $-_p$ と $/_p$ を定義しよう。

$$\begin{aligned} -_p \, y &= (a +_{\mathbb{Z}} y) \bmod p = 0 \text{ となる } a \in \mathbb{F}_p, \\ x \ -_p \ y &= x +_p (-_p y), \\ 1 \, /_p \, y &= (a \times_{\mathbb{Z}} y) \bmod p = 1 \text{ となる } a \in \mathbb{F}_p, \\ x \, /_p \, y &= x \times_p (1/_p y) \end{aligned}$$

これより，文脈上明らかな場合には演算子の添字 $_p$ を省略する。□

例 5.12. $\mathbb{F}_2$ における演算の例を与える。

1. $1 + 1 = \boxed{0}$

表 5.11: $\mathbb{F}_2$ 上の演算表

$+$	0	1
0	0	1
1	1	0

-	0	1
0	0	1
1	1	0

$\times$	0	1
0	0	0
1	0	1

/	0	1
0	-	0
1	-	1

2. $0-1=$ 1

3. $1/0=$ 定義されていない。

$\mathbb{F}_5$ の加減乗除表を https://chatgpt.com/s/t_68e5f6f465fc8191b08e38c11e8ec879 で見つけることができます。 □

定義 5.13 (線形空間)**.** 体 $\mathbb{F}$ と加群 V[9]に関して次を満たす写像 $\mathbb{F}\times V\ni(a,x)\mapsto a\vec{x}\in V$ が存在するとき V は $\mathbb{F}$ 上のベクトル空間または線形空間であると言う。$a,b\in\mathbb{F},\vec{x},\vec{y}\in V$ に対して、以下が成り立つ。

$$
\begin{aligned}
a(b\vec{x})&=(ab)\vec{x}\\
1\vec{x}&=\vec{x}\\
a(\vec{x}+\vec{y})&=a\vec{x}+a\vec{y}\\
(a+b)\vec{x}&=a\vec{x}+b\vec{x}
\end{aligned}
$$

$\mathbb{F}$ の元をスカラー、V の元をベクトルと言う。 □

[9]足し算と引き算がきちんと定義されている代数系。16 で定義します。

定義 5.14 (有限体をスカラーとする線形空間)**.** $\mathbb{F}$ 上の n 次元数ベクトル空間 $\mathbb{F}^n$ にベクトルに関する和とスカラー倍を自然に定義する。$(x_1, \ldots, x_n), (y_1, \ldots, y_n) \in \mathbb{F}^n$, $a \in \mathbb{F}$ に対して、以下のように定義する。

$$a(x_1, \ldots, x_n) = (ax_1, \ldots, ax_n)$$
$$(x_1, \ldots, x_n) + (y_1, \ldots, y_n) = (x_1 + y_1, \ldots, x_n + y_n)$$

□

例 5.15. $\mathbb{F}_2^n = \{0,1\}^n = \{(\overbrace{0 \cdots 0}^{n}), \ldots, (\overbrace{1 \cdots 1}^{n})\}$ は要素数が 2^n である次元 n の $\mathbb{F}_2$ 上の線形空間をなす。 これによって、$\mathbb{F}_2^n$ の要素をベクトルと呼ぶことができる。 □

例 5.16. $\mathbb{F}_2$ 上の $n(n = 4)$ 次元ベクトル空間 $\mathbb{F}_2^n$ に対して、以下が成り立つ。

1. $(0110) + (0101) =$ $\boxed{(0011)}$
2. $1(0110) =$ $\boxed{(0110)}$
3. $0(0110) =$ $\boxed{(0000)}$
4. $(0110) \times (0101) =$ $\boxed{\text{定義されていない。}}$

□

例 5.17 (有限体をスカラーとする線形方程式)**.** 次を満たす $x_1, \ldots, x_4 \in \mathbb{F}_2$ を求めよ。

$$\begin{pmatrix} 1000 \\ 1011 \\ 1111 \\ 0001 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$

いくつかの基本行変形[10]により、

$$\begin{pmatrix} 1000|1 \\ 1011|0 \\ 1111|1 \\ 0001|0 \end{pmatrix} \xrightarrow{\text{前進消去}} \begin{pmatrix} 1000|1 \\ 0111|0 \\ 0011|1 \\ 0001|0 \end{pmatrix} \xrightarrow{\text{後退代入}} \boxed{\begin{pmatrix} 1000|1 \\ 0100|1 \\ 0010|1 \\ 0001|0 \end{pmatrix}}.$$

となる。よって、$(x_1, \ldots, x_4) = \boxed{(1110)}$ である。 □

定義 5.18 (線形結合)**.** ベクトルの集合 $A := \{\vec{v}_1, \ldots, \vec{v}_n\}$ と $a_1, \ldots, a_n \in \mathbb{F}$ に対して、

$$a_1\vec{v}_1 + \cdots + a_n\vec{v}_n$$

を $a_1, \ldots, a_n$ を係数とする A の線形結合と言う。 □

定義 5.19 (有限ベクトル系に対する一次独立)**.** $\mathbb{F}$ 上の線形空間 V と $\vec{v}_1, \ldots, \vec{v}_n \in V$ に対して、以下が成り立つとき、$\vec{v}_1, \ldots, \vec{v}_n$

[10] https://ja.wikipedia.org/wiki/行列の基本変形

は一次独立または線形独立であるといい、そうでないとき一次従属または線形従属であると言う。

$$\begin{aligned}&\text{for all } a_1,\dots,a_n \in \mathbb{F},\\ &(a_1\vec{v}_1+\cdots+a_n\vec{v}_n=0 \implies a_1=\cdots=a_n=0)\end{aligned}$$

□

定義 5.20 (次元)**.** $\mathbb{F}$ 上の線形空間 V の一次独立となるベクトルの個数の最大値が存在するとき、これを V の次元といい、$\dim V$ と記す。 □

定義 5.21 (生成系、完全)**.** 線形空間 V のベクトルの集合

$$G=\{\vec{g}_1,\dots,\vec{g}_n\}\subset V$$

に関して、任意の $v\in V$ が G の線形結合で表すことができるとき、正確に述べると以下が成り立つとき、G は V の**生成系**または**完全系**であると言う。任意の $v\in V$ に対して係数 $a_1,\dots,a_n\in\mathbb{F}$ が存在して以下が成り立つ。

$$v=a_1\vec{g}_1+\cdots+a_n\vec{g}_n \tag{5.22}$$

$v\in V$ に対して、(5.22) のように表すことを v の G による展開という。 □

定義 5.23 (基底)**.** 線形空間 V に対して、部分集合 $B\subset V$ が V の生成系かつ一次独立ならば、B は V の基底であるという。線形空間 V に対して、V の基底は一意とは限らない。

□

命題 5.24. 有限体 $\mathbb{F}$ 上の線形空間 V に対して、以下が成り立つ。

1. サイズ $\dim V$ の一次独立な任意のベクトルの集合は V の基底となる。
2. V の任意の基底 B に対して、$|B| = \dim(V)$ である。
3. $v \in V$ の基底 B による展開は、一意である。
4. V は $\mathbb{F}^{|B|}$ と同型である。つまり、V と $\mathbb{F}^{|B|}$ の間に線形な全単射が存在する。

□

証明. 一般の線形空間に対しても成り立ち、線形代数の授業で学習しているはずです。線形代数の教科書を参照してください。 □

6　線形符号

前節では，有限体をスカラーとする線形空間（ベクトル空間）の性質を学んだ．本節では，その概念を符号理論に応用し，**線形符号 (linear code)** を定義する．線形符号は，符号空間が有限体上の部分空間となるよう設計されたものであり，数学的に解析しやすく，符号化・復号の実装が効率的になるという利点をもつ．

まず，線形符号の基本的な定義を導入し，符号長 n・次元 k・最小距離 d という 3 つの主要パラメータの関係を整理する．続いて，符号の性能を測る指標である**符号化率**を定義し，さらに代表的な線形符号として，**繰り返し符号**と**単一パリティ検査符号**を具体的に扱う．

この節の目標は，線形性という制約が符号にどのような構造的性質と利点をもたらすかを理解することである．これ以降、線形性を符号に課すことで得られる線形符号に関する工学的に有用な機能と性質を明らかにしていく。

定義 6.1 (線形符号、$[n,k]$ 符号)**.** 符号長 n の符号 $C \subset \mathbb{F}^n$ に対して、C が $\mathbb{F}$ 上の線形空間になっているとき、C を $\mathbb{F}$ 上の線形符号という。符号長 n、次元 k の線形符号を $[n,k]$ 符号と呼ぶ。符号長 n、次元 k、最小距離 d の線形符号を $[n,k,d]$ 符号と呼ぶ。(n,M,d) とは異なるので注意しよう。

例: $C = \{000, 111\}$ は $[3,1]$ 線形符号である。

例: $C = \{011, 111\}$ は線形符号ではない。なぜなら $011+111 = 100 \notin C$ が符号からハミ出しているからである。　□

定義 6.2 (符号化率)**.** $\mathbb{F}$ 上の $[n,k]$ 線形符号 C の符号化率は、以下で定義される。

$$R(C) \stackrel{\text{def}}{=} \frac{1}{n}\log_{|\mathbb{F}|}|C| \tag{6.3}$$

$\mathbb{F}$ 上の $[n,k]$ 線形符号 C の符号化率 $R(C)$ に関して以下が成り立つ。

$$R(C) = \frac{k}{n}$$

□

証明. $k = \dim C$ であり、C は $\mathbb{F}^k$ と同型であるから、$|C| = |\mathbb{F}|^k$ となる。これを (6.3) に代入して、証明が完成する。 □

定義 6.4 (繰り返し符号)**.** 以下で定義される基底 B を有する符号を、長さ n の繰り返し符号という。

$$B = \{(\overbrace{1\cdots1}^{n})\}$$

長さ n の繰り返し符号は $[n, k=1, d=n]$ 符号である。
例：長さ 4 の 2 元繰り返し符号は $\{\boxed{(0000)}, \boxed{(1111)}\}$ である。
□

定義 6.5 (単一パリティ検査符号)**.** 以下で定義される、長さ n の符号 C を単一パリティ検査符号という。

$$C = \{x = (x_1, \ldots, x_n) \in \mathbb{F}^n \mid \sum_{i=1}^{n} x_i = 0\}$$

長さ n の単一パリティ検査符号は、$[n, k = n-1, d = 2]$ 符号である。
例：長さ $n = 4$ の単一パリティ検査符号 C の符号語をすべて書き下すと、次の通りである。

$$C = \{0000, 0011, 0101, 0110,$$
$$1001, \boxed{1010}, 1100, \boxed{1111}\}$$

C の基底の一つのとして

$$B = \{1100, 0110, 0011\}$$

がある。線形独立であることは明らかで、C の任意の符号語は B の線形結合で表せることも確かめられる。例として、0101 は 0110+0011 で表せる。
　また、C の基底の一つのとして

$$B = \{1001, 0101, 0011\}$$

もある。 □

7　内積、双対符号，生成行列，パリティ検査行列

前節では，線形符号を有限体上の部分空間として定義し，その基本的な例を見た．本節では，線形符号の構造をより深く理解するために，**内積**と**双対符号**の概念を導入する．これにより，符号間の直交関係を数式的に扱えるようになり，誤り検出や復号理論の基礎となる数理構造を明確にできる．

まず，有限体上で定義される内積を用いて，符号とその直交補空間（双対符号）を定義する．続いて，符号空間を具体的に表現するための行列表現として，**生成行列 (generator matrix)** と**パリティ検査行列 (parity-check matrix)** を導入し，それらが双対関係にあることを示す．これにより,「符号語が符号空間に属するかどうか」を行列演算 $Hx = 0$ によって判定できることがわかる．

この節の目的は，双対性と行列表現を通じて，線形符号の構造とその計算的特徴（符号化・検査・復号）を体系的に理解することである．

定義 7.1 (内積、直交). ベクトル $x, y \in \mathbb{F}^n$ に対して、以下で定義されるものを、用語を乱用して x, y の内積という。

$$\langle \vec{x}, \vec{y} \rangle := x_1 y_1 + \cdots + x_n y_n \in \mathbb{F}$$

さらに、$\langle \vec{x}, \vec{y} \rangle = 0$ となる $\vec{x}, \vec{y}$ は直交するという。

例：$x = (10101), y = (11101)$ に対して、$\langle x, y \rangle = \boxed{1} + \boxed{0} + \boxed{1} + \boxed{0} + \boxed{1} = \boxed{1}$ となり、x, y は直交 $\boxed{\text{しない}}$。

上の定義は、よく使われる内積の定義 (https://bit.ly/3UOZOT4) には当てはまらないので、用語の乱用をしていることに注意しよう。実際、よく使われる内積の定義では $\langle x, x\rangle = 0$ ならば $x = 0$ となる、つまり $x \neq 0$ ならば $\langle x, x\rangle \neq 0$ であるはずだが、$x = \boxed{(1111)}$ とすると $\langle x, x\rangle = 0$ となる。 □

定義 7.2 (双対符号)**.** 線形符号 $C \subset \mathbb{F}^n$ に対して、以下で表される C のすべての符号語と直交するベクトルの集合を C の直交補空間 (用語の乱用をしている) または C の双対符号[11]と言い、$C^\perp$ 書く。

$$C^\perp := \{\vec{x} \in \mathbb{F}^n \mid \langle \vec{x}, \vec{y}\rangle = 0 \text{ for all } \vec{y} \in C\}$$

このとき次が成り立つ. □

例 7.3. 長さ n の繰り返し符号 C と単一パリティ検査符号 D は互いに双対な符号である。 □

証明. まず、$C^\perp \subset D$ を示す。任意の $c = (c_1, \ldots, c_n) \in C$ に対して、C が繰り返し符号であることから、

$$c = (c_1, \ldots, c_1)$$

と表せる。これを用いると、$x = (x_1, \ldots, x_n) \in C^\perp$ は、

$$\langle c, x\rangle = \sum_{i=1}^{n} c_i x_i = c_1(x_1 + \cdots + x_n) = 0, \text{ for all } c_1 \in \mathbb{F}$$

[11] ベクトル空間 V に対する双対空間 V^*(参照 7.2) とは異なる概念なので注意すること。

と等価であることが分かる。$c_1 = 1$ を代入すれば、

$$x_1 + \cdots + x_n = 0$$

となることつまり、$x \in D$ と等価である。よって、$C^\perp = D$ となる。

次に、$D \subset C^\perp$ を示そう。これは今の議論の逆をたどれば明らか。冗長だが、実際にやってみよう。任意の $d = (d_1, \ldots, d_n) \in D$ に対して、$d_1 + \cdots + d_n = 0$ が成り立つ。この d が任意の $c = (c_1, \ldots, c_n) \in C$ に対して、直交すること ($\langle d, c \rangle = 0$) を示せば $d \in C^\perp$ が示せる。C が繰り返し符号であることから、$c = (c_1, \ldots, c_1)$ with $c_1 \in \mathbb{F}$ と表せる。$\langle d, c \rangle = \sum_{i=1}^n d_i c_i = (d_1 + \cdots + d_n)c_1 = 0$, for all $c_1 \in \mathbb{F}$ となり、証明が完了する。 □

命題 7.4 (双対符号の性質)**.** 以下が成り立つ。

1. $\mathbb{F}$ 上の線形符号 C に対して、$C^\perp$ は $\mathbb{F}$ 上の線形符号である
2. $C \cap C^\perp = \{\vec{0}\}$ とは限らない。実際、$C = \{00, 11\} \subset \mathbb{F}^n$ に対して $C^\perp = \{00, 11\}$ なので、$C \cap C^\perp = C$ である。$C = C^\perp$ であるとき、C は自己双対であるという。
3. $\dim C + \dim C^\perp = n$ である：次元定理
4. $(C^\perp)^\perp = C$ である

□

証明. 証明は，実線形空間 V の直交補空間 $V^{\perp}$ に対する証明と同じ様にしてできる。 □

定義 7.5 (生成行列、パリティ検査行列)**.** 線形符号 C の基底のひとつを $\{\vec{g}_1, \ldots, \vec{g}_k\}$ とする。

$$G = \begin{pmatrix} \vec{g}_1 \\ \vdots \\ \vec{g}_k \end{pmatrix}$$

を線形符号 C の生成行列と言う。双対符号 $C^{\perp}$ の基底のひとつを $\{\vec{h}_1, \ldots, \vec{h}_{n-k}\}$ とする。

$$H = \begin{pmatrix} \vec{h}_1 \\ \vdots \\ \vec{h}_{n-k} \end{pmatrix}$$

つまり、$C^{\perp}$ の生成行列を線形符号 C のパリティ検査行列と言う。$\vec{g}_i$ と $\vec{h}_j$ は直交することから、$GH^{\mathsf{T}} = 0$ が成り立つ。□

文脈から誤解の無いときには、行列 G と基底 $\{\vec{g}_1, \ldots, \vec{g}_k\}$ を同一視する。同様に、行列 H と基底 $\{\vec{h}_1, \ldots, \vec{h}_{n-k}\}$ を同一視する。文脈から誤解を生じない場合には、列ベクトル $(x_1, \ldots, x_n)^T$ を行ベクトル $(x_1, \ldots, x_n)$ として、またその逆として書くことがある。

7.4 から双対符号の双対符号は主符号である:$C = (C^{\perp})^{\perp}$ から、次の双対的な性質が成り立つ。

1. C の生成行列 G は C の基底ベクトルを行ベクトルとする行列なので、$C^{\perp}$ のパリティ検査行列 ($C = (C^{\perp})^{\perp}$ の基底ベクトルを行ベクトルとする行列) となる。

2. C のパリティ検査行列 H は $C^{\perp}$ の基底ベクトルを行ベクトルとする行列なので、$C^{\perp}$ の生成行列となる。

3. $C^{\perp}$ の生成行列 $G^{\perp}$ は $C^{\perp}$ の基底ベクトルを行ベクトルとする行列なので、C のパリティ検査行列となる。

4. $C^{\perp}$ のパリティ検査行列 $H^{\perp}$ は $(C^{\perp})^{\perp} = C$ の基底ベクトルを行ベクトルとする行列なので、C の生成行列となる。

例 7.6. 符号長 $n = 7$ の符号 C が次の通り与えられている。

$$C = \{0000000, 0111010, 1100110, 1011100,\\ 1001011, 1110001, 0101101, 0010111\}$$

C に含まれる 3 つのベクトル

$$B = \{1001011, 1100110, 0111010\}$$

は、線形独立であり、C を張る (線形結合が C の任意の要素を B の線形結合で表せる) ので、B は C の基底の一つである。

したがって、

$$G = \begin{pmatrix} 1001011 \\ 1100110 \\ 0111010 \end{pmatrix}$$

は C の生成行列である。 □

次の性質により、与えられたベクトル x が符号 C および $C^{\perp}$ の要素であるかどうかを、行列とベクトル計算によって知ることができる。

命題 7.7. $[n, k]$ 線形符号 C、双対符号 $C^{\perp}$、C の生成行列 G、C のパリティ検査行列 H に対して、以下が成り立つ。

$$x \in C^{\perp} \iff Gx = 0 \tag{7.8}$$

$$x \in C \iff Hx = 0 \tag{7.9}$$

これより，G は $C^{\perp}$ のパリティ検査行列であることと，H は $C^{\perp}$ の生成行列であることが分かる. □

証明. ここでは (7.8) を示す。(7.9) は、H が $C^{\perp}$ の生成行列であることと、$(C^{\perp})^{\perp} = C$ であることから明らか。

まず、$x \in C^{\perp} \Longrightarrow Gx = 0$ を示そう。G の行ベクトル集合を $\{g_1, \ldots, g_k\}$ と書く。$g_i \in C, x \in C^{\perp}$ なので、これらは直交し $\langle g_i, x \rangle = 0$ for $i = 1, \ldots, k$ となる。これを行列とベクトルで表すと、$Gx = 0$ となる。

次に、$x \in C^{\perp} \Longleftarrow Gx = 0$ を示そう。$Gx = 0$ であれば、$\langle g_i, x \rangle = 0$ for $i = 1, \ldots, k$ となる。$\{g_1, \ldots, g_k\}$ は C の基底

であることから、任意の $y \in C$ に対して、$y = \sum_{j=1}^{k} b_j g_j$ と展開できる。ただし、$b_1, \ldots, b_k$ はスカラー $\mathbb{F}$ の元である。

$$\langle y, x \rangle = \langle \sum_{j=1}^{k} b_j g_j, x \rangle = \sum_{j=1}^{k} b_j \langle g_j, x \rangle = \sum_{j=1}^{k} b_j 0 = 0$$

となる。$y \in C$ は任意であるので、$x \in C^{\perp}$ となる。 □

定義 7.10 (線形とは限らない符号の符号化にかかる計算量)**.** 線形とは限らない符号 $C = \{\vec{c}_0, \ldots, \vec{c}_{M-1}\} \subset \mathbb{F}^n$ に対して、メッセージ $m \in \{0, 1, \ldots, M-1\}$ から符号語 $\vec{c} \in C$ への写像は M が大きいときには装置化するのが困難である。実際、$k = 1024$ ビットの情報を送りたいときは、$M = 2^k$ となるが、これを変換表 $m \to \vec{c}_m$ で実現するには、$M \times n$ の表が必要になる。これは、宇宙の全原子に 1 ビットずつ情報を書き込めたとしても足りない[12]。 □

変換表を用いずに、生成行列とベクトルの積によって、符号化を実現することができる。

定義 7.11 (生成行列、生成行列を用いた符号化)**.** $[n, k]$ 線形符号 $C \subset \mathbb{F}^n$ の基底を $\{\vec{g}_1, \ldots, \vec{g}_k\}$、生成行列を G とする。こ

[12] https://bit.ly/47Yx576

のとき情報ベクトル $u = (u_1, \ldots, u_k) \in \mathbb{F}^k$ を

$$uG = (u_1, \ldots, u_k) \begin{pmatrix} g_1 \\ \vdots \\ g_k \end{pmatrix}$$
$$= u_1 g_1 + \cdots + u_k g_k \in C$$

に対応付ける写像は、$\mathbb{F}^k$ から C への一対一である線形写像である。これよ、情報ベクトル u と生成行列 G の積によって、符号化が実現できることが分かる。

□

例 7.12. $[n = 7, k = 3]$ 符号の生成行列を

$$G = \begin{pmatrix} 1001011 \\ 1100110 \\ 0111010 \end{pmatrix}$$

とする。情報ベクトル $u = 000$ は符号語 $c = \boxed{0000000}$ に符号化される。情報ベクトル $u = 111$ は符号語 $c = \boxed{0010111}$ に符号化される。 □

命題 7.13. 次が成り立つ。

1. $[n, k]$ 符号 C のパリティ検査行列 H に対して、フルランクである $k \times n$ 行列 G が $GH^{\mathsf{T}} = 0$ を満たすとき、G は C の生成行列である。

2. $[n, k]$ 符号 C の生成行列 G に対して、フルランクである $n-k \times n$ 行列 H が $GH^{\mathsf{T}} = 0$ を満たすとき、H は C のパリティ検査行列である。

□

証明. 1 を示す。2 は同様に示せる。G の行ベクトルの集合を $\{g_i\}_{i=1}^{k}$ が C の基底となること、すなわち $\{g_i\}$ が独立で、C を張ることを示せば良い。G はフルランクであるので、$\{g_i\}$ は線型独立となる。さらに、$\{g_i\}$ が張る空間の次元は k となる。C の次元は k である。$GH^{\mathsf{T}} = 0$ と (7.9) より g_i は C の符号語となる。したがって、$\{g_i\}$ が張る空間は C に含まれる。これらのことより、G は C の生成行列となることがわかる。 □

基底の冗長性から、生成行列が冗長性を有するのは明らかだが、行列の形で表すと次のようになる。

命題 7.14 (生成行列の冗長性)**.** $k \times n$ 行列 G が符号 C の生成行列であるとする。G とは異なる $k \times n$ 行列 G' が符号 C の生成行列となることがある。$k \times k$ の正則行列 A に対して、AG は C の生成行列となる。 □

証明. A は正則なので、AG の階数は G の階数と等しく k である。AG はフルランクである。$(AG)H = 0$ であるから、7.13 より、AG も C 生成行列となる。 □

閑話休題：パリティ検査行列を使って理解する量子誤り訂正

ここまでで学んだように，線形符号には「双対符号」という概念があり，符号とその双対の間には直交関係が成り立つ．実はこの考え方を少し発展させると，量子情報の理論を使わずとも，量子誤り訂正の基本的な構造を古典符号理論だけで簡潔に説明することができる．
その出発点となるのが，2 つの線形符号 C_X と C_Z の組である．これらが互いの双対と整合するように組み合わされた構造を *CSS (Calderbank–Shor–Steane)* 符号という．CSS 符号は，$C_Z^{\perp} \subset C_X$（または等価的に $C_X^{\perp} \subset C_Z$）という包含関係を満たす 2 つの符号から作られ，対応するパリティ検査行列 H_X, H_Z が直交条件 $H_X H_Z^{\mathsf{T}} = 0$ を満たすように設計される．これらの行列は，それぞれ 位相反転 (Z) 誤り $\mathbf{e}_Z$ とビット反転 (X) 誤り $\mathbf{e}_X$ を検出するために用いられる．
量子状態に、誤りが生じるとその影響はシンドロームとして観測される．Z 型スタビライザの測定結果から得られるシンドロームは $\mathbf{s_Z} = \mathbf{H_X e_X^{\mathsf{T}}}$, X 型スタビライザの測定結果から得られるシンドロームは $\mathbf{s_X} = \mathbf{H_Z e_Z^{\mathsf{T}}}$ と表される．したがって，観測されたシンドローム $(\mathbf{s_X}, \mathbf{s_Z})$ からノイズ $(\mathbf{e}_X, \mathbf{e}_Z)$ の推定値 $(\hat{\mathbf{e}}_X, \hat{\mathbf{e}}_Z)$ を求めることが誤り訂正の目的となる．ここで、量子誤りを訂正するためには、ノイズの推定値 $(\hat{\mathbf{e}}_X, \hat{\mathbf{e}}_Z)$ はノイズと完全に一致している必要はなく次の条件を満たしていれば復号成功となる。

$$\hat{\mathbf{e}}_X + \mathbf{e}_X \in C_X^{\perp}, \quad \hat{\mathbf{e}}_Z + \mathbf{e}_Z \in C_Z^{\perp}$$

これは，古典符号における「シンドローム $\mathbf{s} = H\mathbf{e}^{\mathsf{T}}$ から誤り $\mathbf{e}$ を求める問題」(参照 9) と同じ構造を持っている．
CSS 符号では，それぞれの符号の最小距離を $d_X = \min\{\mathrm{wt}(\mathbf{x}) \mid \mathbf{x} \in C_X \setminus C_Z^{\perp}\}$, $d_Z = \min\{\mathrm{wt}(\mathbf{z}) \mid \mathbf{z} \in C_Z \setminus C_X^{\perp}\}$ と定める．このとき，符号全体の最小距離は $d = \min(d_X, d_Z)$ で表され，$t = \lfloor (d-1)/2 \rfloor$ 個以下の誤りを確実に訂正できる．
つまり，量子誤り訂正とは，直交条件 $H_X H_Z^{\mathsf{T}} = 0$ のもとで，2 つの双対符号の包含関係を保ちながら，観測されたシンドロームから最も尤もらしいノイズを推定する問題として古典符号理論の枠組みで形式化できるのである．

量子誤り訂正理論 若手ワークショップ https://sites.google.com/view/qecminiworkshopjp2025/ の宣伝をする。宿泊費および交通費が支給される

8 ハミング重み @04

前節では，線形符号の構造を生成行列やパリティ検査行列を通じて表現した．本節では，符号の**性能を定量的に評価する指標**として，**ハミング重み (Hamming weight)** を導入する．ハミング重みは，符号語の「1」の個数を数える単純な量だが，符号の誤り検出能力・訂正能力を決定する上で中心的な役割を果たす．

まず，ベクトルのハミング重みと符号全体の**最小ハミング重み**を定義し，それが符号の**最小距離**に一致することを示す．これにより，線形符号では符号語の間の距離をすべて調べなくても，最小重みを求めるだけで訂正能力が分かることが理解できる．

この節の目的は，線形符号の距離的性質を「重み」という観点から把握し，後に扱う復号法や限界式の理論的基礎を整えることである．

定義 8.1 (ハミング重み、最小ハミング重み)**.** ベクトル x の要素のうち、非零の要素の数を x のハミング重みまたは重みといい $w(x)$ と書く。零ベクトルとの距離が重みを与える。す

なわち、以下が成り立つ。

$$w(x) = d(x, 0)$$

例：$w(1010) = d(1010, 0000) = 2$

線形符号 C に対して、C の非零符号語の最小の重み、つまり以下を C の最小ハミング重みまたは単に最小重みといい、$w_{\min}(C)$ または $w(C)$ と書く。

$$w_{\min}(C) := \min_{c \in C : c \neq 0} w(c)$$

□

命題 8.2 (最小距離と最小重みの関係)**.** 線形符号 C の最小距離は C の最小重みに等しい。正確に書くと次の通りである。

$$\min_{x,y \in C : x \neq y} d(x, y) = \min_{c \in C : c \neq 0} w(c)$$

□

証明. 以下より導ける。

$$\begin{aligned}
\min_{x,y \in C : x \neq y} d(x, y) &= \min_{x,y \in C : x \neq y} d(x - y, 0) \\
&= \min_{x,y \in C : x \neq y} w(x - y) \\
&= \min_{x - y \in C : x - y \neq 0} w(x - y) \\
&= \min_{c \in C : c \neq 0} w(c)
\end{aligned}$$

□

例 8.3 (線形符号の最小距離は、最小重みに一致する)**.** C を以下の行ベクトル $\vec{c}_i$ を符号語として有する符号空間 C は、符号語数 $M = 16$、最小距離 $d_{\min} = 3$ を有する。線形とは限らない符号では、最小距離は異なる符号語のペアの距離を測ることが必要である。線形符号ならば、非零符号語の最小重み 3 を求めることで、最小距離を得ることができる。

```
0000000 1000110 0100011 1100101
0010101 1010011 0110110 1110000
0001111 1001001 0101100 1101010
0011010 1011100 0111001 1111111
```

□

9　コセットとシンドローム復号

[13]

定義 9.1 (誤りベクトル)**.** 送信語 $\vec{x} \in \mathbb{F}^n$ と受信語 $\vec{y} \in \mathbb{F}^n$ に対して、

$$\vec{e} := \vec{y} - \vec{x}$$

を誤りベクトルという。
これは、送信語 $\vec{x} \in \mathbb{F}^n$ と誤りベクトル $\vec{e} \in \mathbb{F}^n$ に対して、受信語 $\vec{y} \in \mathbb{F}^n$ が以下のように与えられることを意味している。

$$\vec{y} = \vec{x} + \vec{e}$$

例: 送信語 $\vec{x} = 01010$ に誤りベクトル 01001 が加えられ受信語 $\vec{y} = 00011$ を受信した。 □

定義 9.2 (シンドローム)**.** $\mathbb{F}$ 上の $[n, k]$ 線形符号 C とそのパリティ検査行列 H に対して、以下を定義する。ベクトル $\vec{y} \in \mathbb{F}^n$ に対して、$\vec{s} = H\vec{y} \in \mathbb{F}^{n-k}$ を $\vec{y}$ のシンドロームという。 □

定義 9.3 (転置記号の省略)**.** 文脈から誤解を生じない場合には、列ベクトル $(x_1, \ldots, x_n)^T$ を行ベクトル $(x_1, \ldots, x_n)$ として、またその逆として書くことがある。 □

[13] 来年への教員用メモ：商線形空間と準同型定理は習っているはずなので、シンドロームへの線形写像 $\phi : \mathbb{F}^n \to \mathbb{F}^m, \quad \phi(\mathbf{x}) = H\mathbf{x}^\top$ を定義して、$\mathrm{Ker}(\phi) = C$ と $\mathrm{Im}(\phi)$ がシンドローム空間であることから、準同型定理 $\mathbb{F}^n/C \cong \mathrm{Im}(\phi)$ によってシンプルに説明するのがいいかも。

例 9.4 (シンドロームの計算)**.** パリティ検査行列 H を有する $[7,4]$ 符号 C に関して、$y=(1110111)^T$ のシンドロームは $s=Hy=(\boxed{011})^T$ で与えられる。

$$H=\begin{pmatrix}1110100\\1011010\\1101001\end{pmatrix}$$

□

命題 9.5 (誤りベクトルと受信語は同一のシンドロームを有する。)**.** 符号語 $\vec{x}\in C$ を送信し、誤りベクトル $\vec{e}$が加えられ受信語 $\vec{y}=\vec{x}+\vec{e}$が受信された。誤りベクトル $\vec{e}$ と受信語 $\vec{y}$ は同一のシンドロームを有する。実際、以下が成り立つ。

$$H\vec{y}=H(\vec{x}+\vec{e})=H\vec{x}+H\vec{e}=0+H\vec{e}$$

□

定義 9.6 (同値関係 (equivalent relation))**.** X 上の関係 $R\subset X$ は反射律、推移律、対称律[14]を満たすとき、R は同値関係であるという。
例：親戚であるという人間集合上の関係は、同値関係である。
例：$x,y\in\mathbb{Z}$ に対して、$x-y$ は 3 の倍数である関係 $R_{3\mathbb{Z}}$ は、同値関係である。 □

定義 9.7 (同値類、代表元、商集合)**.** 集合 S の上に同値関係 R が定義されているときには、S の各元 a に対して a に同値であ

[14] http://bit.ly/2AdsqQB

る元を全て集めた集合を考えることができる。この S の部分集合を、a を代表元 (representative) とする同値類 (equivalence class) といい、$[a]$ と書く。

$$[a] := \{x \in S \mid a \sim x\}.$$

集合 S の同値関係 R に関する同値類全体のなす集合を、S を同値関係 R で割った集合、あるいは S の R による商集合と呼び、

$$S/R := \{[x] \mid x \in S\}$$

と表す。商集合は S の分割を与える。言い換えると、$S/R = \{S_1, \ldots, S_n\}$ ならば $S = S_1 \cup \cdots \cup S_n, S_i \cap S_j = \phi$ for $i \neq j$ となる。

例：$\mathbb{Z}/R_{3\mathbb{Z}} = \{[0], [1], [2]\} = \{0 + 3\mathbb{Z}, 1 + 3\mathbb{Z}, 2 + 3\mathbb{Z}\}$ である。ここで、$[i]$ は 3 で割った余りが i である整数の集合と一致する。

例：このクラスの参加者集合を X とする。親戚関係にある人がいなければ、

$$X/\text{親戚関係} = \{\{x\} | x \in X\}$$

となる。 □

定義 9.8 (剰余類、コセット)**.** 符号長 n の $\mathbb{F}$ 上の線形符号 $C \subset \mathbb{F}^n$ に関して、商線形空間[15]、つまり $x - y \in C$ なる同値関係

[15] https://bit.ly/3TY61iB

による分類 (商集合) に自然に線形演算を定義したもの

$$\mathbb{F}^n/C = \{x + C \mid x \in \mathbb{F}^n\}$$

の元 $x + C := \{x + c \mid c \in C\}$ をコセットまたは同値類、剰余類という。
例：$\mathbb{R}^2/\{(x,0)|x \in \mathbb{R}\} = \Big\{(0,y) + \{(x,0)|x \in \mathbb{R}\} \mid y \in \mathbb{R}\Big\} = \Big\{\{(x,y)|x \in \mathbb{R}\} \mid y \in \mathbb{R}\Big\}$

例：$\{00, 10, 01, 11\}/\{00, 10\} = \{\{00, 10\}, \{01, 11\}\}$ となる。これは、$C = \{00, 10\}$ に対して、$00 - 10 \in C$, $11 - 01 \in C$, $00 - 01 \notin C$, $10 - 11 \notin C$ であることから確かめられる。
例：$\{00, 10, 01, 11\}/\{00, 11\} = \{\boxed{\{00, 11\}, \{10, 01\}}\}$ □

命題 9.9 (コセットとシンドロームを同一視する)**.** 二つのベクトル x, y が同じコセットに含まれることと、x, y が同じシンドロームを有することは同値である。この対応によりシンドロームとコセットは 1 対 1 に対応する。

この対応と 9.5 から、シンドローム $H\vec{y}$ に対応するコセット $\{x \in \mathbb{F}^n \mid Hx = Hy\}$ はエラーベクトルを e を含むことが分かる。この中から重みが最小のエラーベクトルを推定エラーベクトルとする復号が、シンドローム復号である。 □

証明. 二つのベクトル x, y が同じコセットに含まれること $x - y \in C$ と、それらのベクトルが同じシンドロームを有するこ

と $Hx = Hy$ は同値であることを示す。

$$\begin{aligned} x - y \in C &\overset{(7.9)}{\Leftrightarrow} H(x-y) = 0 \\ &\Leftrightarrow Hx = Hy \end{aligned}$$

□

定義 9.10 (シンドローム復号法)**.** $\mathbb{F}$ 上の $[n,k]$ 線形符号のパリティ検査行列を H とする。次の復号法をシンドローム復号法という。シンドローム $s := Hy$ に対応するコセットのうちでハミング重みが最小のものを推定誤りベクトル $\hat{e}(s)$ とする。この $\hat{e}(s)$ をコセット代表元という。推定送信語を $\hat{x} = y - \hat{e}$ として出力する。正確に書くと以下の通りである。

$$\begin{aligned} \hat{x}^{(\mathrm{SR})}(y) :&= y - \hat{e}(s) \\ &= y - \operatorname*{argmin}_{e:s=He} w(e) \end{aligned}$$

シンドロームは $|\mathbb{F}|^{n-k}$ 通りあるので、シンドローム s からコセット代表元 $\hat{e}(s)$ への写像を、サイズ $|\mathbb{F}|^{n-k}$ の表を用意することにより実現できる。これは、$n-k$ が小さい、つまり符号化率 $R = \frac{k}{n}$ が大きいときには現実的な方法である。例：$n = 1023, n-k = 10$。シンドローム復号の御利益が実感できる例は、この演習と情報通信実験第 2 で扱う予定です。 □

定理 9.11 (シンドローム復号は最小距離復号と一致する)**.** シンドローム復号は最小距離復号と一致する。形式的に書くと、

受信語 y に対して以下が成り立つ。

$$\hat{x}^{(\mathrm{MD})}(y) = \hat{x}^{(\mathrm{SR})}(y)$$

□

証明.

$$\begin{aligned}
\hat{x}^{(\mathrm{MD})}(y) &= \operatorname*{argmin}_{x \in C} d(x, y) \\
&\overset{(7.9)}{=} \operatorname*{argmin}_{x : Hx = 0} w(y - x) \\
&\overset{(y=x+e)}{=} \operatorname*{argmin}_{y-e : H(y-e)=0} w(e) \\
&= y - \operatorname*{argmin}_{e : Hy = He} w(e) \\
&= y - \operatorname*{argmin}_{e : s = He} w(e) \\
&= \hat{x}^{(\mathrm{SR})}(y)
\end{aligned}$$

□

命題 9.12. 重みが t 以下の全てのベクトルがコセット代表元になることと、シンドローム復号法により重み t 以下の誤りを訂正できることは同値である。 □

証明. ある誤りベクトル e に対して、e が訂正できることと e がコセット代表元であることは同値なので、明らか。 □

10　標準型生成行列、標準型パリティ検査行列、組織符号

本節では，線形符号の行列表現をより実装寄りに整理する．生成行列を行基本変形と列入替で $[I_k\ P]$ の**標準形（systematic form）**に整えれば，符号語の左側 k シンボルが情報ビットの写像そのものになり，復号側で情報抽出が容易になる．対応する**標準型パリティ検査行列** $[-P^{\mathsf{T}}\ I_{n-k}]$ を導入し，$GH^{\mathsf{T}} = 0$ を確認することで，主・双対の整合も明確化する．この節の目的は，$[I_k\ P]$ 形への正規化と，それがもたらす符号化・データ抽出の簡潔さを理解することである．

定義 10.1 (標準型生成行列、組織符号). $[n, k]$ 線形符号の生成行列を G とする。$k \times n$ 生成行列 G が、サイズ k の単位行列 I_k と $k \times n-k$ 行列 P を用いて $G = [I_k \quad P]$ と書けるとき、G は標準形であるという。適当に与えられた生成行列 G は行の基本変形と列の入れ替えを施すと必ず標準形にできる。標準形生成行列による符号化は組織的[16]であると言う。　□

例 10.2. 例：$G' = \begin{pmatrix} 1001011 \\ 1100110 \\ 0111010 \end{pmatrix}$ は標準形で ない 。

[16] 多くの教科書では、標準型生成行列が存在する線形符号を組織的と言う。しかし、組織的でない線形符号は存在しないので、この定義では名付けることに意味が無い。Science Tokyo 生が人間であるとき人間的 Science Tokyo 生というようなものである。

例：$G = \begin{pmatrix} 100\ 1011 \\ 010\ 1101 \\ 001\ 0111 \end{pmatrix}$ は標準形で ある 。

G は G' に適当な行基本変形を施したものである。 □

議論 10.3. 生成行列 G を持つ $\mathbb{F}$ 上の $[n, k]$ 線形符号 C を考える。情報 $u = (u_1, \ldots, u_k) \in \mathbb{F}^k$ に対して符号語は $\vec{c} = uG$ になる。受信器は推定符号語 $\vec{c}$ から情報ベクトル u を戻す操作が必要になる。生成行列 G が標準型の場合、

$$c = uG = u(I_k \quad P) = (u \quad uP)$$

という形に符号語がなるから、符号語から情報ベクトル u を復元するために符号語の左側 k シンボルを取り出すだけで済むようになる。

例 10.4. 10.2 と同じ設定で、$c(u) = (111\ 0001)$ となる u は $c = uG = (u\ uP)$ より $u =$ (111) であることがすぐ分かる。 □

命題 10.5 (符号空間は生成行列の行基本変形に対して不変)**.** 生成行列 G に行基本変形を施すと、情報ベクトル u と符号語 $c(u) = uG$ の対応関係は変わる。符号空間 $C(G) = \{c(u) : u \in \mathbb{F}^k\}$ は変わらない。したがって、最小距離 $d(C)$ および訂正能力 $t(C)$ も変わらない。 □

証明. G の行ベクトル集合は C の基底である。G に行基本変形をしてもランクは変化しないので、C の基底であることに変わりは無い。 □

例　10.6. 10.2 と同じ設定で、$(111)G' =$ $\boxed{(001\ 0111)}$, $(111)G =$ $\boxed{(111\ 0001)}$ となる。 □

命題 10.7 (標準形になっている生成行列に対応するパリティ検査行列)**.** 生成行列

$$G = [I_k \quad P]$$

であるときに G で定義される線形符号のひとつのパリティ検査行列は

$$H = [-P^T \quad I_{n-k}]$$

で与えられる。この形のパリティ検査行列は標準型であると言う。上記のように作った H がパリティ検査行列なら H と G の各行の積が 0 ベクトルになるはずであるが，確かに

$$\begin{aligned} GH^T &= [I_k \quad P][-P^T \quad I_{n-k}]^T \\ &= [I_k \quad P]\begin{bmatrix} -P \\ I_{n-k} \end{bmatrix} \\ &= -I_kP + PI_{n-k} = -P + P = 0 \end{aligned}$$

となっている. □

例 10.8. 以下の標準型生成行列 G に対する標準型パリティ検

査行列 H は以下で与えられる。

$$G = \begin{pmatrix} 100\ 1011 \\ 010\ 1101 \\ 001\ 0111 \end{pmatrix}, H = \boxed{\begin{pmatrix} 110\ 1000 \\ 011\ 0100 \\ 101\ 0010 \\ 111\ 0001 \end{pmatrix}}$$

□

11 線形符号のパリティ検査行列による最小距離の計算

最小距離 $d(C)$ は訂正能力を決める中心量だが，総当たり計算は一般に困難である．本節では，**パリティ検査行列** H の列ベクトルの独立性に着目し，「任意の $d-1$ 列が独立なら $d(C) \geq d$」，「従属な d 列があれば $d(C) \leq d$」という**列独立性判定**に基づく距離評価法を示す．これにより，距離計算を行列の線形代数的判定に還元できることを理解する．

議論 11.1 (一般に最小距離を計算することは困難である)**.** 線形とは限らない符号空間 C に対して、C の最小距離

$$d(C) = \min_{x,y \in C, x \neq y} d(x, y)$$

を計算したい。原理的には、すべての異なる符号語ペア $x, y \in C, x \neq y$ に対して、距離を比較すれば最小距離を得られる。しかし、これには約 $|C|^2/2$ 回の比較が必要になる。線形符号に対しては、以下の 11.2 と 11.3 によって、比較的効率的に最小距離を計算することができる。

定理 11.2 (パリティ検査行列と最小距離)**.** $[n, k]$ 線形符号 C の $n-k \times n$ パリティ検査行列 H に対して、以下が成り立つ。任意の $d' \leq d-1$ に対して、H のどの d' 列を選んでも線形独立ならば、C の最小距離 $d(C)$ は d 以上である。 □

証明. パリティ検査行列 H の第 i 列を $\vec{h}_i$ とおく。

$$H = [\vec{h}_1 \quad \vec{h}_2 \quad \cdots \quad \vec{h}_n]$$

である。最小距離が $d-1$ 以下であると仮定する。つまり、非ゼロ符号語 $\vec{c} = (c_1, \ldots, c_n)$ でハミング重みが $d' \leq d-1$ のものが存在すると仮定する。$\vec{c}$ の非ゼロ要素を $c_{i_1}, \ldots, c_{i_{d'}}$ とする。このとき

$$\begin{aligned} \vec{0} &= H\vec{c} \\ &= c_{i_1}\vec{h}_{i_1} + c_{i_2}\vec{h}_{i_2} + \cdots + c_{i_{d'}}\vec{h}_{i_{d'}} \end{aligned}$$

となる。このことは $\vec{h}_{i_1}, \ldots, \vec{h}_{i_{d'}}$ が線形従属であることを意味するが、これは H のどの $d' \leq d-1$ 列も線形独立であることに矛盾する。 □

定理 11.3. $[n, k]$ 線形符号 C の $n-k \times n$ パリティ検査行列 H に対して以下が成り立つ。H のなかに線形従属になる d 列の組み合わせが一つでも有れば、C の最小距離 $d(C)$ は d 以下である。 □

証明. 重み d の符号語が存在することを示せば十分である。パリティ検査行列 H の第 i 列を $\vec{h}_i$ とおく。

$$H = [\vec{h}_1 \quad \vec{h}_2 \quad \cdots \quad \vec{h}_n]$$

である。条件より、ある d 列は線形従属である。この線形従属な d 列に名前をつける。$\vec{h}_{i_1}, \ldots, \vec{h}_{i_d}$ これらは、線形従属なの

で、係数 $c_{i_1}, \ldots, c_{i_d}$ が存在して

$$c_{i_1}\vec{h}_{i_1} + c_{i_2}\vec{h}_{i_2} + \cdots + c_{i_d}\vec{h}_{i_d} = \vec{0}$$

が成り立つ。ベクトル $\vec{c}$ を、添字 $i_1, \ldots, i_d$ の部分を $c_{i_1}, \ldots, c_{i_d}$ と等しくしそれ以外の部分を 0 にすると $\vec{c}$ のハミング重みは d であり、

$$\begin{aligned} H\vec{c} &= c_{i_1}\vec{h}_{i_1} + \cdots + c_{i_d}\vec{h}_{i_d} \\ &= \vec{0} \end{aligned}$$

であるから、$\vec{c}$ は重み d の符号語である。 □

例 11.4. パリティ検査行列 H によって定義される $[7, 4]$ 符号を C とする。

$$H = \begin{pmatrix} 1011100 \\ 1101010 \\ 0111001 \end{pmatrix}$$

第 2, 6, 7 列を取り出すと線形従属である。したがって、

$$\vec{c} = \boxed{(0100011)}$$

は C の符号語となる。このことは 11.3 から最小距離が 3 以下であることを意味する。 □

12　ハミング符号 @05

本節では，最小距離 3，単誤り訂正の古典的符号である**ハミング符号**を扱う．標準型 H と G を具体的に与え，列ベクトルの性質から $d = 3$ を導く．さらに，**シンドローム復号**がそのまま**最小距離復号**になることを例で確認し，一般の $[2^m-1, 2^m-1-m, 3]$ への拡張と**完全符号**としての充填性も示す．

定義 12.1 (ハミング符号)**.** 符号長 7 のハミング符号は以下のパリティ検査行列で定義される二元線形符号である。

$$H = \begin{pmatrix} 1011\ 100 \\ 1101\ 010 \\ 0111\ 001 \end{pmatrix}$$

これは標準形なので、対応する標準型生成行列は

$$G = \begin{pmatrix} 1000\ 110 \\ 0100\ 011 \\ 0010\ 101 \\ 0001\ 111 \end{pmatrix}$$

となる。このハミング符号の最小距離は 3 である。　□

証明. パリティ検査行列 H の、どの 2 列を取り出しても異なるから、どの 2 列も線形独立である。したがって、11.2 より最小距離は 3 以上である。パリティ検査行列 H の第 1,2,3 列

を足すと $(000)^T$ になるので、これらは線形従属である。したがって、11.3 より最小距離は 3 以下である。こうして、最小距離は 3 であることが示された。 □

定義 12.2 (ハミング符号の復号法)**.** ハミング符号の符号語を送って受信語 $r \in \mathbb{F}_2^7$ を受信したとする。以下の手続きで復号を行う。

1. シンドローム $s := Hr$ を計算する
2. シンドローム s と同じ H の中の列ベクトルを探す。それを i 列目とする
3. i 番目の要素が 1 で他がすべて 0 のベクトルを推定誤りベクトル $\hat{e}$ とする。
4. $r - \hat{e}$ を推定符号語 $\hat{c}$ とする。

上記の通り選ばれた推定誤りベクトル $\hat{e}$ はシンドロームに対応するコセットに含まれる誤りベクトル e、正確に書くと $He = s$ となる e のなかで重みが最小な $\hat{e}$ と一致する。したがって、この復号法はシンドローム復号すなわち最小距離復号となっている。 □

例 12.3 (ハミング符号の復号法の例)**.** $r = (1001110)$ を受信

したとする。

$$s := Hr = \begin{pmatrix} 1011\ 100 \\ 1101\ 010 \\ 0111\ 001 \end{pmatrix} (1001110)^T = \boxed{\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}}$$

次に、s が H の第 $i = \boxed{4}$ 列と等しいことを知る．最後に、推定誤りベクトルを $\hat{e} = (0001000)$ とし、推定送信語 $\hat{c} = r - \hat{e} = (1000110)$ を得る。 □

定義 12.4. 符号長 7 のハミング符号と同様に、m を 2 以上の整数として $[2^m - 1, 2^m - 1 - m, 3]$ ハミング符号を構成できる。長さが m の非ゼロの二元ベクトルは $2^m - 1$ 種類あるが、それらを列ベクトルとして並べた $m \times (2^m - 1)$ のパリティ検査行列によって定義される二元線形符号が、符号長 $2^m - 1$ のハミング符号である。符号長 7 のハミング符号の復号手続きと同じものを使えば、1 つまでの誤りを訂正できる。

$m = 2$ のとき、$[3, 1, 3]$ ハミング符号は長さ 3 の繰り返し符号 $\{000, 111\}$ と一致する。 □

命題 12.5 (ハミング符号は完全符号である)**.** 長さ $n = 2^m - 1$ のハミング符号 C は、完全である。言い換えると、ハミング符号 C の各符号語を中心とする半径 $t(C) = 1$ のハミング球は $\mathbb{F}_2^n$ を余すところなく完全に充填する。 □

証明. C は $(n = 2^m - 1, M := |C| = 2^{2^m - 1 - m}, d = 3)$ 符号である。さらに、$d(C) = 3$ より、$t(C) = 1, V_2(n, t) = n + 1$ と

なる。これらは、ハミング限界 4.9 を等式で満たし、C は完全となる。 □

13　線形符号の最小距離に関する限界式

ここでは，線形符号に課される**距離の限界**を概観する．まず，必要条件として**シングルトン限界** $d \le n-k+1$ を導き，等号達成符号（MDS 符号）の位置づけを明確にする．次に，存在の観点から **Varshamov–Gilbert (VG) 限界**を示し，非構成的版と，列選択により H を逐次構成する**構成的版**の両方を述べる．これにより，「達成可能な (n,k,d)」の見取り図を得る．

この節では $\mathbb{F}=\mathbb{F}_2$ と限定する。

定理 13.1 (シングルトン限界)**.** $[n,k,d]$ 符号 C に対して、以下が成り立つ。

$$d \le n-k+1$$

シングルトン限界は、$[n,k,d]$ 線形符号が存在するための必要条件を与える。シングルトン限界を等式で満たす $[n,k,d=n-k+1]$ 線形符号は最大距離分離符号 (MDS 符号) と呼ばれる。 □

証明. $[n,k,d]$ 線形符号のパリティ検査行列のサイズは $(n-k)\times n$ だが $n-k$ 行しかないから線形独立になれる列の組は高々$n-k$ 列までである。このことは、11.3 により最小ハミング距離は最大でも $n-k+1$ であることを意味する。 □

定義 13.2 (構成的証明)**.** 存在に関する命題「$x \in X$ が存在して命題 $P(x)$ が成り立つ。」を証明するときに、$P(x)=\text{true}$

となる $x \in X$ を明示する証明を構成的証明という。逆に、存在を明示的に示さず、存在しないと仮定して矛盾を導く証明を非構成的証明と言う。大きな有限集合からの最適な要素の選択を含む証明や、ランダムに選択したときに確率が 0 でないことによる証明も非構成的証明と呼ばれる。工学の分野では、興味のある条件を満たす装置の存在証明をしたいときに、構成的証明のほうが望ましい。なぜなら、構成的証明はその実現法も教えてくれるからである。 □

定理 13.3 (非構成的 VG 限界)**.** 線形とは限らない符号空間に対して示した VG 限界 4.14 と同様の定理が線形符号に対しても成り立つ。以下が成り立つとき、$[n, k, d]$ 符号は存在する。

$$2^{k-1} < \frac{2^n}{V_2(n, d-1)} \tag{13.4}$$

□

証明. 球被覆限界 4.11 より、$[n, k-1, d]$ 符号 C_{k-1} に対して、(13.4) ならば、C_{k-1} は最大ではないので、C_{k-1} のどの符号語とも距離が d 以上離れている $x \in \mathbb{F}^n, x \notin C_{k-1}$ が存在する。C_k を $C_{k-1} \cup \{x\}$ によって張られる線形符号とする。C_k の最小距離が d 以上になることを示そう。C_{k-1} から C_k に新たに加えられた符号語は

$$z = ax + y \, (a \in \mathbb{F}, a \neq 0, y \in C_{k-1})$$

と表すことができる。

$$w(z) = w(a^{-1}z) = w(x + a^{-1}y) = d(x, \underbrace{-a^{-1}y}_{\in C_{k-1}}) \geq d$$

となる。最後の不等号は x の選び方より分かる。新たに追加された符号語 z のハミング重みは d 以上になる事がわかった。8.2 より、C_k は $[n, k, d]$ 符号である。 □

定理 13.5 (構成的線形 VG 限界)**.** VG 限界 4.14 および 13.3 の証明は、x の存在に関して構成的で無かったことに注意しよう。以下の条件が成り立つとき、以下の手順で $[n, k, d]$ 符号を構成することができる。

$$2^{n-k} > \sum_{j=1}^{d-2} \binom{n-1}{j} \tag{13.6}$$

等価的に以下のように表せる。

$$2^k < \frac{2^n}{\sum_{j=1}^{d-2} \binom{n-1}{j}}$$

以下の手順で列ベクトル $h_1, \ldots, h_n \in \mathbb{F}^{n-k}$ を選択し、$(n-k) \times n$ パリティ検査行列 $H^{(n)} = (h_1, \ldots, h_n)$ を作ると、任意の $d-1$ 以下の列が線形独立となる。

1. $i := 1$ とする。任意の非零ベクトル $h_1 \in \mathbb{F}^{n-k}$ を選択する。$H^{(1)} = (h_1)$ とする。

2. $h_{i+1} \in \mathbb{F}^{n-k}$ を $H^{(i)}$ に加えた $H^{(i+1)} := (H^{(i)}|h_{i+1})$ の任意の $d-1$ 個以下の列が線形独立になるようにしたい。$H^{(i)}$ の任意の $d-1$ 個以下の列は線形独立であるから、h_{i+1} が $H^{(i)}$ の $d-2$ 本以下の列ベクトルの線形結合で表せないようになっていれば良い。

   $H^{(i)}$ の列 $h_1, \ldots, h_i$ から選ばれた任意の異なる j 列 $\tilde{h}_1, \ldots, \tilde{h}_j$ の非零係数 $a_i \neq 0$ for all $i = 1, \ldots, j$ による線形結合

$$x_j := a_1\tilde{h}_1 + \cdots + a_j\tilde{h}_j \tag{13.7}$$

   で表せるベクトル x_j の集合を $S_j^{(i)}$ と書く $(0 \leq j \leq d-2)$。このように表せないベクトル h_{i+1} をパリティ検査行列に加えればよい。集合

$$\mathbb{F}^{n-k} - \bigcup_{j=0}^{d-2} S_j^{(i)} \tag{13.8}$$

   が空でなければ、この集合に含まれるベクトルを h_{i+1} とすれば良い。

3. $i = n-1$ ならば終了する。$i < n-1$ ならば、$i := i+1$ として、2 に戻る。

□

証明. $1 \leq i \leq n-1$ に対して、ステップ 2 における (13.8) が空集合でなければ、定理は成り立つ。(13.7) の選択は、i 個の

ベクトルから j 個を選択してそれぞれ $|\mathbb{F}|-1$ 通りの非零係数を決定する操作によってなされるので、

$$|S_j^{(i)}| = \binom{i-1}{j}(|\mathbb{F}|-1)^j \overset{(\mathbb{F}=\mathbb{F}_2)}{=} \binom{i}{j}$$

となる。次が成り立つ。

$$|\mathbb{F}^{n-k}| = 2^{n-k} \overset{(13.6)}{>} \sum_{j=1}^{d-2}\binom{n-1}{j}$$
$$\overset{(i\le n-1)}{\ge} \sum_{j=1}^{d-2}\binom{i}{j} = \sum_{j=0}^{d-2}|S_j^{(i)}| \overset{(\text{ユニオン限界})}{\ge} \#\bigcup_{j=0}^{d-2} S_j^{(i)}$$

したがって、(13.8) が空集合でないことがわかる。 □

14 重み分布と検出誤り

重み分布 A_w は符号の**距離構造の全体像**を与える指標である．本節では，重み分布多項式 $A(X), A(X,Y)$ を定義し，BSC(p) における**検出誤り（見逃し）確率**を $A(1-p,p)$ で表せることを導く．最小重み（＝最小距離）だけでなく，全重み分布が性能評価に直結することを理解する．

定義 14.1 (重み分布と重み母関数)**.** 符号長 n の線形符号 C に対して、ハミング重み w の符号語の数を A_w と書く。

$$A_w = \#\{c \in C \mid w_H(c) = w\}$$

$(A_w)_{w=0}^n$ を符号 C の重み分布といい、以下の 2 つの多項式を C の重み分布多項式という。

$$A(X) := \sum_{w=0}^{n} A_w X^w = \sum_{c \in C} X^{w_H(c)}$$

$$A(X,Y) := \sum_{w=0}^{n} A_w X^{n-w} Y^w = \sum_{c \in C} X^{n-w_H(c)} Y^{w_H(c)}$$

上の対応により、重み分布と重み母関数を同一視する。線形符号に対して、$A_w \neq 0$ なる最小の $w > 0$ が、最小重み $w_{\min}(C)$ 等価的に最小距離 $d_{\min}(C)$ を与える。線形符号に対して、零符号語は唯一存在するので、$A_0 = 1$ である。 □

例 14.2. 長さ $n = 3$ の繰り返し符号 $\{000, 111\}$ の重み分布 A は以下の通りである。

$$A_0 = \boxed{1}, A_1 = \boxed{0}, A_2 = \boxed{0}, A_3 = \boxed{1},$$
$$A(X) = \boxed{1 + X^3}, A(X,Y) = \boxed{X^3 + Y^3} \qquad (14.3)$$

長さ $n = 3$ の単一パリティ検査符号 $\{000, 110, 011, 101\}$ の重み分布 B は以下の通りである。

$$B_0 = \boxed{1}, B_1 = \boxed{0}, B_2 = \boxed{3}, B_3 = \boxed{0},$$
$$B(X) = \boxed{1 + 3X^2}, B(X,Y) = \boxed{X^3 + 3XY^2} \qquad (14.4)$$

□

定義 14.5 (誤り検出、検出誤り、誤り見逃し確率)**.** 線形とは限らない符号 C を用いて、反転確率 p の 2 元対称通信路 $\mathrm{BSC}(p)$ で通信を行う。送信語 x に対して、受信語を y とする。受信機は誤り訂正はせずに、通信路で誤りが生じたときには送信者に再送を要求する。このとき、受信語が符号語でない $y \notin C$ ならば、通信路で誤りが生じたと判断する。このとき誤りを検出したという。通信路で誤りが生じているにもかかわらず、誤りを検出できないことを、検出誤りまたは見逃し誤りと言う。検出誤り確率を以下によって定義する。

$$P_u := \Pr(Y \in C, Y \neq X)$$

ここで、送信確率 $\Pr(X = x)$ を陽に使うと、

$$P_u = \sum_{x \in C} \Pr(Y \in C, Y \neq X \mid X = x) \Pr(X = x)$$

となる。 □

命題 14.6 (検出誤り確率の重み分布による表現)**.** 反転確率 p の 2 元対象通信路で線形符号 C で符号化された通信を行うことを考える。重み分布 $A(z) = \sum_{w=0}^{n} A_w z^w$ を有する符号長 n の線形符号 C に対して、誤り見逃し確率は以下で与えられる。

$$P_u = A(p, 1-p) - (1-p)^n \tag{14.7}$$

$$= (1-p)^n \left(A\left(\frac{p}{1-p}\right) - 1 \right) \tag{14.8}$$

□

証明.

$$
\begin{aligned}
P_u &= \Pr(Y \in C, Y \neq X) \\
&= \sum_{x,y \in \mathbb{F}^n} \Pr(X = x, Y = y) \mathbb{1}[y \in C, x \neq y] \\
&= \sum_{x,y \in \mathbb{F}^n} \Pr(Y = y | X = x) \Pr(X = x) \mathbb{1}[y \in C, x \neq y]
\end{aligned}
$$

ここで、誤りベクトル $Z := Y - X$ とすると、以下を得る。

$$
\begin{aligned}
&= \sum_{x,y \in \mathbb{F}^n} \Pr(Z = y - x) \Pr(X = x) \mathbb{1}[y \in C, y - x \neq 0] \\
&= \sum_{z,x \in \mathbb{F}^n} \Pr(Z = z) \Pr(X = x) \mathbb{1}[x + z \in C, z \neq 0]
\end{aligned}
$$

この式に貢献する x、言い換えると $P(X = x) \neq 0$ となる x は $x \in C$ であるから次の等号を得る。

$$
\begin{aligned}
&\overset{(a)}{=} \sum_{z,x \in \mathbb{F}^n} \Pr(Z = z) \Pr(X = x) \mathbb{1}[z \in C, z \neq 0] \\
&= \sum_{z \in \mathbb{F}^n} \sum_{x \in C} \Pr(Z = z) \Pr(X = x) \mathbb{1}[z \in C, z \neq 0] \\
&\overset{(b)}{=} \sum_{1 \leq w \leq n} \sum_{z \in \mathbb{F}^n : w_H(z) = w} \sum_{x \in C} \\
&\qquad \Pr(Z = z) \Pr(X = x) \mathbb{1}[z \in C] \\
&\overset{(c)}{=} \sum_{1 \leq w \leq n} \sum_{x \in C} A_w p^w (1-p)^{n-w} \Pr(X = x) \\
&\overset{(d)}{=} \sum_{1 \leq w \leq n} A_w p^w (1-p)^{n-w} \\
&\overset{(A_0 = 1)}{=} \sum_{0 \leq w \leq n} A_w p^w (1-p)^{n-w} - (1-p)^n \\
&= A(1-p, p) - (1-p)^n
\end{aligned}
$$

となり、(14.7) を得る。(a) では C の線形性を使った。(b) では z の総和を重みが w であるものに分割した。(c) では $w_H(z) > 0$ である z に対して $\sum_{z \in \mathbb{F}^n : w_H(z) = w} \mathbb{1}[z \in C] = A_w$ であることと、(d) では、$\sum_{x \in C} \Pr(X = x) = 1$ であることを使った。

$\Pr(Z=z)=p^w(1-p)^{n-w}$ であることを使った。さらに、

$$\begin{aligned}P_u &= \sum_{1\le w\le n} A_w p^w (1-p)^{n-w} \\ &= (1-p)^n \sum_{w=1}^{n} A_w \Big(\frac{p}{1-p}\Big)^w \\ &\overset{(A_0=1)}{=} (1-p)^n \Big(\sum_{w=0}^{n} A_w \Big(\frac{p}{1-p}\Big)^w - 1\Big)\end{aligned}$$

より、(14.8) を得る。 □

15 重み分布に関する双対定理

最後に，主符号 C と双対符号 $C^\perp$ の**重み分布の対応**を与える **MacWilliams の恒等式**を導く．アダマール変換を用いて $B(X,Y)=|C|^{-1}A(X+Y,X-Y)$ を示し，重み分布が双対性で強く拘束されることを明らかにする．拡張版の恒等式は，位置依存の多項式へ一般化し，復号アルゴリズムの解析にも応用できる．

補題 15.1 (アダマール変換)**.** 写像 $f:\mathbb{F}_2^n\to G$ から、写像 $\hat{f}:\mathbb{F}_2^n\to G$ への変換を以下により定義する。$\hat{f}$ を f のアダマール変換という。ここで、G は加群（加減算が代数系）で

ある。

$$\hat{f}(u) \stackrel{\text{def}}{=} \sum_{v \in \mathbb{F}_2^n} (-1)^{\langle u,v \rangle} f(v) \text{ for } u \in \mathbb{F}_2^n \tag{15.2}$$

$$\langle u, v \rangle = u_1 v_1 + \cdots u_n v_n \in \mathbb{F}_2$$

このとき、$[n, k]$ 線形符号 C に対して以下が成り立つ。

$$\sum_{u \in C} \hat{f}(u) = |C| \sum_{v \in C^\perp} f(v) \tag{15.3}$$

証明.

$$\begin{aligned}
\sum_{u \in C} \hat{f}(u) &\stackrel{(15.2)}{=} \sum_{u \in C} \sum_{v \in \mathbb{F}_2^n} (-1)^{\langle u,v \rangle} f(v) \\
&= \sum_{v \in \mathbb{F}_2^n} f(v) \sum_{u \in C} (-1)^{\langle u,v \rangle} \\
&\stackrel{(a)}{=} \sum_{v \in C^\perp} f(v) \sum_{u \in C} (-1)^{\langle u,v \rangle} + \sum_{v \notin C^\perp} f(v) \sum_{u \in C} (-1)^{\langle u,v \rangle} \\
&\stackrel{(b)}{=} \sum_{v \in C^\perp} f(v)|C| + 0
\end{aligned}$$

(a) では $\mathbb{F}_2^n = C^\perp + (C^\perp)^c$ を利用した。ただし、$(C^\perp)^c := \mathbb{F}_2^n - C^\perp$ である。(b) の第 1 項は、$v \in C^\perp$ に対して、$\langle u, v \rangle = 0$

であることによる。第 2 項が 0 になることを説明する。

$$\begin{aligned}\sum_{u\in C}(-1)^{\langle u,v\rangle} &= \sum_{u\in C:\langle u,v\rangle=0}(-1)^{\langle u,v\rangle} + \sum_{u\in C:\langle u,v\rangle=1}(-1)^{\langle u,v\rangle} \\ &= \sum_{u\in C:\langle u,v\rangle=0} 1 + \sum_{u\in C:\langle u,v\rangle=1}(-1) \\ &= \frac{\#C}{2} - \frac{\#C}{2} = 0\end{aligned}$$

となること (最後の等式) を主張する。まず、$\langle u,v\rangle = 0$ となる $u \in C$ となる $u \in C$ の数 $\sum_{u\in C:\langle u,v\rangle=0} 1$ を数えよう。$v \notin C^{\perp}$ に対して、v は C のパリティ検査行列の行ベクトルの線形結合で表すことはできない。できたと仮定すると、パリティ検査行列の行ベクトルは $C^{\perp}$ に含まれるのでそれらの線形結合 v は $v \in C^{\perp}$ となってしまうからである。したがって、$\mathrm{rank}\binom{H}{v} = \mathrm{rank}(H) + 1$ となる。よって、$u \in C$ となるための制約条件 (H の各行と u の内積が 0 となる) に $\langle u,v\rangle = 0$ を加えると、C の次元が一つ下がって、

$$\#\{u \in C \mid \langle u,v\rangle = 0\} = 2^{\dim C-1} = \frac{\#C}{2}$$

となる。$\langle u,v\rangle = 1$ となる $u \in C$ の数は残りの数 $\frac{\#C}{2}$ だけある。こうして、

$$\sum_{u\in C}(-1)^{\langle u,v\rangle} = \frac{\#C}{2} - \frac{\#C}{2} = 0$$

となることが分かる。 □

定理 15.4 (重み分布に関する双対定理、MacWilliams の恒等式)**.** MacWilliams の恒等式は、$[n,k]$ 主符号 C と $[n,n-k]$ 双対符号 $C^{\perp}$ の重み分布の関係を与える。C の重み分布を $A(X,Y)$、$C^{\perp}$ の重み分布を $B(X,Y)$ と書く。このとき、以下が成り立つ。

$$B(X,Y)=\frac{1}{|C|}A(X+Y,X-Y) \tag{15.5}$$

例：(14.4) と (14.3) の例に対して、(15.5) が確かに成り立つことが確かめられる。

$$\begin{aligned} B(X,Y) &= X^3+3XY^2 \\ &= \frac{1}{2}\boxed{\text{下の式を展開すれば確認できる}} \\ &= \frac{1}{2}\big((X+Y)^3+(X-Y)^3\big) \\ &= \frac{1}{|C|}A(X+Y,X-Y) \end{aligned}$$

□

証明. 15.1 における G を整数係数の 2 変数多項式の集合 $\mathbb{Z}[X,Y]$ とし、

$$f(u):=X^{n-w(u)}Y^{w(u)} \tag{15.6}$$

とする。このとき、(15.3) の左辺は以下より、$B(X,Y)$ となる。

$$\sum_{u\in C^{\perp}} f(u)=\sum_{u\in C^{\perp}} X^{n-w(u)}Y^{w(u)}=B(X,Y)$$

15.1 の (15.3) より次が成り立つ。

$$\sum_{u\in C^\perp} f(u) = \frac{1}{|C|}\sum_{u\in C}\hat{f}(u)$$

$$\hat{f}(u) \stackrel{\text{def}}{=} \sum_{v\in\mathbb{F}_2^n}(-1)^{\langle u,v\rangle} f(v) \text{ for } u\in\mathbb{F}_2^n$$

この右辺に登場する $\hat{f}(u)$ は、(15.6) に対して、次のようにシンプルな多項式で表せる。

$$\begin{aligned}
\hat{f}(u) &= \sum_{v\in\mathbb{F}_2^n}(-1)^{\langle u,v\rangle} X^{n-w(v)}Y^{w(v)} \\
&= \sum_{v\in\mathbb{F}_2^n}(-1)^{u_1v_1+\cdots+u_nv_n} X^{(1-v_1)+\cdots+(1-v_n)}Y^{v_1+\cdots+v_n} \\
&\stackrel{(a)}{=} \prod_{i=1}^{n}(X+(-1)^{u_i}Y) \\
&= \prod_{i=1}^{n}\begin{cases} X+Y, & u_i=0 \\ X-Y, & u_i=1 \end{cases} \\
&= (X+Y)^{n-w(u)}(X-Y)^{w(u)}
\end{aligned}$$

(a) は、右辺を $n=2,3,\ldots$ の場合に展開すると正しいことが分かる。(15.3) の右辺は以下を満たすことが分かる。

$$\begin{aligned}
\sum_{u\in C}\hat{f}(u) &= \sum_{u\in C}(X+Y)^{n-w(u)}(X-Y)^{w(u)} \\
&= A(X+Y, X-Y)
\end{aligned}$$

こうして、証明が完成する。 □

次の定理は、Hartman-Rudolph 復号アルゴリズムの導出のためにここに記したが、授業では扱わない。将来、演習で扱うかもしれません。

定理 15.7 (拡張 MacWilliams 恒等式)**.**

$$
\begin{aligned}
X &:= (X_1, \ldots, X_n) \\
Y &:= (Y_1, \ldots, Y_n) \\
\mathrm{P}_C(X;Y) &:= \sum_{c \in C} \prod_{j \in [n]} X_j^{1-c_j} Y_j^{c_j} \\
\mathrm{P}_{C^\perp}(X;Y) &:= \sum_{c \in C^\perp} \prod_{j \in [n]} X_j^{1-c_j} Y_j^{c_j}
\end{aligned}
$$

とする。次が成り立つ。

$$
P_C(X;Y) = \frac{1}{|C|} P_{C^\perp}(X+Y; X-Y)
$$

$X := \underline{1}, Y := X$ とすることで、次を得る。

$$
\begin{aligned}
\mathrm{P}_C(X) &:= \sum_{c \in C} \prod_{j \in [n]} X_j^{c_j} \\
P_C(X) &= \frac{1}{|C|} P_{C^\perp}\left(\prod_{j=1}^{n} \frac{1+X_j}{1-X_j} \right) \prod_{j=1}^{n} (1-X_j)
\end{aligned}
$$

□

証明. 15.1 における G を整数係数の 2 変数多項式の集合 $\mathbb{Z}[X,Y]$ とし、

$$f(u)=\prod_{j=1}^{n}X_j^{1-u_j}Y^{u_j}$$

とする。このとき、次が成り立つ。

$$\sum_{u\in C^{\perp}}f(u)=\mathrm{P}_{C^{\perp}}(X;Y) \tag{15.8}$$

$$\begin{aligned}
\hat{f}(u)&=\sum_{v\in\mathbb{F}_2^n}(-1)^{\langle u,v\rangle}\prod_{j=1}^{n}X^{1-v_j}Y^{v_j}\\
&=\sum_{v\in\mathbb{F}_2^n}(-1)^{u_1v_1+\cdots+u_nv_n}X_1^{1-v_1}\cdots X_n^{1-v_n}Y_1^{v_1}\cdots Y_n^{v_n}\\
&\overset{(a)}{=}\prod_{j=1}^{n}(X_j+(-1)^{u_i}Y_j)\\
&=\prod_{j=1}^{n}(X_j+Y_j)^{1-u_j}(X_j-Y_j)^{u_j}
\end{aligned}$$

(a) では、因数分解をした。例として、$n=2$ のとき、(a) は

次となる。

$$
\begin{aligned}
&(X_1 + (-1)^{u_1} Y_1)(X_2 + (-1)^{u_2} Y_2) \\
&= X_1 X_2 + (-1)^{u_2} X_1 Y_2 + (-1)^{u_1} Y_1 X_2 + (-1)^{u_1+u_2} Y_1 Y_2 \\
&= (-1)^{u_1 v_1 + u_2 v_2} X_1^{(1-v_1)} X_2^{(1-v_2)} Y_1^{v_1} Y_2^{v_2} \Big|_{(v_1,v_2)=(0,0)} \\
&+ (-1)^{u_1 v_1 + u_2 v_2} X_1^{(1-v_1)} X_2^{(1-v_2)} Y_1^{v_1} Y_2^{v_2} \Big|_{(v_1,v_2)=(0,1)} \\
&+ (-1)^{u_1 v_1 + u_2 v_2} X_1^{(1-v_1)} X_2^{(1-v_2)} Y_1^{v_1} Y_2^{v_2} \Big|_{(v_1,v_2)=(1,0)} \\
&+ (-1)^{u_1 v_1 + u_2 v_2} X_1^{(1-v_1)} X_2^{(1-v_2)} Y_1^{v_1} Y_2^{v_2} \Big|_{(v_1,v_2)=(1,1)}
\end{aligned}
$$

これより、次が成り立つ。

$$\sum_{u \in C} \hat{f}(u) = P_C(X+Y, X-Y) \tag{15.9}$$

(15.8) と (15.9) を (15.3) に代入して、証明が完成する。 □

16　群 @06

本節では，代数系の概念を出発点として，その中で最も基本的な構造である**群（group）**を定義する．群は「演算に対して閉じ，結合則を満たし，単位元と逆元をもつ集合」であり，環や体などより複雑な構造を理解するうえでの基礎となる．まず，代数系や半群の定義から始め，群および可換群の性質を整理する．その後，整数や行列など具体的な例を通して群の直感をつかみ，単位元・逆元の一意性，および逆元の演算規則を学ぶ．

定義 16.1 (代数系)**.** 整数の集合 $\mathbb{Z}$ に関して、$a, b \in \mathbb{Z}$ に対して $a+b$ と言う演算+が定義されている。このように、一般に集合 A とその集合上で定義された演算 $\circ$ に対して、以下が成り立つ組 $(A, \circ)$ を代数系という。

(閉性) $\forall a_1, a_2 \in A$ に対して、

$$a_1 \circ a_2 \in A$$

例：$(\mathbb{R}, \{+, -\})$ は代数系である。
例：$(\mathbb{N}, \{+, -\})$ は減算に関して閉じてないので、代数系ではない。 □

定義 16.2 (半群、群、可換群)**.** 整数集合 $\mathbb{Z}$ と $\mathbb{Z}$ 上で定義された演算 $+$ からなる代数系 $(A := \mathbb{Z}, \circ := +)$ は、以下の性質を満たす。

(結合性) 演算結果が実行する順序によらない。正確に述べると $\forall a_1, a_2, a_3 \in A$ に対して以下が成り立つ。

$$a_1 \circ (a_2 \circ a_3) = (a_1 \circ a_2) \circ a_3$$

(単位元の存在) $e \in A$ が存在して、

$$e \circ a = a \circ e = a$$

(逆元の存在) 任意の $a \in A$ に対して、$a' \in A$ が存在して、

$$a' \circ a = a \circ a' = e$$

(可換性) 任意の $a_1, a_2 \in A$ に対して

$$a_1 \circ a_2 = a_2 \circ a_1$$

逆に、与えられた代数系 $(A, \circ)$ に対して、次の名前を与える。

1. 単位元の存在・逆元の存在・結合性が成り立つ代数系 $(A, \circ)$ を、群という。
2. 可換性が成り立つ群 $(A, \circ)$ を可換群という。
3. 結合性が成り立つ代数系 $(A, \circ)$ を、半群という。
4. 結合性と単位元の存在が成り立つ代数系 $(A, \circ)$ を、モノイドという。

□

例 16.3. 群に関する例と反例を挙げる。

1. 整数、有理数、実数、複素数の集合を、それぞれ G と書く。$(G,+)$ は可換群を成す。単位元は $\boxed{0} \in G$ であり、$a \in G$ の逆元は $\boxed{-a} \in G$ である。

2. 0 を除いた有理数、実数、複素数の集合を、それぞれ G と書く。$(G,\times)$ は可換群を成す．単位元は $\boxed{1} \in G$ であり、$a \in G$ の逆元は $\boxed{1/a} \in G$ である。

3. 0 を除いた整数の集合 $(G := \mathbb{Z} \setminus \{0\},\times)$ は、乗法に関して群とならない。実際、$\boxed{1} \in G$ が単位元となるが、$2 \in G$ の逆元、言い換えると

$$2 \times a = a \times 2 = 1 \text{ となる } a \in G$$

が存在しない。

4. 整数 $n > 0$ に対して、n の倍数からなるを集合 $n\mathbb{Z}$ と書く。$(n\mathbb{Z},+)$ は可換群となる。

5. 整数 $n > 0$ に対して、

$$\mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z} := \{0,1,\ldots,n-1\}$$

と書く。なぜこのように書くかは、後で分かる。$a,b \in \mathbb{Z}_n$ に対して、

$$a + b \overset{\text{def}}{=} a + b \bmod n$$

と定義する。ただし、左辺の $+$ は $\mathbb{Z}_n$ における加算を、右辺の $+$ は $\mathbb{Z}$ における加算を表し、$a+b \bmod n$ は $a+b$ を n で割った余りを表している。$(\mathbb{Z}_n, +)$ は可換群となる。群 $\mathbb{Z}$ と群 $n\mathbb{Z}$ から新たな群 $\mathbb{Z}/n\mathbb{Z}$ を構成したとみなせる。このような群を商群というのだが、今回の講義では商群の作り方を学ぶ。

$n = 3$ とすると、

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

6. サイズ n の複素正則行列の集合は、乗法に関して群をなす。これを、複素一般線形群といい GL_n と書く。単位元はサイズ n の単位行列 I_n であり、行列 $A \in \mathrm{GL}_n$ の逆元は逆行列 A^{-1} である。正則行列は言い換えると逆元が存在する行列なので、群となることは当然である。

7. サイズ n の複素正方行列の集合を M_n と書く。M_n は乗法に関して群をなさない。以下でこれを説明する。単位元はサイズ n の単位行列 I_n である。非正則な行列 $A \in M_n$ に対して、逆元つまり

$$AA' = A'A = I_n$$

となる逆行列 $A' \in M_n$ は存在しない。

8. 複素一般線形群 GL_n の元のうち、行列式が 1 である行列の集合は、乗法に関して群をなす。これを、複素特殊線形群と言い、SL_n と書く。以下では、閉性 $A_1, A_2 \in \mathrm{SL}_n \Rightarrow A_1A_2 \in \mathrm{SL}_n$ を示す。$\det A_1 = \det A_1 = 1$ である。

$$\det A_1A_2 = \det A_1 \det A_1 = 1$$

となるので、$A_1A_2 \in \mathrm{SL}_n$ が示せた。

9. サイズ n のユニタリ行列の集合は、乗法に関して群をなす。これを、ユニタリ群といい U_n と書く。

10. 代数系 $(\mathbb{Z}, -)$ では、結合律の成り立たない。実際、

$$(5-3)-2 \neq 5-(3-2)$$

となる。

□

定義 16.4 (演算子に関する慣習)**.** 群 $(G, \circ)$ に関して、以下の慣習が広く使われている。

- 演算が加算+である加法群 $(G, +)$ に対して、
  1. G は可換であることが慣習として想定される。可換な加法群を G を加群と言う。
  2. 単位元を 0 と書く。

3. a の逆元を $-a$ と書く。
4. $b+(-a)$ を $b-a$ と書く。

- 演算が乗算 $\times$ である乗法群 $(G,\times)$ に対して、

1. 単位元を 1 と書く。
2. 自然数 $n>0$ に対して、$\overbrace{a\times\cdots\times a}^{n \text{ times}}$ を a^n と書く。
3. a^0 を 1 と定める。
4. a の逆元を a^{-1} と書く。
5. 自然数 $n>0$ に対して、$\overbrace{a^{-1}\times\cdots\times a^{-1}}^{n \text{ times}}$ を a^{-n} と書く。
6. $b\times(a^{-1})$ を b/a と書く。
7. $\times$ は省略されることがある。

本講義では、群 G の演算子がなんであるかに興味が無い場合には、$(G,\circ)$ を用いるか、表記を簡潔にするために G を乗法群として扱う。 □

定義 16.5 (位数)**.** 群 G の要素数を G の位数といい、$\mathrm{ord}(G)$ と書く。群 G の元 $g\in G$ に対して、

$$g^1, g^2, \dots,$$

と並べたときに初めて単位元 1 になる $g^k=1$ に対して、k を元 $g\in G$ の位数といい、$\mathrm{ord}(g)$ と書く。 □

命題 16.6 (単位元は一意である)**.** 群 $(G, \times)$ に関して、単位元は唯一である。 □

証明. e, e' を単位元とする。e, e' が単位元であることから、(16.2)(単位元の存在) より、

$$ee' = e',$$
$$ee' = e$$

を得る。よって、結局 $e' = e$ である。 □

命題 16.7 (逆元は一意である)**.** 群 $(G, \times)$ に関して、$a \in G$ の逆元は一意に存在する。 □

証明. a', a'' を a の逆元とする。(16.2)(逆元の存在) より

$$a'a = e$$

を得る。両辺 LHS, RHS に右から a'' をかけるとそれぞれ

$$(\text{LHS}) \times a'' = (a'a)a'' = a'(aa'') = a'e = a'$$
$$(\text{RHS}) \times a'' = ea'' = a''$$

となり、結局 $a' = a''$ である。 □

命題 16.8 (逆元の逆元は元に戻る)**.** 群 $(G, \times)$ の元 $a \in G$ に対して、以下が成り立つ。

$$(a^{-1})^{-1} = a$$

□

証明. $(a^{-1})^{-1} =: a'$ と書く。a' は a^{-1} の逆元なので、(16.2)(単位元の存在) より、

$$a'a^{-1} = 1$$

となる。この両辺 LHS, RHS に、右から a を乗ずると

$$(\text{LHS})a = (a'a^{-1})a = a'(a^{-1}a) = a'1 = a'$$
$$(\text{RHS})a = 1a = a$$

となり、$a' = a$ を得る。

□

例 16.9. 可換とは限らない加法群 $(G, +)$ に対して、以下が成り立つ。

$$-(-a) = a$$

□

命題 16.10. 群 $(G, \times)$ の要素 $x, y \in G$ について,

$$(xy)^{-1} = y^{-1}x^{-1}$$

が成り立つ。 □

証明. 単位元を e と書く。 xy の逆元が $y^{-1}x^{-1}$ であること、つまり

$$(xy)(y^{-1}x^{-1}) = e \tag{16.11}$$
$$(y^{-1}x^{-1})(xy) = e \tag{16.12}$$

を示せば良い。

$$\begin{aligned}(xy)(y^{-1}x^{-1}) &\overset{\text{(i)}}{=} x\big(y(y^{-1}x^{-1})\big)\\ &\overset{\text{(ii)}}{=} x\big((yy^{-1})x^{-1}\big)\\ &\overset{\text{(iii)}}{=} x\big(ex^{-1}\big)\\ &\overset{\text{(iv)}}{=} x\big(x^{-1}\big)\\ &\overset{\text{(v)}}{=} e\end{aligned}$$

となる．第１，２等号には結合律を，第３、５等号には逆元の性質を，第４等号には単位元の性質を使った．こうして (16.11) は示された。(16.12) も同様に示せる。 □

例 16.13. 可換とは限らない加法群 $(G,+)$ に対して、以下が成り立つ。$x,y\in G$ に対して $x+y$ の逆元は $(-y)+(-x)$ である。正確に書くと、

$$-(x+y)=(-y)+(-x)$$

である。実際、

$$\begin{aligned}(x+y)+(-y)+(-x) &= x+(y+(-y))+(-x)\\ &= x+0+(-x)\\ &= x+(-x)\\ &= 0\end{aligned}$$

により確かめられる。 □

x	I	-I	iI	-iI	X	-X	iX	-iX	Y	-Y	iY	-iY	Z	-Z	iZ	-iZ
I	I	-I	iI	-iI	X	-X	iX	-iX	Y	-Y	iY	-iY	Z	-Z	iZ	-iZ
-I	-I	I	-iI	iI	-X	X	-iX	iX	-Y	Y	-iY	iY	-Z	Z	-iZ	iZ
iI	iI	-iI	-I	I	iX	-iX	X	-X	iY	-iY	Y	-Y	iZ	-iZ	Z	-Z
-iI	-iI	iI	I	-I	-iX	iX	-X	X	-iY	iY	-Y	Y	-iZ	iZ	-Z	Z
X	X	-X	iX	-iX	I	-I	iI	-iI	iZ	-iZ	-Z	Z	-iY	iY	Y	-Y
-X	-X	X	-iX	iX	-I	I	-iI	iI	-iZ	iZ	Z	-Z	iY	-iY	-Y	Y
iX	iX	-iX	-X	X	-iI	iI	I	-I	Z	-Z	-iZ	iZ	Y	-Y	-iY	iY
-iX	-iX	iX	X	-X	iI	-iI	-I	I	-Z	Z	iZ	-iZ	-Y	Y	iY	-iY
Y	Y	-Y	iY	-iY	-iZ	iZ	Z	-Z	I	-I	iI	-iI	iX	-iX	-X	X
-Y	-Y	Y	-iY	iY	iZ	-iZ	-Z	Z	-I	I	-iI	iI	-iX	iX	X	-X
iY	iY	-iY	-Y	Y	-Z	Z	iZ	-iZ	iI	-iI	-I	I	X	-X	-iX	iX
-iY	-iY	iY	Y	-Y	Z	-Z	-iZ	iZ	-iI	iI	I	-I	-X	X	iX	-iX
Z	Z	-Z	iZ	-iZ	iY	-iY	-Y	Y	-iX	iX	X	-X	I	-I	iI	-iI
-Z	-Z	Z	-iZ	iZ	-iY	iY	Y	-Y	iX	-iX	-X	X	-I	I	-iI	iI
iZ	iZ	-iZ	-Z	Z	Y	-Y	-iY	iY	X	-X	-iX	iX	iI	-iI	-I	I
-iZ	-iZ	iZ	Z	-Z	-Y	Y	iY	-iY	-X	X	iX	-iX	-iI	iI	I	-I

図 16.15: パウリ群 $\mathcal{P}_1$ の演算表

例 16.14. パウリ群 $\mathcal{P}_1$ は、次の行列の集合と自然な行列の積によって定義されます。

$$\mathcal{P}_1 = \{\pm I, \pm iI, \pm X, \pm iX, \pm Y, \pm iY, \pm Z, \pm iZ\}$$

ここで

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

この群は非可換で、位数 (サイズ) は 16 です。演算表は 16.15 になります。 □

17　部分群、剰余類群、正規部分群

本節では，群の内部構造をさらに詳しく調べる．まず，群の中に含まれる小さな群である**部分群（subgroup）**を定義し，その性質を確認する．次に，部分群による同値関係を導入し，群の元をその関係で分類することで**剰余類（coset）**と**商集合**を構成する．さらに，群の演算と両立する特別な部分群である**正規部分群（normal subgroup）**を定義し，それを法として新たな群を作る**商群（quotient group）**の概念を導く．

定義 17.1 (部分群)**.** 群 $(G, \times)$ の部分集合 $H \subset G$ に対して、$(H, \times)$ が群であるとき、H は G の部分群であると言う。 □

例 17.2. 整数 $m > 0$ に対して、$m\mathbb{Z}$ は m の倍数の集合とする。

$$m\mathbb{Z} := \{mx \mid x \in Z\}$$

$(m\mathbb{Z}, +)$ は $(\mathbb{Z}, +)$ の部分群である。 □

定義 17.3. 群 G とその部分集合 $S \subset G$ に対して、

$$Sg := \{sg \mid s \in S\} \text{ for } g \in G$$
$$gS := \{gs \mid s \in S\} \text{ for } g \in G$$

と書く。群の演算が加算で定義されている場合には $S+g, g+S$ を同様に定義する。

$$S + g := \{s + g \mid s \in S\}$$
$$g + S := \{g + s \mid s \in S\}$$

□

定義 17.4 (正規部分群、 normal subgroup)**.** 群 G とその部分群 $N \subset G$ に対して、

$$\forall g \in G, gN = Ng \tag{17.5}$$

が成り立つとき、N は正規であるといい、$N \triangleleft G$ と書く。 □

命題 17.6. 可換群 G の任意の部分群 N は正規である。 □

証明. 以下のように示すことができる。

$$Ng = \{ng \mid n \in N\} = \{gn \mid n \in N\} = gN$$

□

例 17.7. 整数 $m > 0$ に対して、$m\mathbb{Z}$ は $\mathbb{Z}$ の正規部分群である。 □

証明. 17.6 より明らかだが、定義通りに確かめると、任意の $i \in \mathbb{Z}$ に対して、

$$\begin{aligned} i + m\mathbb{Z} &= \{i + mx \mid x \in \mathbb{Z}\} \\ &= \{mx + i \mid x \in \mathbb{Z}\} \\ &= m\mathbb{Z} + i \end{aligned}$$

となることから分かる。$m\mathbb{Z}$ が (17.5) の N に相当することに注意しよう。 □

命題 17.8 (正規部分群に関する同値な定義)**.** 次は同値である。

1. $N \triangleleft G$ である。つまり、$\forall g \in G$ に対して $gN = Ng$
2. $\forall g \in G$ に対して、$gNg^{-1} = N$
3. $\forall n \in N, \forall g \in G$ に対して、

$$gng^{-1} \in N \tag{17.9}$$

[17]

□

証明. 演習問題として出す。 □

例 17.10. $N := \{\pm I, \pm iI\}$ はパウリ群 $\mathcal{P}_1$ の正規部分群です。 □

証明. まず、N は明らかに群です :I が単位元。$(\pm iI)^{-1} = \mp iI$ が含まれる。積も閉じており、例えば $(iI)(iI) = -I$ 。したがって部分群です。

(17.9) を使うことにします。次に、任意の $g \in P_n$ に対して

$$g(\pm I)g^{-1} \in N, \quad g(\pm iI)g^{-1} \in N$$

[17]部分群 $H \subset G$ と $g \in G$ に対して、gHg^{-1} は、G の部分群になり、H の共役部分群であるという。$g, g' \in G$ は、$g' = gxg^{-1}$ for some $x \in G$ であるとき、共役であるという。共役関係は同値関係である。この同値関係による G の分類を共役類という。

が成り立つことを確認します。実際、

$$g(\omega I)g^{-1} = \omega\left(gIg^{-1}\right) = \omega I$$

for $\omega \in \{\pm 1, \pm i\}$ です。なぜなら I は恒等行列だから $gIg^{-1} = I$ 。したがって、 $g(\omega I)g^{-1} = \omega I$ は変わらず同じ集合内 N にとどまります。 □

定義 17.11 (部分群を法とする左合同関係、左剰余類 (left coset))**.** 群 $(G, \times)$ とその部分群 $H \subset G$ に対して、ある $h \in H$ が存在して

$$g_1 h = g_2$$

言い換えると、

$$g_1^{-1} g_2 \in H \text{ or } g_2^{-1} g_1 \in H$$

となるとき $g_1, g_2 \in G$ は H を法として左合同であるといい、

$$g_1 \equiv g_2 \,(\mathrm{mod} H)$$

と書く。この関係 $g_1 \sim g_2$ は同値関係である。g を代表元とする同値類 $[g] := \{g' \in G \mid g \sim g'\}$ を左剰余類という。これに対して、

$$[g] = gH \tag{17.12}$$

が成り立つ。この同値関係による商集合を

$$G/H := G/\sim = \{[g] \mid g \in G\} = \{gH \mid g \in G\}$$

と書く。

演算が可換とは限らない加算で定義されている群 $(G, +)$ の場合には、$g_1 \sim g_2$ を $\exists h \in H, g_1 + h = g_2$ いいかえると $-g_1 + g_2 \in H$ または $-g_2 + g_1 \in H$ によって定義し、左剰余類は $[g] = g + H$ となる。この場合も、商集合は G/H と書く。

左を右に置き換えたもので、右剰余類を定義する。H が正規部分群であれば、$gH = Hg$ となり左右剰余類の区別は無くなる。 □

証明. 群 $(G, \times)$ 上の左合同関係 $\sim$ が同値関係であることを示す。 $g \times 1 = g$ なので、$g \sim g$ となるので、反射律が成り立つ。 $g_1 h = g_2$ ならば両辺に右から h^{-1} をかけて $g_2 h^{-1} = g_1$ となるので、対称律も成り立つ。$g_1 h = g_2, g_2 h' = g_3$ ならば $g_1 h h' = g_3$ なので、推移律も成り立つ。

(17.12) は、以下より明らか。

$$\begin{aligned}
[g] &= \{g' \mid g \sim g'\} \\
&= \{g' \mid \exists h \in H, gh = g'\} \\
&= \{gh \mid h \in H\} \\
&= gH
\end{aligned}$$

□

例 17.13. 整数の加算に関する群 $(\mathbb{Z}, +)$ の部分群 $(m\mathbb{Z}, +)$ に対して、商集合 $\mathbb{Z}/m\mathbb{Z}$ は以下を満たす。

1. $i, j \in \mathbb{Z}$ に対して、$i \sim j \Leftrightarrow -i + j \in m\mathbb{Z}$ である。
2. $i \in \mathbb{Z}$ に対して、$[i] = i + m\mathbb{Z}$ である。
3. $[i] \in \mathbb{Z}/m\mathbb{Z}$ に対して、以下が成り立つ。

$$\begin{aligned}[i] &:= \{j \in \mathbb{Z} \mid i \sim j\} \\ &= \{j \in \mathbb{Z} \mid -i + j \in m\mathbb{Z}\} \\ &= \{j \in \mathbb{Z} \mid i \equiv j \bmod m\mathbb{Z}\}\end{aligned}$$

4. $[i] \in \mathbb{Z}/m\mathbb{Z}$ は、m シフトに対して不変である。正確に述べると以下が成り立つ。

$$[i] = [m + i]$$

5. $\mathbb{Z}/m\mathbb{Z} = \{[0], [1], \ldots, [m-1]\}$ と書ける。

□

補題 17.14. モノイド（単位元 $1 \in S$ を有し結合性を満たす代数系[18]上の同値関係 $\sim$ によって定義される同値類 $[x] := \{x' \in S \mid x \sim x'\}$ が以下を満たすとする。

[18]群 $(S, \times)$ にしか適用しないから群から始めても良かったんだけど、剰余類の well-definedness とその成立を分離するためにこうしました。

1. 演算が well-defined であること：$\forall x, x', y, y' \in S$ に対して、

$$[x] = [x'], [y] = [y'] \Rightarrow [x \times y] = [x' \times y'] \tag{17.15}$$

2. 逆元が存在すること：$\forall x \in S$ に対して、$\exists x' \in S$ が存在して、

$$[x \times x'] = [1] \tag{17.16}$$

となる。

このとき、$x, y \in S$ に対して

$$[x] \times [y] \stackrel{\text{def}}{=} [x \times y]$$

と定義することにより、商集合 $(S/\sim, \times)$ は群となる。

証明. 演算の結果が代表元の取り方によらないことは、(17.15) によって保証される。結合則

$$\forall [x], [y], [z] \in S/\sim, \quad \Big([x] \times [y]\Big) \times [z] = [x] \times \Big([y] \times [z]\Big)$$

が満たされることは、S の結合則に帰着させて

$$\begin{aligned} ([x][y])[z] &= [xy][z] \\ &= [(xy)z] \\ &= [x(yz)] \\ &= [x][yz] \\ &= [x]([y][z]) \end{aligned} \tag{17.17}$$

と示される。$[1] \in S/\sim$ が単位元となることも同様に示せる。

$$[1][x] = \boxed{[1x]} = [x]$$
$$[x][1] = \boxed{[x1]} = [x]$$

(17.16) によって

$$[x][x'] = [xx'] = [1]$$

となる $[x'] \in S/\sim$ が存在する。これは、$[x] \in S/\sim$ の逆元 $[x'] \in S/\sim$ が存在することを意味する。こうして、商集合 $(S/\sim, \times)$ は群となることが分かった。 □

定義 17.18 (剰余類群、商群)**.** 群 G の部分群 N が正規部分群であるとする。$(G/N, \times)$ は以下で定義される演算により群となる。$(G/N, \times)$ は N を法とする商群または剰余類群または単に剰余群と呼ばれる。

$$[g_1] \times [g_2] \stackrel{\text{def}}{=} [g_1 \times g_2] \text{ for } [g_1], [g_2] \in G/N$$

書き換えると、

$$(g_1 N) \times (g_2 N) \stackrel{\text{def}}{=} (g_1 \times g_2)N \text{ for } g_1 N, g_2 N \in G/N$$

である。 □

証明. 17.14 を使用する。$S := G$ とし、さらに N を法とする合同関係を同値関係 $\sim$ とする。(17.15) と (17.16) が成り立つことを示す。

(17.16) は $x' = x^{-1}$ と選べば明らかである。(17.15) が満たされること、つまり $\forall x, x', y, y' \in G$ に対して、

$$[x] = [x'], [y] = [y'] \Rightarrow [xy] = [x'y']$$

を示せば十分である。$[x] = [x'], [y] = [y']$ 言い換えると

$$x^{-1}x' \in N, y^{-1}y' \in N$$

より、$[xy] = [x'y']$ を示す。$x^{-1}x' \in N$ と $y \in G$ と N の正規性 (17.9) から

$$y^{-1}(x^{-1}x')y \in N$$

となる。これと、次より $[xy] = [x'y']$ となることが分かる。

$$\begin{aligned}(xy)^{-1}(x'y') &\overset{(16.13)}{=} (y^{-1}x^{-1})(x'y') \\ &= y^{-1}(x^{-1}(x'y')) \\ &= y^{-1}(x^{-1}x')y' \\ &= y^{-1}(x^{-1}x')ey' \\ &= y^{-1}(x^{-1}x')yy^{-1}y' \\ &= \underbrace{y^{-1}(x^{-1}x')y}_{\in N}\underbrace{y^{-1}y'}_{\in N} \in N\end{aligned}$$

□

例 17.19. 可換群 $(\mathbb{Z}, +)$ の部分群 $(m\mathbb{Z}, +)$ に対して、商群 $(\mathbb{Z}/m\mathbb{Z}, +)$ は以下を満たす。

1. $\mathbb{Z}/m\mathbb{Z} = \{[0], [1], \ldots, [m-1]\}$ と書ける。
2. $(\mathbb{Z}/m\mathbb{Z}, +)$ は以下で定義される演算$+$によって、群となる。

$$[i] + [j] \stackrel{\text{def}}{=} [i + j] \text{ for } [i], [j] \in \mathbb{Z}/m\mathbb{Z}$$

3. $i, j \in \mathbb{Z}$ に対して、

$$[i] + [j] = [\boxed{i + j} \bmod \boxed{m}]$$

と書ける。

4. 単位元は、$[0]$ である。
5. $[i] \in \mathbb{Z}/m\mathbb{Z}$ の逆元 $-[i]$ について、以下が成り立つ。

$$-[i] = [m - i]$$

実際、 $[i] + [m - i] = [i + m - i] = [m] = [0]$ となる。

6. $m = 3$ のとき、

$+$	$[0]$	$[1]$	$[2]$
$[0]$	$[0]$	$[1]$	$[2]$
$[1]$	$[1]$	$[2]$	$\boxed{[0]}$
$[2]$	$[2]$	$\boxed{[0]}$	$\boxed{[1]}$

□

定義 17.20 (中心、 center)**.** 群 G に対して、$Z(G) = \{z \in G \mid zg = gz\ (\forall g \in G)\}$ を G の中心であるという。 □

命題 17.21. $Z(G)$ は可換群である。 □

例 17.22. 非可換群 $\mathcal{P}_1$（1 量子ビットのパウリ群）を考える。$\mathcal{P}_1$ は以下を満たす。

1. 元の集合は

$$\mathcal{P}_1 = \{\pm I, \pm iI, \pm X, \pm iX, \pm Y, \pm iY, \pm Z, \pm iZ\}$$

であり、位数は 16 である。

2. 群演算は、行列の通常の行列積で定義される。

3. 各元は以下の行列で与えられる。

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

4. 単位元は I である。

5. 各元の逆元は、エルミート共役で与えられる。たとえば $X^{-1} = X$, $Y^{-1} = Y$, $Z^{-1} = Z$, $(iI)^{-1} = -iI$。

6. 正規部分群（中心部分群）は次で与えられる。

$$Z(\mathcal{P}_1) = \{\pm I, \pm iI\}.$$

7. 商群

$$\mathcal{P}_1/Z(\mathcal{P}_1)$$

の各剰余類は次のように表される。

$$\begin{aligned}[I] &= \{\pm I, \pm iI\},\\ [X] &= \{\pm X, \pm iX\},\\ [Y] &= \{\pm Y, \pm iY\},\\ [Z] &= \{\pm Z, \pm iZ\}.\end{aligned}$$

$$\mathcal{P}_1/Z(\mathcal{P}_1) = \{[I], [X], [Y], [Z]\}$$

であり、符号や位相を無視したパウリ作用素群である。これは可換群であり、

$$\mathcal{P}_1/Z(\mathcal{P}_1) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$$

が成り立つ。

8. 例えば、位相を無視したパウリ作用素の積は次の表で与えられる。

$\times$	$[I]$	$[X]$	$[Y]$	$[Z]$
$[I]$	$[I]$	$[X]$	$[Y]$	$[Z]$
$[X]$	$[X]$	$[I]$	$[Z]$	$[Y]$
$[Y]$	$[Y]$	$[Z]$	$[I]$	$[X]$
$[Z]$	$[Z]$	$[Y]$	$[X]$	$[I]$

□

18 環 @07

前章で学んだ群や加群の概念を拡張し，加算と乗算という二つの演算を同時に扱う代数的構造を考える．このような構造は「環」と呼ばれ，整数や多項式など多くの数学的対象を統一的に扱う枠組みを与える．

定義 18.1 (環、単位的可換環)**.** 加算 $+$ と乗算 $\times$ が定義されている代数系 $(R, \{+, \times\})$ は、以下を満たすとき、環であると言う。

1. 代数系 $(R, +)$ は可換群、すなわち加群である。
2. 代数系 $(R, \times)$ は半群である。
3. 代数系 $(R, \{+, \times\})$ は、以下の分配律と呼ばれる性質を満たす。任意の $a_1, a_2, a_3 \in R$ に対して、以下を満たす。

$$a_1(a_2 + a_3) = a_1a_2 + a_1a_3$$
$$(a_1 + a_2)a_3 = a_1a_3 + a_2a_3$$

□

定義 18.2 (単位的環、単位的可換環)**.** 乗法に関して可換である環を、可換環という。乗法に関して単位元の存在を満たす環を、単位的環という。 □

例 18.3. 環に関する例と反例を与える。

1. 整数・有理数・複素数・実数の集合は、単位的可換環である。

2. 自然数の集合は、環ではない。

3. サイズ m の正方複素行列の集合 M_m は単位的非可換環である。

4. X を変数とする実数係数一変数多項式の集合 $\mathbb{R}[X]$ に対して、代数系 $(\mathbb{R}[X], \{+, \times\})$ は単位的可換環となる。加法の単位元は零多項式 $f(X) = 0$、乗法の単位元は定数多項式 $f(X) = 1$ になる。

5. m を 2 以上の整数として $\mathbb{Z}/m\mathbb{Z} = \{[0], [1], \ldots, [m-1]\}$ とし、$(\mathbb{Z}/m\mathbb{Z}, \{+, \times\})$ は単位的可換環となる。加法の単位元は $[0]$、乗法の単位元は $[1]$ である。

$$[i] + [j] \stackrel{\text{def}}{=} [i + j \bmod m]$$
$$[i] \times [j] \stackrel{\text{def}}{=} [i \times j \bmod m]$$

$m = 3$ のとき、

$+$	$[0]$	$[1]$	$[2]$
$[0]$	$[0]$	$[1]$	$[2]$
$[1]$	$[1]$	$[2]$	$[0]$
$[2]$	$[2]$	$[0]$	$[1]$

$\times$	$[0]$	$[1]$	$[2]$
$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$
$[2]$	$[0]$	$[2]$	$[1]$

6. 二つの環 R, S の直積 $R \times S$ とする。$(r_1, s_1), (r_2, s_2) \in R \times S$ についてそれら和と積を

$$(r_1, s_1) + (r_2, s_2) \stackrel{\text{def}}{=} (r_1 + r_2, s_1 + s_2)$$
$$(r_1, s_1) \times (r_2, s_2) \stackrel{\text{def}}{=} (r_1 \times r_2, s_1 \times s_2)$$

で定義した代数系 $(R \times S, \{+, \times\})$ は環になる。これを R, S の直積環と呼び、加法の単位元は $(0_R, 0_S)$、乗法の単位元は $(1_R, 1_S)$ になる。

□

19 体

環のうち，零でないすべての元が乗法に関して逆元をもつものを「体」という．体は，分数計算が可能な環とみなすことができ，線形代数や符号理論の基礎をなす重要な概念である．

定義 19.1 (体)**.** 代数系 $(\mathbb{F}, \{+, \times\})$ は以下を満たすとき、体であるという。有限なサイズの体を有限体という。

1. $(\mathbb{F}, +)$ は可換群である：
2. $(\mathbb{F} \setminus \{0\}, \times)$ は可換群である。

3. 分配則：任意の $a, b, c \in \mathbb{F}$ に対して、以下が成り立つ。

$$a(b+c) = ab + ac,$$
$$(a+b)c = ac + bc$$

□

5.3 で例をいくつか挙げました。

命題 19.2. 体 $\mathbb{F}$ と $x, y \in \mathbb{F}$ に対して、以下が成り立つ。

1. $-(-x) = x$
2. $x \times 0 = 0 \times x = 0$
3. $(-x) \times y = x \times (-y) = -(x \times y)$ である。系として $(-1) \times 1 = -1$ を得る。
4. $(-x) \times (-y) = x \times y$ である。系として $(-1) \times (-1) = 1$ を得る。
5. $\mathbb{F} \neq \{0\}$ ならば $0 \neq 1$ である。
6. $xy = 0$ ならば $x = 0$ or $y = 0$ である。

□

証明. 演習問題や試験問題で出す。 □

20　体を係数とする多項式環

体を係数とする多項式の集合は，自然な加法と乗法を備えた環をなす．このような環は「多項式環」と呼ばれ，有限体の構成や符号理論の多くの議論の基盤となる．

定義 20.1 (多項式環)**.** 体 $\mathbb{F}$ の元を係数に持つ有限の次数を有する多項式全体を $\mathbb{F}[X]$ と書く。正確には、体 $\mathbb{F}$ に対して、以下を定義する。

$$\mathbb{F}[X] = \left\{ \sum_{i=0}^{d} a_i X^i \mid d \geq 0, a_i \in \mathbb{F} \right\}$$

$(\mathbb{F}[X], \{+, \times\})$ は自然な加算と乗算によって単位的可換環となり、$\mathbb{F}$ 上の多項式環と呼ばれる。乗法単位元は $f(X) = 1$ であり、加法単位元は $f(X) = 0$ である。$f(X) = 0$ は零多項式と呼ばれる。

2 つの多項式

$$f(X) = \sum_{i=0}^{d} f_i X^i, g(X) = \sum_{i=0}^{e} g_i X^i$$

に対して、

$$d = e, f_i = g_i \text{ for } (i = 0, 1, \ldots, d)$$

のとき f と g は等しいといい、$f(X) = g(X)$ と書く。　□

定義 20.2 (モニック多項式)**.** 多項式 $f(X) = \sum_{i=0}^{d} f_i X^i \in \mathbb{F}[X]$ に対して、最大次数の係数 f_d が $1 \in \mathbb{F}$ である多項式はモニックであると言う。

$1 + X + X^2 \in \mathbb{F}_2[X]$ はモニック多項式で ある 。

$1 + X + 2X^2 \in \mathbb{F}_3[X]$ はモニック多項式で ない 。 □

命題 20.3 (多項式線形空間)**.** 自然にスカラー倍と和を定義することで、$\mathbb{F}[X]$ は $\mathbb{F}$ 上の線形空間となる。モニック単項式の集合

$$\{1, X, X^2, \dots\}$$

は $\mathbb{F}[X]$ の基底となる。 □

議論 20.4. 以下のような次数が有限でないものは一般に多項式ではない。これらは、形式的べき級数と呼ばれる。

$$\sum_{i=0}^{\infty} a_i X^i$$

形式的べき級数は、一般に $\mathbb{F}[X]$ に含まれていないことに注意しよう。

定義 20.5 (次数)**.** 多項式 $a(X) = \sum_{i=0}^{d} a_i X^i$ に対して、d を $a(X)$ の次数といい、$\deg a(X) = d$ と書く。$a(X) = 0$ に対して、$\deg a(X) \stackrel{\text{def}}{=} -\infty$ と定める。$\deg f(X) \leq 0$ であるとき、$f(X)$ は定数多項式であると言う。 □

例 20.6. 多項式環 $\mathbb{F}_2[X]$ の元に関する計算の例を挙げる。

$$\begin{aligned}&(X+X^2)+(1+X+X^3)\\&=1+(1+1)X+X^2+X^3\\&=1+X^2+X^3\end{aligned}$$

$$\begin{aligned}&(1+X)^2\\&=(1+X)\times(1+X)\\&=1+X+X+X^2\\&=1+(1+1)X+X^2=1+X^2\end{aligned}$$

$$\begin{aligned}&(1+X)^3\\&=(1+X)\times(1+X)\times(1+X)\\&=1+(\boxed{1+1+1})X+(\boxed{1+1+1})X^2+X^3\\&=\boxed{1+X+X^2+X^3}\end{aligned}$$

□

定義 20.7 (ベクトル表現、$\mathbb{F}[X;d]$)**.** 次数 d 未満の多項式

$$f(X)=\sum_{i=0}^{d-1}f_iX^i\in\mathbb{F}[X]$$

全体からなる集合を $\mathbb{F}[X;d]$ と書く。$f(X)$ に対して、長さ d の系列

$$(f_0,f_1,\ldots,f_{d-1})\in\mathbb{F}^{\deg f}$$

を $f(X)$ のベクトル表現という。これ以降、

$$f(X) \text{ と } (f_0, f_1, \ldots, f_{d-1})$$

を同一視して扱う。 □

例 20.8. $\mathbb{F}[X;d]$ が体になるように、$+, \times$ をうまく定義したい。$(\mathbb{F}[X], \{+, \times\})$ の拡張として $(\mathbb{F}[X;d], +)$ は加群になるが、$(\mathbb{F}[X;d], \times)$ は群にならない。例えば、$\mathbb{F} := \mathbb{F}_2, d = 3$ として、

$$(011) + (110) = \boxed{(101)} \in \mathbb{F}[X;d]$$

となるが、

$$(011) \times (110) = (0110) + (0011) = (0101) \notin \mathbb{F}[X;d]$$

となって、$\mathbb{F}[X;d]$ からはみ出してしまう。20.9 のように演算を定義すると、$(\mathbb{F}[X;d], \{+, \times\})$ は体になる。このような体の作り方を学んでいく。 □

21 イデアル

環の部分集合の中でも，加法や環の元との積に関して閉じている集合は特別な性質をもつ．これらを「イデアル」と呼び，環から商環を構成するための基本概念となる．

定義 21.1 (左イデアル)**.** 整数 $n > 0$ に対して、$n\mathbb{Z}$ は n の倍数となる整数の集合である。n の倍数どうしを足しても n の

```
+      | [000] [100] [010] [110] [001] [101] [011] [111]
-------+-------------------------------------------------
[000]  | [000] [100] [010] [110] [001] [101] [011] [111]
[100]  | [100] [000] [110] [010] [101] [001] [111] [011]
[010]  | [010] [110] [000] [100] [011] [111] [001] [101]
[110]  | [110] [010] [100] [000] [111] [011] [101] [001]
[001]  | [001] [101] [011] [111] [000] [100] [010] [110]
[101]  | [101] [001] [111] [011] [100] [000] [110] [010]
[011]  | [011] [111] [001] [101] [010] [110] [000] [100]
[111]  | [111] [011] [101] [001] [110] [010] [100] [000]


x      | [000] [100] [010] [110] [001] [101] [011] [111]
-------+-------------------------------------------------
[000]  | [000] [000] [000] [000] [000] [000] [000] [000]
[100]  | [000] [100] [010] [110] [001] [101] [011] [111]
[010]  | [000] [010] [001] [011] [110] [100] [111] [101]
[110]  | [000] [110] [011] [101] [111] [001] [100] [010]
[001]  | [000] [001] [110] [111] [011] [010] [101] [100]
[101]  | [000] [101] [100] [001] [010] [111] [110] [011]
[011]  | [000] [011] [111] [100] [101] [110] [010] [001]
[111]  | [000] [111] [101] [010] [100] [011] [001] [110]
```

図 20.9: 既約多項式 $1 + X + X^3$ で生成された有限体 $\mathbb{F}_{2^3}$

倍数になるので、$n\mathbb{Z}$ は加算に関して閉じている。n の倍数は任意の整数倍しても n の倍数である。この構造を抽象化したものがイデアルである。

環 $(R, \{+, \times\})$ の部分集合 $I \subset R$ が、加法群としての部分群であり、R のどの元を左からかけても、また I に含まるれとき、$(I, \{+, \times\})$ を左イデアルという。正確に述べると、部分集合 I で、

1. $(I, +)$ は加群である。

2. 積に関する閉性：$RI \subset I$ である。正確に述べると、以下が成り立つ。

$$rx \in I, \text{ for all } r \in R, x \in I \tag{21.2}$$

が成立するときに I を R の左イデアルと呼ぶ。同様に、(21.2) の RI を IR に置き換える、または rx を xr に置き換えることで右イデアルを定義する。 □

定義 21.3 (両側イデアル)**.** 環 $(R, \{+, \times\})$ の左イデアルかつ右イデアルであるものを、両側イデアルまたは単にイデアルという。可換環 R の部分集合 I が R の左イデアルまたは右イデアルならば、$IR = RI$ なので I は両側イデアルである。 □

例 21.4. 両側イデアルの例を与える。

1. 21.1 の前半に書かれていることにより、単位的可換環 $(\mathbb{Z}, \{+, \times\})$ に対して、$(m\mathbb{Z}, \{+, \times\})$ は両側イデアルであることが分かる。

2. 単位的可換環である $\mathbb{F}$ 係数多項式環 $(\mathbb{F}[X], \{+, \times\})$ と、非零多項式 $m(X) \in \mathbb{F}[X]$ に対して、以下が成り立つ。$m(X)$ 倍多項式集合を以下で定義する。

$$\langle m(X) \rangle := \{f(X)m(X) \mid f(X) \in \mathbb{F}[X]\}$$

このとき、$(\langle m(X) \rangle, \{+, \times\})$ は両側イデアルである。実際、$m(X)$ 倍多項式どうしを足しても $m(X)$ 倍多項式で

あるし、$m(X)$ 倍多項式に任意の多項式倍しても $m(X)$ 倍多項式である。

3. 2 つの可換環の間の準同型写像のカーネルは両側イデアルになる。(演習問題で扱います)

□

22 イデアルの生成系

イデアルは，しばしばいくつかの元の線形結合として生成することができる．この節では，イデアルを生成する集合や単項イデアルの概念を導入する．

定義 22.1 (イデアルの生成系、単項イデアル)**.** [19]環 R の部分集合 $X \subset R$ に対して、R を係数とする有限個の X の R 係数の線形結合からなる集合

$$\langle X \rangle = \{r_1 x_1 + \cdots + r_n x_n \mid n \in \mathbb{N}, r_i \in R, x_i \in X\}$$

は R の左イデアルとなり X によって生成されたイデアルと呼ばれ $\langle X \rangle$ と書く。環 R の単一の元 a により生成された R のイデアル $\{ra \mid r \in R\}$ は、単項イデアルといい、$\langle a \rangle$ と書く。□

[19]教員用メモ：左右イデアルは扱わないから，両側イデアルだけでいいのでは？

証明. $\langle X\rangle$ が R の左イデアルであることは、$\langle X\rangle$ の任意の元 (それぞれ n, m 個の X の R 係数の線形結合)

$$r_1x_1 + \cdots + r_nx_n \in \langle X\rangle$$
$$r'_1x'_1 + \cdots + r'_nx'_m \in \langle X\rangle$$

に対して、和

$$r_1x_1 + \cdots + r_nx_n + r'_1x'_1 + \cdots + r'_nx'_m$$

が $\langle X\rangle$ に含まれている ($n+m$ 個の X の R 係数の線形結合からなる集合) こと、$r \in R$ 倍が

$$r(r_1x_1 + \cdots + r_nx_n) = rr_1x_1 + \cdots + rr_nx_n \in \langle X\rangle$$

となることによって、確認できる。 □

例 22.2. 以下が成り立つ

1. 整数環 $\mathbb{Z}$ の整数 $m(>0) \in \mathbb{Z}$ に対して、$m\mathbb{Z}$ は m によって生成される単項両側イデアルである。$m\mathbb{Z} = \langle m\rangle$
2. 多項式環 $\mathbb{F}[X]$ の多項式 $m(X)(\neq 0) \in \mathbb{F}[X]$ に対して、$\langle m(X)\rangle$ は $m(X)$ によって生成される単項両側イデアルである。

□

23　剰余類環

群の商構造と同様に，環においてもイデアルを法とする剰余類を考えることができる．こうして得られる新たな環を「剰余類環」または「商環」と呼ぶ．剰余類環は有限体や商体の構成に不可欠な概念である．

群の正規部分群から商群を構成したように、環の両側イデアルから商環と呼ばれる新たな環を構成することができる。

定義 23.1 (イデアルを法として合同、商環、剰余類環 (residue class ring modulo))**.** 環 $(R, \{+, \times\})$ の両側イデアル I に対して，以下を定義する。I は加群 $(R, +)$ の部分群である。$(R, +)$ は 18.1 より可換群であったことを思い出そう。部分群 I は、可換群であり、17.6 より正規部分群であることが分かる。同値関係「正規部分群 I を法として合同」による同値類 R/I に対して、17.18 より $(R/I, +)$ は可換群となることが分かる。

両側イデアル I によって定まる商集合 $R/I = \{[r] \mid r \in R\}$ に自然に拡張された加法と乗法

$$[r_1] + [r_2] \stackrel{\text{def}}{=} [r_1 + r_2]$$
$$[r_1] \times [r_2] \stackrel{\text{def}}{=} [r_1 \times r_2]$$

からなる代数系 $(R/I, \{+, \times\})$ は環をなす。この環を I を法とする商環または剰余類環または単に剰余環という。　□

証明. まず、演算が矛盾無く定義 (well-defined) されているこ

とを示す。つまり、代表元の取り方に演算がよらないこと

$$\forall r, r', s, s' \in R,$$
$$[r] = [r'], [s] = [s'] \Longrightarrow [r+s] = [r'+s'] \tag{23.2}$$
$$[r] = [r'], [s] = [s'] \Longrightarrow [rs] = [r's'] \tag{23.3}$$

を示す。$(R, +)$ は可換群なので 17.6 から I は R の正規部分群となることがわかる。R, I を 17.18 における G, N とみなすと、(23.2) が成り立つことが分かる。

(23.3) を示す。$[r] = [r'], [s] = [s']$ すなわち $-r + r' = x \in I, -s + s' = y \in I$ となる $x, y \in I$ が存在するとして、$[rs] = [r's']$ を示す。I の左イデアル性から $ry \in I$、右イデアル性から $xs \in I$、左または右イデアル性から $xy \in I$ が分かる。したがって以下が成り立つ。

$$\begin{aligned} -(rs) + (r's') &= -(rs) + (r+x)(s+y) \\ &= -(rs) + rs + ry + xs + xy \\ &= ry + xs + xy \in I \end{aligned}$$

これは、$[rs] = [r's']$ を意味している。

次に、(17.17) と同様に R の乗算の結合則に帰着させて、$(R/I, \times)$ の結合則は確認できる。分配則も R の分配則に帰着して以下のように示せる。

$$\begin{aligned} &[a]([r] + [s]) = [a]([r+s]) = [a(r+s)] \\ &= [ar + as] = [ar] + [as] = [a][r] + [a][s] \end{aligned}$$

□

例 23.4. 単位的可換環 $(\mathbb{Z}, \{+, \times\})$ の両側イデアル $m\mathbb{Z}$ に対して、商環 $(\mathbb{Z}/m\mathbb{Z}, \{+, \times\})$ は以下を満たす。

1. $\mathbb{Z}/m\mathbb{Z} = \{[0], [1], \ldots, [m-1]\}$ と書ける。
2. $(\mathbb{Z}/m\mathbb{Z}, \{+, \times\})$ は以下で定義される演算によって、環となる。

$$[i] + [j] \stackrel{\text{def}}{=} [i + j] \text{ for } [i], [j] \in \mathbb{Z}/m\mathbb{Z}$$
$$[i] \times [j] \stackrel{\text{def}}{=} [i \times j] \text{ for } [i], [j] \in \mathbb{Z}/m\mathbb{Z}$$

3. $i, j \in \mathbb{Z}$ に対して、

$$[i] + [j] = (i + m\mathbb{Z}) + (j + m\mathbb{Z}) = [\boxed{i + j} \bmod \boxed{m}]$$
$$[i] \times [j] = (i + m\mathbb{Z}) \times (j + m\mathbb{Z}) = [\boxed{i \times j} \bmod \boxed{m}]$$

と書ける。

4. 加法単位元は $[0]$、乗法単位元は $[1]$ である。
5. $m = 3$ のとき、以下が成り立つ。

$+$	$[0]$	$[1]$	$[2]$
$[0]$	$[0]$	$[1]$	$[2]$
$[1]$	$[1]$	$[2]$	$\boxed{[0]}$
$[2]$	$[2]$	$\boxed{[0]}$	$\boxed{[1]}$

$\times$	$[0]$	$[1]$	$[2]$
$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$\boxed{[2]}$
$[2]$	$[0]$	$\boxed{[2]}$	$\boxed{[1]}$

□

例 23.5. 単位的可換環 $(\mathbb{F}[X], \{+, \times\})$ の両側イデアル $\langle m(X)\rangle$ に対して、商環 $(\mathbb{F}[X]/\langle m(X)\rangle, \{+, \times\})$ は以下を満たす。

1. $f(X) \in \mathbb{F}[X]$ に対して，以下が成り立つ。

$$\begin{aligned}
&[f(X)] \\
&= \{g(X) \in \mathbb{F}[X] \mid -g(X) + f(X) \in \langle m(X)\rangle\} \\
&= \{g(X) \in \mathbb{F}[X] \mid g(X) \equiv f(X) \bmod \langle m(X)\rangle\} \\
&= [f(X) \bmod m(X)]
\end{aligned}$$

2. 商環 $\mathbb{F}[X]/\langle m(X)\rangle$ は集合として次にようにかける。

$$\mathbb{F}[X]/\langle m(X)\rangle = \left\{ [f(X)] \middle| f(X) = \sum_{i=0}^{\deg m - 1} f_i X^i, f_i \in \mathbb{F} \right\}$$

3. $(\mathbb{F}[X]/\langle m(X)\rangle, \{+, \times\})$ は以下で定義される演算によって、環となる。$[a(X)], [b(X)] \in \mathbb{F}[X]/\langle m(X)\rangle$ に対して、

$$\begin{aligned}
[a(X)] + [b(X)] &\stackrel{\text{def}}{=} [a(X) + b(X)] \\
[a(X)] \times [b(X)] &\stackrel{\text{def}}{=} [a(X) \times b(X)]
\end{aligned}$$

と定義する。

4. $a(X), b(X) \in \mathbb{F}[X]$ に対して、

$$
\begin{aligned}
&[a(X)] + [b(X)] \\
&= \big(a(X) + b(X)\big) + \langle m(X)\rangle \\
&= [\boxed{a(X) + b(X)} \bmod \boxed{m(X)}] \\
&[a(X)] \times [b(X)] \\
&= \big(a(X) \times b(X)\big) + \langle m(X)\rangle \\
&= [\boxed{a(X) \times b(X)} \bmod \boxed{m(X)}]
\end{aligned}
$$

と書ける。

5. 加法単位元は $[0]$、乗法単位元は $[1]$ である。

6. $\mathbb{F} = \mathbb{F}_2, m(X) = 1 + X + X^2$ のとき、以下が成り立つ。

$+$	$[0]$	$[1]$	$[X]$	$[1+X]$
$[0]$	$[0]$	$[1]$	$[X]$	$[1+X]$
$[1]$	$[1]$	$[0]$	$[1+X]$	$[X]$
$[X]$	$[X]$	$[1+X]$	$\boxed{[0]}$	$\boxed{[1]}$
$[1+X]$	$[1+X]$	$[X]$	$\boxed{[1]}$	$\boxed{[0]}$

$\times$	$[0]$	$[1]$	$[X]$	$[1+X]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[X]$	$[1+X]$
$[X]$	$[0]$	$[X]$	$\boxed{[1+X]}$	$\boxed{[1]}$
$[1+X]$	$[0]$	$[1+X]$	$\boxed{[1]}$	$\boxed{[X]}$

$[1+X]\times[1+X]=[X]$ であることは以下から分かる。

$$
\begin{aligned}
&(1+X)(1+X)=1+X+X+X^2\\
&=1+(1+1)X+X^2=1+X^2\\
&(1+X^2)/(1+X+X^2)=\text{商}\,1\text{、剰余}\,X\\
&[1+X^2]=[X]
\end{aligned}
$$

ベクトル表現すると、以下の通りとなる。

$+$	$[00]$	$[10]$	$[01]$	$[11]$
$[00]$	$[00]$	$[10]$	$[01]$	$[11]$
$[10]$	$[10]$	$[00]$	$[11]$	$[01]$
$[01]$	$[01]$	$[11]$	$[00]$	$[10]$
$[11]$	$[11]$	$[01]$	$[10]$	$[00]$

$\times$	$[00]$	$[10]$	$[01]$	$[11]$
$[00]$	$[00]$	$[00]$	$[00]$	$[00]$
$[10]$	$[00]$	$[10]$	$[01]$	$[11]$
$[01]$	$[00]$	$[01]$	$[11]$	$[10]$
$[11]$	$[00]$	$[11]$	$[10]$	$[01]$

□

24　多項式環に関する性質

多項式環においても整数環と同様の除法や既約性の概念が成り立つ．この節では，多項式の除法アルゴリズムや既約多項式の性質を確認し，有限体構成への準備を行う．

命題 24.1 (剰余定理)**.** 任意の被除多項式 $n(X) \in \mathbb{F}[X]$ と非零な除多項式 $d(X) \in \mathbb{F}[X]$ に対して、

$$\begin{aligned} n(X) &= q(X)d(X) + r(X), \\ \deg r(X) &< \deg d(X) \end{aligned} \tag{24.2}$$

となる $q(X) \in \mathbb{F}[X]$ と $r(X) \in \mathbb{F}[X]$ が一意に存在する。このとき、$q(X) \in \mathbb{F}[X]$ を商 (quotient) 、$r(X) \in \mathbb{F}[X]$ を剰余 (remainder) といい、

$$n(X)/d(X) = \text{商 } q(X) \text{ 剰余 } r(X)$$

と書く。 □

証明. （存在性）実数係数多項式 $\mathbb{R}[X]$ において、$n(X), d(X)$ から $q(X), r(X)$ を求める筆算を思い出してみよう。

$$\begin{aligned} n(X) &= X^3 - 2X^2 + 0X - 4 \\ d(X) &= X - 3 \end{aligned}$$

とする。

$$
\begin{array}{r}
X^2+\ \ X+3 \\
\hline
X-3)X^3-2X^2+0X-4 \\
\underline{X^3-3X^2\qquad\qquad} \\
+X^2+0X \\
\underline{+X^2-3X\qquad} \\
+3X-4 \\
\underline{+3X-9} \\
+5
\end{array}
$$

各ステップ $i=1,2,\ldots$ で単項式 $q^{(i)}(X)$ と $d(X)$ の積を $n^{(i)}$ から引いていると見なせるので、

$$
\begin{aligned}
&n^{(0)}(X) := n(X) \\
&n^{(1)}(X) := n^{(0)}(X) - q^{(1)}(X)d(X) \\
&n^{(2)}(X) := n^{(1)}(X) - q^{(2)}(X)d(X) \\
&\quad\vdots \\
&n^{(i)}(X) = n^{(i-1)}(X) - q^{(i)}(X)d(X) \qquad (24.3)
\end{aligned}
$$

と書ける。上の例だと、

$$
\begin{aligned}
&q^{(1)}(X) = X^2, q^{(2)}(X) = X, q^{(3)}(X) = 3 \\
&n^{(1)}(X) = X^2 + 0X, n^{(2)}(X) = 3X - 4, n^{(3)} = 5
\end{aligned}
$$

となる。そして、ステップ k で、$d(X)$ の次数を下回ったら、すなわち

$$\deg n^{(k+1)}(X) < \deg d(X)$$

となったら、

$$q(X) := \sum_{i=1}^{k+1} q^{(i)}(X),$$
$$r(X) := n^{(k+1)}(X)$$

を出力する。次数が単調に減っていくので、多くても

$$\deg n(X) - \deg d(X)$$

ステップ以内にこの操作は終了する。この操作で得られた $(q(X), r(X))$ が (24.2) を満たすことは、(24.3) を次のように代入していくことにより確かめられる。

$$\begin{aligned}
&n(X)\\
&= n^{(0)}(X)\\
&= q^{(1)}(X)d(X) + n^{(1)}(X)\\
&= q^{(1)}(X)d(X) + q^{(2)}(X)d(X) + n^{(2)}(X)\\
&\vdots\\
&= q^{(1)}(X)d(X) + \cdots + q^{(k+1)}(X)d(X) + n^{(k+1)}(X)\\
&= \big(q^{(1)}(X) + \cdots + q^{(k+1)}(X)\big)d(X) + n^{(k+1)}(X)\\
&= q(X)d(X) + r(X)
\end{aligned}$$

（一意性）一致するとは限らない商と剰余の組を 2 つ $(q(X), r(X)), (q'(X), r'(X))$ を考える。つまり、

$$n(X) = q(X)d(X) + r(X), \qquad \deg r(X) < \deg d(X),$$
$$n(X) = q'(X)d(X) + r'(X), \qquad \deg r'(X) < \deg d(X)$$

である。この式より、

$$(q(X) - q'(X))d(X) = r(X) - r'(X) \tag{24.4}$$

を得る。$q(X) \neq q'(X)$ と仮定すると、左辺の次数が $\deg d(X)$ 以上になるが、右辺の次数は $\deg d(X)$ 未満とならなければならないから矛盾するので、$q(X) = q'(X)$ である。これと (24.4) より $r(X) = r'(X)$ も分かる。 □

整数環における素数に対応するものである、多項式環における既約多項式を定義する。

定義 24.5 (既約多項式、可約多項式)**.** 非定数多項式 $f(X) \in \mathbb{F}[X]$ に対して、どんな非定数多項式 $a(X), b(X)$ を用いても

$$f(X) = a(X)b(X)$$

と書けないとき、$f(X)$ は既約であるという。定数多項式 $f(X) \in \mathbb{F}[X]$ に対して、$f(X)$ は既約であるという。既約でない多項式 $f(X) \in \mathbb{F}[X]$ は可約であると言う。 □

例 24.6. 体 $\mathbb{F}$ によって $f(X) \in \mathbb{F}[X]$ が既約か可約かは変わる。

$$f(X) = X^2 + 1$$

は、

1. $\mathbb{F} = \mathbb{R}$ の場合、任意の $x \in \mathbb{R}$ に対して、$f(x) \geq 1$ なので、$\boxed{\text{既}}$約である。

2. $\mathbb{F} = \mathbb{C}$ の場合、$f(X) = \boxed{(X + \sqrt{-1})(X - \sqrt{-1})}$ なので、$\boxed{\text{可}}$約である。

3. $\mathbb{F} = \mathbb{F}_2$ の場合、$f(X) = \boxed{(X+1)(X+1)}$ なので、$\boxed{\text{可}}$約である。

□

定義 24.7 (約数、約多項式)**.** 非定数多項式 $f(X) \in \mathbb{F}[X]$ に対して、多項式 $a(X), b(X) \in \mathbb{F}[X]$ を用いて

$$f(X) = a(X)b(X)$$

と書けるとき、$f(X)$ は $a(X)$ で割り切れるといい、または $a(X)$ は $f(X)$ の約数または約多項式であると言い、$a(X) | f(X)$ と書く。 □

定義 24.8 (最大公約多項式)**.** $a(X), b(X) \in \mathbb{F}[X]$ に対して、$a(X), b(X)$ の約多項式の中で次数が最大のモニック多項式を、$a(X), b(X)$ の最大公約多項式と言い、$\gcd(a(X), b(X))$ と書く。$a(X) \neq 0$ に対して $\gcd(a(X), 0) = a(X)$ をモニック化した多項式、$\gcd(0, 0) = 0$ と定義する。 □

25　ユークリッドの互除法 @08

2つの整数 a, b の最大公約数を求めるアルゴリズムであるユークリッドの互除法 http://bit.ly/3Qu7t9Z は高校生のときに学んだと思います。

99221 と 97343 の最大公約数を g とする。拡張ユークリッドの互除法を用いて、$g = 99221x + 97343y$ となる整数 x, y を求めてみよう。

```
99221=1*97343+1878
97343=51*1878+1565
1878=1*1565+313
1565=5*313+0
g=313=52*99221+(-53*97343)
x=52
y=-53
```

この節では、2つの多項式 $a(X), b(X) \in \mathbb{F}[X]$ の最大公約多項式を求めるアルゴリズムに拡張することができることを学びましょう。整数に関するユークリッド互除法が有限の計算で終了することを保証する証明の要点は、整数 a と $b \neq 0$ に対して、$a = bq + r, 0 \leq r < |b|$ となる q, r が一意に定まることと、$|a| \leq |b|$ という性質を使っていることであった。この性質より、各割り算の商の絶対値は単調減少 $|r_0| \geq |r_1| > \cdots > |r_{m-1}| > |r_m|$ なので、ある m で $r_{m+1} = 0$ となりアル

ゴリズムは終了する。このような代数系をユークリッド整域 https://bit.ly/3snTFWi と言う。体 $\mathbb{F}$ を係数とする多項式の集合 $\mathbb{F}[X]$ の要素の $f(X)$ に対しても、絶対値の代わりに次数 $\deg(f)$ を考えれば、ユークリッド整域になる。この拡張によって、多項式 $f(X)$ と $g(X)$ の最大公約多項式がユークリッドの互除法によって計算できる。

定義 25.1 (多項式に対するユークリッドの互除法)**.** $r_1(X) \neq 0$ である 2 つの多項式 $r_0(X), r_1(X) \in \mathbb{F}[X]$ を入力とし、出力 $r_m(X)$ を出力する以下のアルゴリズムをユークリッドの互除法という。多項式 $f(X)$ を f と書く。以下の割り算を $i \geq 0$ に対して計算する。

$$r_i(X)/r_{i+1}(X) = \text{商 } q_{i+1}(X) \text{ 剰余 } r_{i+2}(X)$$

剰余定理 24.1 から $\deg r_{i+1} > \deg r_{i+2}$ となる。したがって、有限ステップで $\deg(r_{m+1}) = -\infty$ つまり $r_{m+1}(X) = 0$ とな

るはずである。割り切れるまで次の割り算を繰り返す。

$$
\begin{aligned}
r_0(X) &= \quad q_1(X)r_1(X) \quad + r_2(X), \\
r_1(X) &= \quad q_2(X)r_2(X) \quad + r_3(X), \\
&\vdots \\
r_i(X) &= q_{i+1}(X)r_{i+1}(X) + r_{i+2}(X) \\
&\vdots \\
r_{m-2}(X) &= q_{m-1}(X)r_{m-1}(X) + r_m(X) \\
r_{m-1}(X) &= \quad q_m(X)r_m(X) \quad + \overbrace{r_{m+1}(X)}^{=0}
\end{aligned}
\tag{25.2}
$$

□

命題 25.3. ユークリッドの互除法の出力 $r_m(X)$ は、$\mathbb{F}$ 値倍を除いて最大公約数多項式 $\gcd(r_0(X), r_1(X))$ に等しい。 □

証明. $r_m(X)$ をモニック化した多項式は $\gcd(r_m(X), 0)$ に等しいので、各第 i ステップ

$$r_i(X) := q_{i+1}(X)r_{i+1}(X) + r_{i+2}(X)$$

で、$r_i(X)$ と $r_{i+1}(X)$ の公約多項式全体の集合 C_i は $r_{i+1}(X)$ と $r_{i+2}(X)$ の公約多項式全体 C_{i+1} の集合に等しいことを示せば十分である。

$c(X) \in C_{i+1}$ ならば、$c(X) \mid r_{i+1}(X), c(X) \mid r_{i+2}(X)$ であ

るから[20]、

$$c(X) \mid q_{i+1}(X)r_{i+1}(X) + r_{i+2}(X) = r_i(X)$$

となり、$c(X) \in C_i$ が分かる。

逆に、$c(X) \in C_i$ ならば、$c(X) \mid r_i(X), c(X) \mid r_{i+1}(X)$ であるから、

$$c(X) \mid r_i(X) - q_{i+1}(X)r_{i+1}(X) = r_{i+2}(X)$$

となり、$c(X) \in C_{i+1}$ が分かる。

□

命題 25.4 (拡張ユークリッドの互除法). 2 つの多項式

$$r_0(X), r_1(X) \in \mathbb{F}[X]$$

に対して、最大公約多項式 $\gcd(r_0(X), r_1(X))$ の $r_0(X)$ と $r_1(X)$ による線形和表現 (ベズーの等式)

$$r_0(X)n_0(X) + r_1(X)n_1(X) = \gcd(r_0(X), r_1(X))$$

を与える $n_0(X), n_1(X) \in \mathbb{F}[X]$ が存在する。 □

[20] $d|n$ は d は n を割り切るを意味します。

証明. ユークリッド互除法 (25.2) を行列とベクトルによって表現し直すと、次のように書ける。

$$\begin{aligned}\vec{r}_0 &= Q_1\vec{r}_1\\ \vec{r}_1 &= Q_2\vec{r}_2\\ &\vdots\\ \vec{r}_{m-1} &= Q_m\vec{r}_m\end{aligned}$$

$$Q_i := \begin{pmatrix} q_i(X) & 1\\ 1 & 0\end{pmatrix}, \vec{r}_i := \begin{pmatrix} r_i(X)\\ r_{i+1}(X)\end{pmatrix}$$

これをまとめると、

$$\vec{r}_0 = Q_1\cdots Q_m\vec{r}_m$$

となる。$Q'_i := \begin{pmatrix} 0 & 1\\ 1 & -q_i(X)\end{pmatrix}$ とすれば、$Q'_iQ_i = I_2$ であるので、両辺に左から $Q'_m\cdots Q'_1$ をかけることにより次を得る。

$$Q'_m\cdots Q'_1\vec{r}_0 = \vec{r}_m \tag{25.5}$$

が成り立つ。$\begin{pmatrix} n_0(X) & n_1(X)\\ n_2(X) & n_3(X)\end{pmatrix} := Q'_m\cdots Q'_1$ とすれば、(25.5) の第 1 成分は

$$r_m(X) = \gcd(r_0, r_1) = n_0(X)r_0(X) + n_1(X)r_1(X)$$

という r_0 と r_1 の線形和の形で表現できる。ここで、第 1 等号は $\mathbb{F}$ 値定数倍を除いて等しいという意味である。 □

例 25.6. ユークリッドアルゴリズムと拡張ユークリッドアルゴリズムの例を与える．$r_0(X) = X^3 + X^2 + X + 1, r_1(X) = 3X^2 + 2 \in \mathbb{F}_5[X]$ に対して，

$$X^3 + X^2 + X + 1 = \left(3X^2 + 2\right)(2X + 2) + (2X + 2)$$
$$3X^2 + 2 = (2X + 2)(4X + 1) + (0)$$

となるので，$\gcd\left(X^3 + X^2 + X + 1,\quad 3X^2 + 2\right) = X + 1$ であり，$X + 1$ を $a(X), b(X)$ の線形和で表すと，

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

となる． □

26 有限体の構成

本節では，任意の体 $\mathbb{F}$ とその上の既約多項式 $p(X) \in \mathbb{F}[X]$ を用いて，剰余類環 $\mathbb{F}[X]/\langle p(X)\rangle$ が体を与えることを示す．次数 $\deg p = m$ の既約多項式を選べば，得られる拡大体のサイズは $|\mathbb{F}|^m$ となり，元は次数 m 未満の多項式の剰余類で表される．逆元の存在は $\gcd(a(X), p(X)) = 1$ とベズーの等式から従い，これにより剰余類環が**単位的可換環**を越えて**体**になることが分かる．最後に，素数体 $\mathbb{Z}/p\mathbb{Z}$ の構成に触れ，有限体のサイズが素数冪に限られる事実へとつなげる．

定理 26.1. 体 $\mathbb{F}$ を係数とする次数 $m \geq 1$ の~~モニックな~~既約多項式 $p(X) \in \mathbb{F}[X]$ に対して、イデアル $\langle p(X) \rangle$ を法とする剰余類環

$$\Big(\mathbb{F}[X]/\langle p(X) \rangle, \{+, \times\} \Big)$$

はサイズが $|\mathbb{F}|^{\deg p}$ の体となる。 □

証明. 23.5 より $(\mathbb{F}[X]/\langle p(X) \rangle, \{+, \times\})$ は単位的可換環になるので、非零元

$$[a(X)] (\neq [0]) \in \mathbb{F}[X]/\langle p(X) \rangle$$

に対して逆元が存在することを示せば十分である。$p(X)$ は既約なので、最大公約数 $\gcd(a(X), p(X)) = 1$ である。したがって、25.4 より，$y(X), z(X) \in \mathbb{F}[X]$ が存在して、

$$a(X)y(X) + p(X)z(X) = 1$$

となる。両辺 $\bmod\ p(X)$ すると

$$a(X)y(X) \bmod p(X) = 1 \bmod p(X)$$

となるから、

$$[a(X)][y(X)] = [a(X)y(X)] = [1]$$

となり、この $[y(X)] \in \mathbb{F}[X]/\langle p(X) \rangle$ が $[a(X)]$ の逆元となる。□

例 26.2. 既約多項式 $p(X) := 1 + X + X^3 \in \mathbb{F}_2[X]$ で生成された有限体 $\mathbb{F}_8 := \left(\mathbb{F}_2[X]/\langle p(X)\rangle, \{+, \times\}\right)$ の演算表を示す。

+	[000]	[100]	[010]	[110]	[001]	[101]	[011]	[111]
[000]	[000]	[100]	[010]	[110]	[001]	[101]	[011]	[111]
[100]	[100]	[000]	[110]	[010]	[101]	[001]	[111]	[011]
[010]	[010]	[110]	[000]	[100]	[011]	[111]	[001]	[101]
[110]	[110]	[010]	[100]	[000]	[111]	[011]	[101]	[001]
[001]	[001]	[101]	[011]	[111]	[000]	[100]	[010]	[110]
[101]	[101]	[001]	[111]	[011]	[100]	[000]	[110]	[010]
[011]	[011]	[111]	[001]	[101]	[010]	[110]	[000]	[100]
[111]	[111]	[011]	[101]	[001]	[110]	[010]	[100]	[000]

x	[000]	[100]	[010]	[110]	[001]	[101]	[011]	[111]
[000]	[000]	[000]	[000]	[000]	[000]	[000]	[000]	[000]
[100]	[000]	[100]	[010]	[110]	[001]	[101]	[011]	[111]
[010]	[000]	[010]	[001]	[011]	[110]	[100]	[111]	[101]
[110]	[000]	[110]	[011]	[101]	[111]	[001]	[100]	[010]
[001]	[000]	[001]	[110]	[111]	[011]	[010]	[101]	[100]
[101]	[000]	[101]	[100]	[001]	[010]	[111]	[110]	[011]
[011]	[000]	[011]	[111]	[100]	[101]	[110]	[010]	[001]
[111]	[000]	[111]	[101]	[010]	[100]	[011]	[001]	[110]

非ゼロ元 $x \in \mathbb{F}_8$ に対して，かけると単位元 $[100]$ になる，逆元 $x^{-1} \in \mathbb{F}_8$ が唯一存在することが分かる．以下は，前回の授業でやったことと同じなので，説明しない．ここで、$[f_0 f_1 f_2]$ は $[f_0 + f_1 X + f_2 X^2]$ を表していることに注意しよう。例：$[011] = [0 + X + X^2]$ である。$[011] \times [111] = [001]$ であるこ

とは以下より確かめることができる。

$$\begin{aligned}
[011] \times [111] &= [X + X^2] \times [1 + X + X^2] \\
&= [(X + X^2) \times (1 + X + X^2)] \\
&= [(X + X^2) + (X^2 + X^3) + (X^3 + X^4)] \\
&= [X + (1 + 1)X^2 + (1 + 1)X^3 + X^4] \\
&= [X + X^4 \bmod p(X)] \\
&= [X^2] \\
&= [001]
\end{aligned}$$

□

39.5 で証明を与えるが、有限体のサイズ q は素数のベキに限る。すでに 5.4 で天下り的に定義したが、素数サイズの有限体は次のように構成される。

例 26.3. $\mathbb{Z}$ の上の素数 p に対して、イデアル $p\mathbb{Z}$ を法とする剰余類環

$$\Big(\mathbb{Z}/p\mathbb{Z}, \{+, \times\}\Big)$$

はサイズ p の有限体をなす。例として $\mathbb{F}_{11} := \mathbb{Z}/11\mathbb{Z}$ の演算表を示す。

+	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]
[0]	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]
[1]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]	[0]
[2]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]	[0]	[1]
[3]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]	[0]	[1]	[2]
[4]	[4]	[5]	[6]	[7]	[8]	[9]	[10]	[0]	[1]	[2]	[3]
[5]	[5]	[6]	[7]	[8]	[9]	[10]	[0]	[1]	[2]	[3]	[4]
[6]	[6]	[7]	[8]	[9]	[10]	[0]	[1]	[2]	[3]	[4]	[5]
[7]	[7]	[8]	[9]	[10]	[0]	[1]	[2]	[3]	[4]	[5]	[6]
[8]	[8]	[9]	[10]	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]
[9]	[9]	[10]	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]
[10]	[10]	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]

x	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]
[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]
[2]	[0]	[2]	[4]	[6]	[8]	[10]	[1]	[3]	[5]	[7]	[9]
[3]	[0]	[3]	[6]	[9]	[1]	[4]	[7]	[10]	[2]	[5]	[8]
[4]	[0]	[4]	[8]	[1]	[5]	[9]	[2]	[6]	[10]	[3]	[7]
[5]	[0]	[5]	[10]	[4]	[9]	[3]	[8]	[2]	[7]	[1]	[6]
[6]	[0]	[6]	[1]	[7]	[2]	[8]	[3]	[9]	[4]	[10]	[5]
[7]	[0]	[7]	[3]	[10]	[6]	[2]	[9]	[5]	[1]	[8]	[4]
[8]	[0]	[8]	[5]	[2]	[10]	[7]	[4]	[1]	[9]	[6]	[3]
[9]	[0]	[9]	[7]	[5]	[3]	[1]	[10]	[8]	[6]	[4]	[2]
[10]	[0]	[10]	[9]	[8]	[7]	[6]	[5]	[4]	[3]	[2]	[1]

□

証明. $\mathbb{Z}/\langle p\rangle$ は単位的可換環になるので、非零元

$$[a] \in \mathbb{Z}/\langle p\rangle$$

に対して逆元が存在することを示せば十分である。p は素数なので、最大公約数 $\gcd(a,p) = 1$ である。したがって、$y, z \in \mathbb{Z}$

が存在して、

$$ay + pz = 1$$

となる。これより、

$$[a][y] = [1]$$

となり、この $[y] \in \mathbb{Z}/\langle p \rangle$ が $[a]$ の逆元となる。 □

27 因数定理と代数の基本定理

この節では，多項式の基本的な性質である因数定理と代数の基本定理を確認する．これらの結果は次節でリード・ソロモン符号（RS 符号）の性質を証明する際に繰り返し用いられる．証明自体は高校数学で学んだ実係数多項式の場合と同様であるため，ここでは簡単に述べるにとどめる．

補題 27.1 (因数定理と代数の基本定理)**.** 多項式 $f(X) \in \mathbb{F}[X]$ に対して $f(a) = 0$ であるとき、$a \in \mathbb{F}$ は $f(X)$ の根であると言う。因数定理: 多項式 $(X - a)|f(X)$ となることと $f(a) = 0$ となることは同値である．代数の基本定理: 体 $\mathbb{F}$ の上の n 次多項式は $\mathbb{F}$ の上で高々n 個の相違なる根を有する。

証明. $a \in \mathbb{F}$ を多項式 $f(X) \in \mathbb{F}[X]$ の根とする。このとき、$d(X) := X - a$ として剰余定理 24.1 を使用すると、

$$\begin{aligned} f(X) &= q(X)(X - a) + r(X), \\ \deg r(X) &< \deg d(X) = 1 \end{aligned} \tag{27.2}$$

となる、$q(X), r(X) \in \mathbb{F}[X]$ が唯一存在することが分かる。(27.2) より r は定数多項式 $r(X) = r_0$ となる。$a \in \mathbb{F}$ は $f(X)$ の根:$f(a) = 0$ であるから、$f(a) = r_0$ となる。こうして、因数定理

$$f(a) = 0 \Rightarrow f(X) = q(X)(X - a), \deg q(X) = n - 1$$

を得る。逆は明らか．$q(X)$ の次数は $f(X)$ の次数より 1 だけ小さい．$q(X)$ について同様の議論をしていくと、いつか根を持たないようになる．根 1 つにつき次数を少なくとも 1 つ消費する必要があるので、体 $\mathbb{F}$ の上の n 次多項式は $\mathbb{F}$ の上で高々 n 個の相違なる根を有する。 □

28 リード・ソロモン符号、RS 符号

この節では、有限体上の代表的な代数符号である**リード・ソロモン符号（Reed–Solomon code, RS 符号）を導入する。RS 符号は、有限体上の多項式評価によって構成され、符号長 n・情報長 k の線形符号として定義される。また、RS 符号は最大距離分離符号（MDS 符号）**の一種であり、最小距離がシングルトン限界に一致するという優れた性質をもつ。本節では、RS 符号の定義・基底・生成行列を示し、その最小距離と復号アルゴリズムについて説明する。

定義 28.1 (RS 符号、リード・ソロモン符号). $\alpha_1, \ldots, \alpha_n$ を評価点と呼び、互いに異なる $\mathbb{F}_q$ の元とする．このため、$n \leq q$

となる。$\mathbb{F}_q[X;k]$ は $\mathbb{F}_q$ を係数とする次数が k 未満の多項式

$$f(X) = \sum_{i=0}^{k-1} f_i X^i, \quad f_i \in \mathbb{F}_q$$

の集合である。情報多項式 $f(X) \in \mathbb{F}_q[X;k]$ に対して、評価点 $\alpha_1, \ldots, \alpha_n$ における多項式 $f(X)$ の評価値ベクトル

$$\vec{c}(f) := \big(f(\alpha_1), f(\alpha_2), \ldots, f(\alpha_n)\big) \in \mathbb{F}_q^n$$

を符号語とする符号空間を、$\mathbb{F}_q$ 上の $[n,k]$RS 符号という。正確に書くと、

$$\Big\{\vec{c}(f) \in \mathbb{F}_q^n \mid f(X) \in \mathbb{F}_q[X;k]\Big\}$$

として定義される。 □

定義 28.3 (RS 符号を使った通信システム)**.** RS 符号を使った通信システムは以下の構成要素からなる。

- 送信器
  1. 情報ベクトル $\vec{f} := (f_0, \ldots, f_{k-1}) \in \mathbb{F}_q^k$ から、
  2. 情報多項式 $f(X) \in \mathbb{F}_q[X;k]$ を求める。
  3. 情報多項式 $\vec{f}$ に対応する符号語 $\vec{c}(\vec{f}) \in \mathbb{F}_q^n$ を計算して、通信路に入力する。
- 通信路：通信路は入力 $\vec{c}$ にエラーベクトル $\vec{e} \in \mathbb{F}_q^n$ を加えた出力 $\vec{r} = \vec{c} + \vec{e}$ を出力する。

- 受信器

  1. 通信路出力である受信語 $r \in \mathbb{F}_q^n$ から推定送信語 $\hat{c}(\vec{r}) \in \mathbb{F}_q^n$ を推定する。
  2. $\hat{c}(\vec{r})$ に対応する f、正確に述べると $\hat{c}(r) = c(\hat{f})$ となる推定情報多項式 $\hat{f}(X)$ または等価的に推定情報ベクトル $\hat{f}$ を求める。

□

定理 28.4 (RS 符号の基底)**.** 評価点 $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{F}_q$ によって定義される $\mathbb{F}_q$ 上の $[n, k]$RS 符号 C に対して、以下が成り立つ。

1. C は $\mathbb{F}_q$ 上の $[n, k]$ 線形符号になる。
2. 以下の符号語の集合は、C の基底となる.

$$\left\{\vec{c}(f) \in \mathbb{F}_q^n \mid f(X) \in \{1, X, X^2, \ldots, X^{k-1}\}\right\} \subset C$$
$$\vec{c}(f) := \big(f(\alpha_1), \ldots, f(\alpha_n)\big) \in \mathbb{F}_q^n$$

この基底の符号語を具体的に並べると、

$$\begin{aligned}\{&(1, 1, \ldots, 1),\\ &(\alpha_1, \alpha_2, \ldots, \alpha_n),\\ &(\alpha_1^2, \alpha_2^2, \ldots, \alpha_n^2),\\ &\quad\vdots\\ &(\alpha_1^{k-1}, \alpha_2^{k-1}, \ldots, \alpha_n^{k-1})\}\end{aligned} \tag{28.5}$$

となる。

3. C の生成行列は C の基底ベクトルを行ベクトルとして並べた行列なので、以下の行列は C の生成行列となる。

$$G = \begin{bmatrix} \alpha_1^0 & \alpha_2^0 & \dots & \alpha_n^0 \\ \alpha_1^1 & \alpha_2^1 & \dots & \alpha_n^1 \\ \alpha_1^2 & \alpha_2^2 & \dots & \alpha_n^2 \\ \vdots & \ddots & \ddots & \vdots \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \dots & \alpha_n^{k-1} \end{bmatrix}$$

ただし、$0^0 = 1$ とする。この生成行列 G を使って情報ベクトル $\vec{f}$ から符号語 $\vec{c}(\vec{f}) = \vec{f}G$ に直接、符号化することができる。

□

証明. 1. $\mathbb{F}_q[X;k]$ は $\mathbb{F}_q$ 上の k 次元線形空間であったことを思い出そう。$\mathbb{F}_q[X;k]$ からの写像

$$\phi : \mathbb{F}_q[X;k] \ni f(X) \mapsto (f(\alpha_1), \dots, f(\alpha_n)) \in \mathbb{F}_q^n$$

を定義する[21]。$\phi(\mathbb{F}_q[X;k]) = C$ である。したがって、ϕ が線形全単射であることを示せば十分である。

[21] これは上で符号語 $c(f)$ と書いていたものを多項式からベクトルへの写像であることを強調して $\phi(f)$ と書いただけである.

線形性：

$$\begin{aligned}\phi(af) &= \big(af(X)|_{X=\alpha_1}, \ldots, af(X)|_{X=\alpha_n}\big)\\ &= \big((af)(\alpha_1), \ldots, (af)(\alpha_n)\big)\\ &= (af(\alpha_1), \ldots, af(\alpha_n))\\ &= a(f(\alpha_1), \ldots, f(\alpha_n))\\ &= a\phi(f)\end{aligned}$$

$$\begin{aligned}&\phi(f_1 + f_2)\\ &= \big((f_1 + f_2)(\alpha_1), \ldots, (f_1 + f_2)(\alpha_n)\big)\\ &= (f_1(\alpha_1) + f_2(\alpha_1), \ldots, f_1(\alpha_n) + f_2(\alpha_n))\\ &= \phi(f_1) + \phi(f_2)\end{aligned}$$

全単射性：$\phi(f_1(X)) = \phi(f_2(X))$ ならば $f_1(X) = f_2(X)$ を示せば良い.

$$\begin{aligned}&\big(f_1(\alpha_1), \ldots, f_1(\alpha_n)\big) = \big(f_2(\alpha_1), \ldots, f_2(\alpha_n)\big)\\ &\Rightarrow \big((f_1 - f_2)(\alpha_1), \ldots, (f_1 - f_2)(\alpha_n)\big) = (0, \ldots, 0)\\ &\overset{\text{(a)}}{\Rightarrow} (f_1 - f_2)(X) = 0\\ &\Rightarrow f_1(X) = f_2(X)\end{aligned}$$

(a) では、$(f_1 - f_2) \in \mathbb{F}_q[X; k]$ と代数の基本定理 (次数 k 未満の非零多項式の根の数は k 未満である) を次のように使った．$(f_1 - f_2)$ は k 次未満の多項式である．(a) の直

前の式より，$(f_1 - f_2)$ は $n(\geq k)$ 個の根を持っているので，非ゼロ多項式ではありえない．したがって，$(f_1 - f_2)$ は零多項式である:$(f_1 - f_2)(X) = 0$。

2. $\mathbb{F}_q[X;k]$ の単項式からなる集合

$$B := \{1, X, X^2, \ldots, X^{k-1}\}$$

は $\mathbb{F}_q[X;k]$ の基底である。一般に、ある線形空間 V の基底を線形全単射で別の線形空間 W に移したベクトルの集合は W の基底になる。ここでは、

$$\{\phi(f) \mid f(X) \in B\}$$

が C の基底になることになるが、これは (28.5) と一致する。

3. 生成行列の作り方 7.5 と前項より明らか。

□

例 28.6 (RS 符号)**.** $\mathbb{F}_{11} := \mathbb{Z}/11\mathbb{Z} = \{[0], [1], \ldots, [10]\}$ 上の $[n = 8, k = 4]$ RS 符号の生成行列 G は以下で与えられる。ただし、

$$\alpha_1 = [0], \alpha_2 = [1], \ldots, \alpha_8 = [7]$$

と選んだ。

$$G = \begin{pmatrix} [1][1][1][1][1][1][1][1] \\ [0][1][2][3][4][5][6][7] \\ [0][1][4][9][5][3][3][5] \\ [0][1][8][5][9][4][7][2] \end{pmatrix}$$

□

例 28.7 (RS 符号)**.** 既約多項式 $p(X) = 1 + X^2 + X^3 \in \mathbb{F}_2[X]$ によって定義される

$$\mathbb{F}_8 := \mathbb{F}_2[X]/\langle p(X) \rangle = \{[000], [100], \ldots, [111]\}$$

上の $[n = 8, k = 4]$ RS 符号の生成行列 G は以下で与えられる。ただし、

$$\alpha_1 = [000], \alpha_2 = [100], \ldots, \alpha_8 = [111]$$

と選んだ。

$$G = \begin{pmatrix} [100][100][100][100][100][100][100][100] \\ [000][100][010][110][001][101][011][111] \\ [000][100][001][101][111][011][110][010] \\ [000][100][101][010][011][001][111][110] \end{pmatrix}$$

□

定理 28.8 (RS 符号の最小距離)**.** $[n,k]$RS 符号 C の任意の非ゼロ符号語 $\vec{x}(\neq \vec{0}) \in C$ のハミング重み $w(\vec{x})$ に関して以下が成り立つ。

$$w(\vec{x}) \geq n-k+1$$

したがって、

$$w_{\min}(C) = d_{\min}(C) \geq n-k+1$$

となる。シングルトン限界 13.1$d_{\min}(C) \leq n-k+1$ より、結局

$$d_{\min}(C) = n-k+1$$

となる。つまり、RS 符号は最大距離分離符号 (MDS 符号) となる。 □

証明. $f(X)$ から $(f(\alpha_1),\ldots,f(\alpha_n))$ に移す写像 ϕ は線形全単射であった (28.4 の証明参照) から，C の非ゼロ符号語は、

$$\vec{x}(f) = \big(f(\alpha_1),\ldots,f(\alpha_n)\big) \neq (0,\ldots,0)$$
$$\text{with } f(X)(\neq 0) \in \mathbb{F}_q[X;k]$$

と書ける。この非零符号語の重み、言い換えると $f(\alpha_i) \neq 0$ となる i $(1 \leq i \leq n)$ の個数を調べよう。まず次の事実を確認しよう。

- 零多項式は零符号語となる。いいかえると、

$$\phi(0) =: \mathbb{F}_q[X;k] \ni 0 \mapsto (0,\ldots,0) \in \mathbb{F}_q^n$$

である。しかるに対偶を考えれば、非零符号語は非零多項式から生成されることが分かる。

- 次数 k 未満の非ゼロ多項式 $f(X)$ の根の個数は k 未満である

- 評価点 $\alpha_1,\ldots,\alpha_n$ は全て異なる

これらのことから、非ゼロ符号語 $\vec{x}(f)$ の第 i 成分がゼロとなる、すなわち $f(\alpha_i)=0$ となる i $(1\le i\le n)$ の個数は k 未満であることが分かる．言い換えると，$f(\alpha_i)\neq 0$ となる i $(1\le i\le n)$ の個数は $n-k+1$ 以上である．こうして，$w(\vec{x})\ge n-k+1$ が示せた． □

29 RS 符号の復号アルゴリズム

RS 符号の復号は、「誤りが混入した評価値列 $r_1,\ldots,r_n$ から、もとの多項式 $f(X)$ を再構成する」問題である。送信側では、情報多項式 $f(X)\in\mathbb{F}_q[X;k]$ の評価

$$c_i = f(\alpha_i), \quad i=1,\ldots,n$$

を送るが、受信側では誤りベクトル $\vec{e}$ が加わって

$$r_i = c_i + e_i = f(\alpha_i) + e_i$$

が観測される。目標は、誤りの少ない場合に正しい $f(X)$ を取り戻すことである。

29.1　補間の立場からの導入

誤りが全く無いとき、受信点 (α_i, r_i) はすべて $(\alpha_i, f(\alpha_i))$ である。したがって、n 個の点 (α_i, r_i) を通る次数 $< n$ の多項式 $g(X)$ を補間すれば、ただちに $g(X) = f(X)$ が得られる。このときの $g(X)$ はラグランジュ補間多項式（有限体でも実数でも「任意の n 点を通る多項式は次数 $< n$ で一意に存在」します。）

$$g(X) = \sum_{i=1}^{n} r_i \, \ell_i(X), \quad \ell_i(X) = \prod_{\substack{1 \le j \le n \\ j \neq i}} \frac{X - \alpha_j}{\alpha_i - \alpha_j}$$

で与えられる。

しかし、受信語に誤りが含まれると一部の r_i は $f(\alpha_i)$ と異なり、もはや低次数 $(< k)$ の多項式では全点を同時に通れない。このとき高次数 $(\ge k)$ の $g(X)$ を補間すれば全点 (α_i, r_i) for $i = 1, \ldots, n$ は通るが、$g(X)$ は本来の $f(X)$ とは異なる。ここで次の発想に切り替える。

29.2　二変数補間多項式の導入

受信点列 (α_i, r_i) 全てを「ある二変数多項式の零点」として表すことを考える。すなわち、係数が $\mathbb{F}_q$ に属する多項式

$$Q(X, Y) = Q_0(X) + Q_1(X)Y$$

を用意し、

$$Q(\alpha_i, r_i) = 0 \quad (i = 1, \ldots, n)$$

を満たすように定義する。このとき $Q(X, Y) = 0$ は平面上の曲線を定め、$Y = g(X)$ のグラフ上の全ての点 (α_i, r_i) で値が 0 になる。言い換えると、$Q(X, Y)$ は $Y = g(X)$ のグラフを「消す=0 にする」（vanish する）多項式である。

誤りが少なければ、多くの点 $(\alpha_i, f(\alpha_i))$ もこの曲線上に存在する。したがって $Q(X, f(X)) = Q_0(X) + f(X)Q_1(X)$ は多数の根を持ち、次数条件を適切に設定すれば恒等的に 0 でなければならない。その結果、次の関係が導かれる。

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

これが RS 符号の限界距離復号アルゴリズムの核心的な考え方である。

この節では、まず補間多項式 $Q(X, Y)$ の存在を示し、その構成法と次数制約を定めた上で、正しい $f(X)$ がどのように回復されるかを数学的に証明する。

補題 29.1 (RS 符号に対する限界距離復号アルゴリズム (Berlekamp–Welch 型)). n 個の異なる評価点 $\alpha_1, \ldots, \alpha_n$ によって定義された $\mathbb{F}$ 上の $[n,k]$RS 符号 C に対して、訂正能力は

$$t(C) = \left\lfloor \frac{d(C)-1}{2} \right\rfloor = \left\lfloor \frac{n-k}{2} \right\rfloor$$

である。情報多項式 $f(X) \in \mathbb{F}[X;k]$ が符号化された送信語 $\vec{c} = (f(\alpha_1), \ldots, f(\alpha_n)) \in C$ が送られて、誤りベクトル $\vec{e}$ が加えられた受信語 $\vec{r} = \vec{c} + \vec{e} \in \mathbb{F}^n$ を受信した通信シナリオを考えよう。以下のアルゴリズムは、受信語 $(r_1, \ldots, r_n) \in \mathbb{F}$ を入力とし、推定符号語 $\hat{\vec{c}}$ または等価的に $\hat{\vec{c}} = (\hat{f}(\alpha_1), \ldots, \hat{f}(\alpha_n))$ となる推定情報多項式 $\hat{f} \in \mathbb{F}[X;k]$ を出力するアルゴリズムである。誤りの重みが t 以下の場合、このアルゴリズムは正しく復号結果を出力する:$\hat{f}(X) = f(X)$。

1. まず、

$$Q(\alpha_i, r_i) = 0, \text{ for } i = 1, \ldots, n \tag{29.2}$$

$$\deg Q_0 < n - t \tag{29.3}$$

$$\deg Q_1 < t + 1 \tag{29.4}$$

を満たす $\mathbb{F}_q$ を係数とする非ゼロ二変数多項式

$$Q(X,Y) = Q_0(X) + Q_1(X)Y \in \mathbb{F}[X,Y] \tag{29.5}$$

が存在するので、このような $Q(X,Y)$ を一つ求める。$Q(X,Y)$ は補完多項式と呼ばれる。補完多項式 $Q(X,Y)$ の存在と求め方は、証明で述べる。

2. 次に、推定情報多項式を

$$\hat{f}(X) := -Q_0(X)/Q_1(X)$$

によって計算し (この割り算が割り切れることは証明します)、送信された符号語を

$$\hat{\vec{c}} := (\hat{f}(\alpha_1), \ldots, \hat{f}(\alpha_n))$$

と推定する。

22

証明. 【補間多項式の存在】$Q_1(X)$ と $Q_0(X)$ の係数を次のように名前をつける。

$$Q_0(X) = \sum_{i \geq 0} q_{0,i} X^i \in \mathbb{F}[X; n-t]$$
$$Q_1(X) = \sum_{i \geq 0} q_{1,i} X^i \in \mathbb{F}[X; t+1]$$

(29.2) は，多項式 $Q_1(X), Q_0(X)$ のそれぞれの係数ベクトル $\vec{q}_0, \vec{q}_1$ を変数とみなした連立数 n、変数が $n+1$ 個の以下の同次線形方程式である.

$$A\vec{q} = \vec{0} \text{ または } A_0\vec{q}_0 + A_1\vec{q}_1 = \vec{0} \qquad (29.6)$$

[22]推定誤りベクトル $\hat{\vec{e}} := \vec{r} - \hat{\vec{c}}$ の重みが t を超えていたら、復号結果をエラーとすることでこの復号法は復号半径 $t(C)$ の限界距離復号と一致する。

ただし、

$$
\begin{aligned}
&A := (A_0\ A_1) \in \mathbb{F}^{n\times n+1}, \vec{q} := (\vec{q}_0\ \vec{q}_1)\\
&\vec{q}_0 := (q_{0,0}, \ldots, q_{0,n-t-1}) \in \mathbb{F}^{n-t}\\
&\vec{q}_1 := (q_{1,0}, \ldots, q_{1,t}) \in \mathbb{F}^{t+1}
\end{aligned}
$$

である。A のランクが n 以下であることと次元定理から、この線形方程式の解空間の次元は 1 以上となるので、非零解を含むはずである。

$$
A_0 := \begin{pmatrix}
\alpha_1^0 & \alpha_1^1 & \alpha_1^2 & \cdots & \alpha_1^{n-t-1}\\
\alpha_2^0 & \alpha_2^1 & \alpha_2^2 & \cdots & \alpha_2^{n-t-1}\\
\vdots & \vdots & \vdots & & \vdots\\
\alpha_n^0 & \alpha_n^1 & \alpha_n^2 & \cdots & \alpha_n^{n-t-1}
\end{pmatrix} \in \mathbb{F}^{n\times n-t}
$$

$$
A_1 := \begin{pmatrix}
r_1 & r_1\alpha_1 & r_1\alpha_1^2 & \cdots & r_1\alpha_1^t\\
r_2 & r_2\alpha_2 & r_2\alpha_2^2 & \cdots & r_2\alpha_2^t\\
\vdots & \vdots & \vdots & & \vdots\\
r_n & r_n\alpha_n & r_n\alpha_n^2 & \cdots & r_n\alpha_n^t
\end{pmatrix} \in \mathbb{F}^{n\times t+1}
$$

A を復号行列と呼ぶ。この線形方程式 (29.6) を解いて、非ゼロ解 $\vec{q} = (\vec{q}_0, \vec{q}_1)$ を一つ求めて、(29.5) に代入して補完多項式 $Q(X, Y)$ を得る。

【推定符号語が正しいこと:$f(X) = \hat{f}(X)$】誤りの数を $w := w(\vec{e}) \leq t$ と書く。受信語 $(r_1, \ldots, r_n)$ の $n - w$ 個の要素は誤っていないので，$n - w$ 個の $i \in \{1, \ldots, n\}$ について第 i

受信シンボル r_i と第 i 送信シンボル c_i が一致する、すなわち $r_i = c_i = f(\alpha_i)$ である。従って (29.2) より，$n - w(\geq n - t)$ 個の添字 i について $Q(\alpha_i, f(\alpha_i)) = 0$ である。これより，以下が成り立つことが分かる。

$$Q(X, f(X)) \text{ は } n - t \text{ 個以上の異なる根を持つ} \quad (29.7)$$

$Q_1(X)$ と $Q_0(X)$ の次数に関する制限 (29.4) と (29.3) より，$\deg Q(X, f(X))$ は $n-t$ 未満である。代数の基本定理より、次数が $n - t$ 未満の非ゼロ多項式の解の数は $n - t$ 未満でなければならない。一方、(29.7) も成り立つので、$Q(X, f(X))$ はゼロ多項式でなければならない．言い換えると，

$$0 = Q\big(X, f(X)\big) = Q_0(X) + f(X)Q_1(X)$$

となり，$Q_0(X)/Q_1(X)$ は割りきれるはずである。これより、$f(X) = -Q_0(X)/Q_1(X) = \hat{f}(X)$ を得る． □

議論 29.8 (RS 符号の復号手続きは効率的である)**.** 変数の数は高々符号長 n の 2 倍であり、変数が m 個の線形連立方程式は約 m^3 の手間 (有限体の四則演算) で解けるから、符号語をしらみ潰しに調べる安直な方法に比べて、上記の手順は遥かに効率が良い。しかし、実際の製品では更に高速な手順が通常用いられる。

例 29.9 (RS 符号の復号)**.** $\mathbb{F}_{11} := \mathbb{Z}/11\mathbb{Z} = \{[0], [1], \ldots, [10]\}$ 上の $[n = 8, k = 4]$ RS 符号に対して $d = n - k + 1 = 5, t = 2$

である．生成行列 G は以下で与えられる。ただし、

$$\alpha_1 = [0], \alpha_2 = [1], \ldots, \alpha_8 = [7]$$

と選んだ。

$$G = \begin{pmatrix} [1][1][1][1][1][1][1][1] \\ [0][1][2][3][4][5][6][7] \\ [0][1][4][9][5][3][3][5] \\ [0][1][8][5][9][4][7][2] \end{pmatrix}$$

情報ベクトル	$f = [5][6][9][6]$
符号語	$c = [5][4][2][2][7][9][0][5]$
誤りベクトル	$e = [7][0][0][5][0][0][0][0]$
受信語	$r = [1][4][2][7][7][9][0][5]$

とすると、復号行列 A は以下の通りとなる。

$$A = \begin{pmatrix} [1]\,[0]\,[0]\,[0]\,[0]\,\,[0]\,\,[1]\,\,[0]\,\,[0] \\ [1]\,[1]\,[1]\,[1]\,[1]\,\,[1]\,\,[4]\,\,[4]\,\,[4] \\ [1]\,[2]\,[4]\,[8]\,[5]\,[10]\,[2]\,\,[4]\,\,[8] \\ [1]\,[3]\,[9]\,[5]\,[4]\,\,[1]\,\,[7]\,[10]\,[8] \\ [1]\,[4]\,[5]\,[9]\,[3]\,\,[1]\,\,[7]\,\,[6]\,\,[2] \\ [1]\,[5]\,[3]\,[4]\,[9]\,\,[1]\,\,[9]\,\,[1]\,\,[5] \\ [1]\,[6]\,[3]\,[7]\,[9]\,[10]\,[0]\,\,[0]\,\,[0] \\ [1]\,[7]\,[5]\,[2]\,[3]\,[10]\,[5]\,\,[2]\,\,[3] \end{pmatrix}$$

$$\overset{\text{行基本変形}}{\Longrightarrow}\begin{pmatrix}
[1] & [0] & [0] & [0] & [0] & [0] & [1] & [0] & [0] \\
[0] & [1] & [1] & [1] & [1] & [1] & [3] & [4] & [4] \\
[0] & [0] & [1] & [3] & [7] & [4] & [3] & [9] & [0] \\
[0] & [0] & [0] & [1] & [6] & [3] & [2] & [9] & [3] \\
[0] & [0] & [0] & [0] & [1] & [10] & [10] & [9] & [1] \\
[0] & [0] & [0] & [0] & [0] & [1] & [1] & [4] & [7] \\
[0] & [0] & [0] & [0] & [0] & [0] & [1] & [5] & [4] \\
[0] & [0] & [0] & [0] & [0] & [0] & [0] & [1] & [3]
\end{pmatrix}$$

$$\overset{\text{行基本変形}}{\Longrightarrow}\begin{pmatrix}
[1] & [0] & [0] & [0] & [0] & [0] & [0] & [0] & [0] \\
[0] & [1] & [0] & [0] & [0] & [0] & [0] & [0] & [7] \\
[0] & [0] & [1] & [0] & [0] & [0] & [0] & [0] & [9] \\
[0] & [0] & [0] & [1] & [0] & [0] & [0] & [0] & [1] \\
[0] & [0] & [0] & [0] & [1] & [0] & [0] & [0] & [2] \\
[0] & [0] & [0] & [0] & [0] & [1] & [0] & [0] & [6] \\
[0] & [0] & [0] & [0] & [0] & [0] & [1] & [0] & [0] \\
[0] & [0] & [0] & [0] & [0] & [0] & [0] & [1] & [3]
\end{pmatrix}$$

$A\vec{q} = \vec{0}$ の非零解を一つ選んで、

$$\vec{q}_0 = [0][4][2][10][9][5]$$
$$\vec{q}_1 = [0][8][1]$$

とする。これらより、補完多項式 $Q(X, Y)$ を求めて、以下の

割り算を実行する。

$$-Q_0(X)/Q_1(X) = \text{商}\ ([5] + [6]X + [9]X^2 + [6]X^3) \quad \text{剰余}\ 0$$

こうして、推定情報ベクトル

$$\hat{f} = [5][6][9][6]$$

を得る。 □

例 29.10 (RS 符号)**.** 既約多項式 $p(X) = 1 + X^2 + X^3 \in \mathbb{F}_2[X]$ によって定義される

$$\mathbb{F}_8 := \mathbb{F}_2[X]/\langle p(X)\rangle = \{[000], [100], \ldots, [111]\}$$

上の $[n = 8, k = 4]$ RS 符号の生成行列 G は以下で与えられる。ただし、

$$\alpha_1 = [000], \alpha_2 = [100], \ldots, \alpha_8 = [111]$$

と選んだ。

$$G = \begin{pmatrix} [100][100][100][100][100][100][100][100] \\ [000][100][010][110][001][101][011][111] \\ [000][100][001][101][111][011][110][010] \\ [000][100][101][010][011][001][111][110] \end{pmatrix}$$

$$
\begin{aligned}
f &= [111][101][000][110] \\
c &= [111][100][010][110][110][000][111][110] \\
e &= [000][000][000][000][000][000][101][110] \\
r &= [111][100][010][110][110][000][010][000]
\end{aligned}
$$

$$
A = \begin{pmatrix}
[100]\ [000]\ [000]\ [000]\ [000]\ [000]\ [111]\ [000]\ [000] \\
[100]\ [100]\ [100]\ [100]\ [100]\ [100]\ [100]\ [100]\ [100] \\
[100]\ [010]\ [001]\ [101]\ [111]\ [110]\ [010]\ [001]\ [101] \\
[100]\ [110]\ [101]\ [010]\ [011]\ [111]\ [110]\ [101]\ [010] \\
[100]\ [001]\ [111]\ [011]\ [010]\ [101]\ [110]\ [100]\ [001] \\
[100]\ [101]\ [011]\ [001]\ [110]\ [010]\ [000]\ [000]\ [000] \\
[100]\ [011]\ [110]\ [111]\ [101]\ [001]\ [010]\ [100]\ [011] \\
[100]\ [111]\ [010]\ [110]\ [001]\ [011]\ [000]\ [000]\ [000]
\end{pmatrix}
$$

$$
\overset{\text{行基本変形}}{\Longrightarrow}
\begin{pmatrix}
[100]\ [000]\ [000]\ [000]\ [000]\ [000]\ [111]\ [000]\ [000] \\
[000]\ [100]\ [100]\ [100]\ [100]\ [100]\ [011]\ [100]\ [100] \\
[000]\ [000]\ [100]\ [110]\ [111]\ [010]\ [101]\ [100]\ [110] \\
[000]\ [000]\ [000]\ [100]\ [000]\ [111]\ [110]\ [000]\ [100] \\
[000]\ [000]\ [000]\ [000]\ [100]\ [001]\ [000]\ [110]\ [100] \\
[000]\ [000]\ [000]\ [000]\ [000]\ [100]\ [000]\ [000]\ [110] \\
[000]\ [000]\ [000]\ [000]\ [000]\ [000]\ [100]\ [011]\ [110] \\
[000]\ [000]\ [000]\ [000]\ [000]\ [000]\ [000]\ [100]\ [100]
\end{pmatrix}
$$

$$\overset{\text{行基本変形}}{\Longrightarrow}\begin{pmatrix}
[100] & [000] & [000] & [000] & [000] & [000] & [000] & [000] & [100] \\
[000] & [100] & [000] & [000] & [000] & [000] & [000] & [000] & [100] \\
[000] & [000] & [100] & [000] & [000] & [000] & [000] & [000] & [010] \\
[000] & [000] & [000] & [100] & [000] & [000] & [000] & [000] & [111] \\
[000] & [000] & [000] & [000] & [100] & [000] & [000] & [000] & [110] \\
[000] & [000] & [000] & [000] & [000] & [100] & [000] & [000] & [110] \\
[000] & [000] & [000] & [000] & [000] & [000] & [100] & [000] & [101] \\
[000] & [000] & [000] & [000] & [000] & [000] & [000] & [100] & [100]
\end{pmatrix}$$

$$\vec{q_0} = [100][100][010][111][110][110]$$
$$\vec{q_1} = [101][100][100]$$

$-\ Q_0(X)/Q_1(X)$
$= \text{商}\ [111] + [101]X + [000]X^2 + [110]X^3 \quad \text{剰余}\ 0$

$$\hat{f} = [111][101][000][110]$$

□

30 巡回符号 @09

定義 30.1 (巡回シフト)**.** 長さ n のベクトル $c = (c_0, \ldots, c_{n-1}) \in \mathbb{F}^n$ に対して、

$$(c_{n-1}, c_0, \ldots, c_{n-2}) =: Sc$$

を c の右巡回シフトといい、Sc と書く。

$$(c_{n-i}, \ldots, c_{n-1}, c_0, \ldots, c_{n-i-1})$$

を c の i 回右巡回シフトといい、$S^i c$ と書く。
例：$S(010) = (001)$
例：$S(1010) =$ $\boxed{(0101)}$
例：$S^2(10101) =$ $\boxed{(01101)}$
同様にして、左巡回シフトを定義できるが、$n-1$ 回右巡回シフト S^{n-1} で表すことができるので、あえて定義しない。右巡回シフトを単に巡回シフトという。 □

命題 30.2 (巡回シフトは線形写像である)**.** $S^i : \mathbb{F}^n \to \mathbb{F}^n$ は線形全単射写像である。$c \mapsto S^i c$ ベクトル行列表現は、例えば $n = 4, i = 1$ では、

$$Sc = \begin{pmatrix} 0001 \\ 1000 \\ 0100 \\ 0010 \end{pmatrix} \vec{c}^{\mathsf{T}}$$

によって与えられる。 □

証明.

$$\begin{aligned}
&S^i(\vec{c}+\vec{d})\\
&= S^i(c_0+d_0,\ldots,c_{n-1}+d_{n-1})\\
&= (c_{n-i}+d_{n-i},\ldots,c_{n-1}+d_{n-1},\\
&\qquad c_0+d_0,\ldots,c_{n-i-1}+d_{n-i-1})\\
&= S^i\vec{c}+S^i\vec{d}
\end{aligned}$$

$S^i(a\vec{c}) = aS^i(\vec{c})$ も同様にして示せる。全単射であることは以下より分かる。

$$S^i\vec{c} = S^i\vec{d} \Rightarrow S^i(\vec{c}-\vec{d}) = \vec{0} \Rightarrow \vec{c}-\vec{d} = \vec{0} \Rightarrow \vec{c} = \vec{d}$$

ここで零ベクトルに巡回シフトされるのは零ベクトルに限ることを用いた。 □

定義 30.3 (巡回符号)**.** 巡回シフトに関して閉じている、正確に書くと

$$\forall c \in C, Sc \in C$$

を満たす、$\mathbb{F}_q$ 上の線形符号 C を $\mathbb{F}_q$ 上の線形巡回符号または単に巡回符号という．線形でない巡回符号は非線形巡回符号と呼ばれる。
例：単一パリティ検査符号 6.5 は巡回符号である。例えば符号

長 $n=4$ の単一パリティ検査符号

$$\begin{aligned} C = \{&(0000),\\ &(1001),(0011),(0110),(1100),\\ &(1010),(0101),\\ &(1111)\} \end{aligned}$$

は巡回符号で ある 。

$$\begin{aligned} C = \{&(0000),\\ &(1000),(0100),(0010),(0001)\} \end{aligned}$$

は 非線形巡回 符号である。なぜなら、巡回性は満たされるが、

$$(1000)+(0100)=(1100)\notin C$$

であるからである。 □

定義 30.4 (符号語多項式)**.** ベクトル $\vec{c}=(c_0,\ldots,c_{n-1})\in\mathbb{F}^n$ に対して多項式

$$c(X)=c_0+c_1X+\cdots+c_{n-1}X^{n-1}\in\mathbb{F}[X;n]$$

を $\vec{c}$ の符号語多項式という。符号語多項式と符号語を同一視する。
例：$(101)=1+X^2$,
例：$(110)=S(101)=S(1+X^2)=1+X$ □

31　巡回 RS 符号

例 31.1 (巡回 RS 符号). $\mathbb{F}_q$ の非ゼロ要素 β が $n>0$ 乗して始めて 1 に等しくなるとする。ただし、$\beta=1$ のときは $n=1$ と定義する。n は $q-1$ を割り切る。評価点 $\beta^0,\dots,\beta^{n-1}$ によって定義された $\mathbb{F}_q$ 上の $[n,k]$RS 符号

$$C=\left\{\vec{c}(f)\mid f(X)\in\mathbb{F}_q[X;k]\right\}$$
$$\vec{c}(f):=\left(f(\beta^0),f(\beta^1),\dots,f(\beta^{n-1})\right)$$

は巡回符号となる。　□

証明. 【$n\mid q-1$ であること】後に 37.10 で示すが、任意の非零元 $\alpha\in\mathbb{F}_q$ に対して、$\alpha^{q-1}=1$ が成り立つ[23]。$q-1$ を n で割った商と余りをそれぞれ a,b と書く。$q-1=an+b, 0\le b<n$ である。これに対して、$1=\beta^{q-1}=\beta^{an+b}=\beta^{an}\beta^b=\beta^b$ となる。n は β^n となる最小の自然数であったのと、$0\le b<n$ であったので、$b=0$ でなければならない．つまり，$q-1=an$ となり，n は $q-1$ を割り切ることがわかる．

【巡回符号であること】C は RS 符号であることと 28.4 より線形符号である．C の巡回性を示せば十分である。情報多項式 $f(X)\in\mathbb{F}_q[X;k]$ に対して、$S\vec{c}(f)=\vec{c}(g)$ となる情報多項式 $g(X)\in\mathbb{F}_q[X;k]$ の存在を示せば十分である。情報多項式

[23] q が素数 p の場合にはフェルマーの小定理 $a^{p-1}\equiv 1 \pmod{p}$ http://bit.ly/2Rm56Ww として知られている。

$g(X)$ を以下のように選ぶ。

$$g(X) \stackrel{\text{def}}{=} f(\beta^{-1}X) = f(\beta^{n-1}X) \in \mathbb{F}_q[X;k]$$

すると、

$$\begin{aligned}
&S\vec{c}(f)\\
&= S\big(f(\beta^0), f(\beta^1), \ldots, f(\beta^{n-1})\big)\\
&= \big(f(\beta^{n-1}), f(\beta^0)\ldots, f(\beta^{n-3}), f(\beta^{n-2})\big)\\
&\stackrel{\text{(a)}}{=} \big(g(\beta^0), g(\beta^1), \ldots, g(\beta^{n-1})\big)\\
&= \vec{c}(g)
\end{aligned}$$

となる。(a) では、$g(X) = f(\beta^{n-1}X)$ を使った。C は右巡回シフトに関して閉じていることがわかった。 □

例 31.2 (巡回 RS 符号の計算例)**.** $\mathbb{F}_4 := \mathbb{F}_2[X]/\langle 1 + X + X^2\rangle$ に対して、$\beta := [01] \in \mathbb{F}_4$ は 3 乗するとはじめて $[10]$ になる。β によって定義される $\mathbb{F}_4$ 上の $[3,2,2]$RS 符号を考える。

$$\begin{aligned}
C &:= \{(f(\beta^0), f(\beta^1), f(\beta^2) \mid f(X) \in \mathbb{F}_4[X;2]\}\\
&= \{(f([10]), f([01]), f([11])) \mid f(X) \in \mathbb{F}_4[X;2]\}
\end{aligned}$$

16 通りの情報多項式 $f(X) \in \mathbb{F}_4[X;2]$ に対して、符号多項式 $c(X)$ は以下の通り与えられる。

```
f=([00][00]),c=([00][00][00])
f=([10][00]),c=([10][10][10])
f=([01][00]),c=([01][01][01])
```

```
f=([11][00]),c=([11][11][11])
f=([00][10]),c=([10][01][11])
f=([10][10]),c=([00][11][01])
f=([01][10]),c=([11][00][10])
f=([11][10]),c=([01][10][00])
f=([00][01]),c=([01][11][10])
f=([10][01]),c=([11][01][00])
f=([01][01]),c=([00][10][11])
f=([11][01]),c=([10][00][01])
f=([00][11]),c=([11][10][01])
f=([10][11]),c=([01][00][11])
f=([01][11]),c=([10][11][00])
f=([11][11]),c=([00][01][10])
```

巡回性を有する符号多項式毎に分類されるように並び替えると以下のようになる。確かに巡回性が満たされている。

```
f=([00][00]),c=([00][00][00])

f=([10][00]),c=([10][10][10])

f=([01][00]),c=([01][01][01])

f=([11][00]),c=([11][11][11])

f=([11][10]),c=([01][10][00])
f=([11][01]),c=([10][00][01])
f=([11][11]),c=([00][01][10])

f=([00][10]),c=([10][01][11])
f=([00][01]),c=([01][11][10])
f=([00][11]),c=([11][10][01])

f=([10][11]),c=([01][00][11])
f=([10][10]),c=([00][11][01])
f=([10][01]),c=([11][01][00])

f=([01][01]),c=([00][10][11])
f=([01][11]),c=([10][11][00])
f=([01][10]),c=([11][00][10])
```

$\beta = [01]$ を n =3 乗するとはじめて $[10]$ になる。情報多項式 $f(X) = X$ に対応する符号語は

$$([10], [01], [11]) \tag{31.3}$$

であるが、これの右巡回シフトは

$$([11], [10], [01]) \tag{31.4}$$

である。

ここで $g(X) = [01]^{-1}X = [11]X$ を考え、この多項式に対応する符号語を考えると、

$$\begin{aligned}
&(g([01]^0), g([01]^1), g([01]^2)) \\
&= (g([10]), g([01]), g([11])) \\
&= ([11][10], [11][01], [11][11]) \\
&= ([11], [10], [01])
\end{aligned}$$

となり $f(X)$ に対応する符号語 (31.3) を右巡回シフトしたベクトル (31.4) に等しくなっている。 □

32 巡回符号は剰余類環 $\mathbb{F}[X]/\langle X^n - 1\rangle$ のイデアルである

$\mathbb{F}$ をスカラーとする符号長 n の線形符号は，$\mathbb{F}^n$ の部分線形空間として代数的な特徴付けをすることができる．この節で

は，$\mathbb{F}$ をスカラーとする長さ n の巡回符号が，多項式剰余類環 $\mathbb{F}[X]/\langle X^n-1\rangle$ のイデアルとして特徴付けられること 32.5 を導くことにより，巡回符号の代数的な構造を明らかにする．

定義 32.1 (剰余類環 $\mathbb{F}[X]/\langle X^n-1\rangle$ と多項式空間 $\mathbb{F}[X;n]$ は同型な線形空間である)**.** n 次未満の多項式環 $\mathbb{F}[X;n]$ と多項式剰余類環 $\mathbb{F}[X]/\langle X^n-1\rangle$ は，23.5 より n 次未満の多項式からなるので，ともに要素数は同じ $|\mathbb{F}|^n$ 個である．また，$\mathbb{F}[X;n]$ と $\mathbb{F}[X]/\langle X^n-1\rangle$ にそれぞれ自然に定義された和とスカラー倍によって，$\mathbb{F}$ 上の線形空間となる。さらに，全単射である線形写像

$$f(X)\in\mathbb{F}[X;n]\mapsto[f(X)]\in\mathbb{F}[X]/\langle X^n-1\rangle$$

により、$\mathbb{F}$ 上の線形空間として、$\mathbb{F}[X;n]$ と $\mathbb{F}[X]/\langle X^n-1\rangle$ は同型になる。この対応を用いて、 $f(X)\in\mathbb{F}[X;n]$ と $[f(X)]\in\mathbb{F}[X]/\langle X^n-1\rangle$ を同一視して、文脈に応じて解釈することとする。 □

証明. $\mathbb{F}[X;n]$ は，$\mathbb{F}[X;n]$ 上の和と定数多項式倍をスカラー倍として定義すれば，$\mathbb{F}$ 上の線形空間になる．$\mathbb{F}[X]/\langle X^n-1\rangle$ が $\mathbb{F}$ 上の線形空間になるのは，和はすでに定義されているので，$a\in\mathbb{F},[f(X)]\in\mathbb{F}[X]/\langle X^n-1\rangle$ に対してスカラー倍を

$$a[f(X)]\stackrel{\text{def}}{=}[af(X)]\in\mathbb{F}[X]/\langle X^n-1\rangle \qquad (32.2)$$

と定義すればよい． □

命題　32.3. 多項式 $c(X) \in \mathbb{F}[X;n]$ と多項式剰余類環 $\mathbb{F}[X]/\langle X^n-1\rangle$ の剰余類 $[\cdot]$ に対して次が成り立つ.

$$S^i c(X) = [X^i c(X)]$$

この等式は 32.1 の対応により $S^i c(X) \in \mathbb{F}[X;n]$ と $[X^i c(X)] \in \mathbb{F}[X]/\langle X^n-1\rangle$ が一致することを表している. 言い換えると, $c(X)$ を i 回右巡回シフトした多項式は $X^i c(X)$ を X^n-1 で割った剰余多項式と一致する

$$S^i c(X) = X^i c(X) \bmod X^n - 1$$

ことを表している. □

証明. （ $i=1$ の場合）$c(X) = \sum_{j=0}^{n-1} c_j X^j$ とおく剰余環では $[X^n] = [1]$ だから

$$\begin{aligned} Xc(X) &= \sum_{j=0}^{n-1} c_j X^{j+1} = c_{n-1}X^n + \sum_{j=0}^{n-2} c_j X^{j+1} \\ &\equiv c_{n-1} + \sum_{j=0}^{n-2} c_j X^{j+1} \end{aligned}$$

右辺の X^j の係数はちょうど c_{j-1}（添字は $\bmod n$ ）なので

$$[Xc(X)] = \sum_{j=0}^{n-1} c_{j-1} X^j = Sc(X)$$

よって $Sc(X) = [Xc(X)]$ が示された．一般の i について上で示した $Sc = [Xc]$ と，$[\cdot]$ が環準同型であることから

$$S^i c = S\left(S^{i-1}c\right) = S\left(\left[X^{i-1}c\right]\right) = [X]\left[X^{i-1}c\right] = \left[X^i c\right]$$

が帰納法で従う．以上より命題が成立する。 □

例 **32.4.** $(1101) = 1 + X + X^3 \in \mathbb{F}_2[X;4]$ を 1 回右巡回シフトすると $(1110) = 1 + X + X^2$ になる。

$$\begin{aligned} X(1 + X + X^3) &= X + X^2 + X^4 \\ &\equiv 1 + X + X^2 (\mathrm{mod} X^4 - 1) \\ &= (1110) \end{aligned}$$

$(1234) = 1 + 2X + 3X^2 + 4X^3 \in \mathbb{F}_5[X;4]$ を 1 回右巡回シフトすると $(4123) = 4 + X + 2X^2 + 3X^3$ になる。

$$\begin{aligned} &X(1 + 2X + 3X^2 + 4X^3) \\ &= X + 2X^2 + 3X^3 + 4X^4 \\ &= 4(X^4 - 1) + 4 + X + 2X^2 + 3X^3 \\ &\equiv 4 + X + 2X^2 + 3X^3 (\mathrm{mod} X^4 - 1) \\ &= (4123) \end{aligned}$$

□

次の定理により巡回符号 $C \subset \mathbb{F}[X;n]$ は $C \subset \mathbb{F}[X]/\langle X^n - 1\rangle$ のイデアルとみなせることが分かる．

定理 32.5. 以下は同値である。

1. $C \subset \mathbb{F}[X;n]$ は符号長 n の $\mathbb{F}$ 上の巡回符号である
2. $C \subset \mathbb{F}[X]/\langle X^n-1\rangle$ は剰余類環 $\mathbb{F}[X]/\langle X^n-1\rangle$ のイデアルである

□

証明. 【$2 \Rightarrow 1$】イデアルの元 $[c(X)] \in C$ に対して、C のイデアル性により任意の整数 i に対して、C の巡回性:

$$S^i c(X) \overset{32.1}{=} [S^i c(X)] \overset{32.3}{=} [X^i c(X)] \overset{(a)}{=} [X^i][c(X)] \overset{(b)}{\in} C$$

が成り立つ。(a) では剰余類環演算の定義 23.1、(b) ではイデアルの性質 (21.2) を使った。同じ理由から、任意のスカラー $a \in \mathbb{F}$ と符号語 $c(X), c'(X) \in C$ に対して、

$$ac(X) \overset{32.1}{=} [ac(X)] \overset{(a)}{=} [a][c(X)] \overset{(b)}{\in} C$$

$$c(X)+c'(X) \overset{32.1}{=} [c(X)+c'(X)] \overset{(a)}{=} [c(X)]+[c'(X)] \overset{(b)}{\in} C$$

である。C の線形性が示せた。これより、C が巡回符号であることが分かる。

【$1 \Rightarrow 2$】$[c(x)] \in C$ と $[u(X) := \sum_{i\geq 0}^{n-1} u_i X^i] \in \mathbb{F}[X]/\langle X^n-$

$1\rangle$ に対して

$$\begin{aligned}
[u(X)][c(X)] &= \left[\textstyle\sum_{i\geq 0}^{n-1} u_i X^i\right][c(X)] \\
&\overset{\text{(a)}}{=} \textstyle\sum_{i=0}^{n-1}[u_i X^i][c(X)] \\
&\overset{(32.2)}{=} \textstyle\sum_{i=0}^{n-1} u_i[X^i][c(X)] \\
&\overset{\text{(a)}}{=} \textstyle\sum_{i=0}^{n-1} u_i[X^i c(X)] \\
&\overset{32.3}{=} \textstyle\sum_{i=0}^{n-1} u_i \underbrace{S^i c(X)}_{\in C} \overset{\text{(c)}}{\in} C
\end{aligned}$$

となりイデアルの積に関する閉性 (21.2) が満たされる。(c) では、符号 C の線形性を用いた。さらに、$[c(X)], [c'(X)] \in C$ に対して、

$$\begin{aligned}
[c(X)] + [c'(X)] &\overset{\text{(a)}}{=} [c(X) + c'(X)] \\
&\overset{32.1}{=} c(X) + c'(X) \overset{\text{(c)}}{\in} C
\end{aligned}$$

となるので，C は加群である。したがって、C が剰余類環 $\mathbb{F}[X]/\langle X^n - 1\rangle$ のイデアル 21.3 であることが分かる。 □

33 巡回符号の生成多項式

この節では，巡回符号のいくつかの性質を導き，符号化に有用な生成多項式を学ぶ.

定理 33.1. 多項式剰余類環 $\mathbb{F}_q[X]/\langle X^n-1\rangle$ のイデアル I(巡回符号である) に対して、I に属する非ゼロ多項式で最小の次数を持つものを $[g(X)]$ とする。以下が成り立つ。

1. I の生成元 $[g(X)]$ の $g(X) \in \mathbb{F}[X;n]$ は X^n-1 を割り切る。
2. I は一つの生成元 $[g(X)] \in I$ で生成される。$I = \langle [g(X)] \rangle$

□

証明. 1. イデアル I の生成元 $g(X)$ は X^n-1 を割り切ることを主張する。割り切れないと仮定すると

$$(X^n-1) \div g(X) = \text{商 } q(X) \text{ あまり } r(X) \neq 0$$

言い換えると、

$$\begin{aligned}(X^n-1) &= g(X) \times q(X) + r(X)\\ \deg r(X) &< \deg g(X)\end{aligned}$$

となる。これより

$$\begin{aligned}r(X) &= -g(X) \times q(X) \bmod X^n-1\\ &= g(X) \times (-q(X)) \bmod X^n-1\end{aligned}$$

対応する剰余類で表すと、

$$[r(X)] = [g(X)] \times [-q(X)] \in I$$

となる。$[r(X)]$ はイデアル I の要素であり、$r(X)$ は非ゼロで $g(X)$ より小さい次数を持ち $g(X)$ の選び方に矛盾する。従って X^n-1 は $g(X)$ の多項式倍である。

2. 剰余類環 $\mathbb{F}_q[X]/\langle X^n-1\rangle$ のイデアル I が与えられたとする。自明な I、言い換えると $I=\{[0]\}$ の場合と $I=\mathbb{F}_q[X]/\langle X^n-1\rangle$ の場合を考えよう。このとき、I が一つの要素、それぞれ $[0]$ と $[1]$ で生成されることは明らかである。

$$\{[0]\}=\langle[0]\rangle, \mathbb{F}_q[X]/\langle X^n-1\rangle=\langle[1]\rangle$$

非自明なイデアル I に対して証明を与える[24]。任意の $[f(X)]\in I$ に対して $[f(X)]=[a(X)][g(X)]$ となる $[a(X)]\in\mathbb{F}[X]/\langle X^n-1\rangle$ が存在することを示せば良い．$[f(X)]\in I$ となる $f(X)\in\mathbb{F}[X;n]$ は $g(X)$ によって割り切れることを主張する．割り切れないと仮定して矛盾を導く．1 より $g(X)|X^n-1$ であるから，$\deg g(X)\leq n$ である．

$$f(X)\div g(X)=\text{商 } q(X) \text{ あまり } \underbrace{r(X)}_{\neq 0}$$

とする．言い換えると、

$$f(X)=q(X)\times g(X)+r(X)$$
$$\deg r(X)<\deg g(X)$$

[24]教員用メモ：非自明であることは使っていないのでは？

となる。これらを $\mathbb{F}[X]/\langle X^n-1\rangle$ の剰余類で表した

$$[r(X)] = \underbrace{[f(X)]}_{\in I} - \underbrace{[g(X)] \times [q(X)]}_{\in I}$$

はイデアルの加群性から I の要素であり、$r(X)$ は非ゼロで $g(X)$ より小さい次数を持ち $g(X)$ の選び方に矛盾するので、$r(X) = 0$ となる，つまり任意の $[f(X)] \in I$ に対して $[q(X)] \in \mathbb{F}[X]/\langle X^n-1\rangle$ が存在して $[f(X)] = [q(X)][g(X)]$ となることが示された．これより，$[g(X)]$ はイデアル I の生成元であることがわかる。

□

定義 33.2 (生成多項式)**.** 巡回符号 C に含まれる、次数最小のモニックな非零符号語 $g(X)$ を C の生成多項式という。ただし、C の次元が 0 である、すなわち $C = \{0\}$ である場合には、$g(X) = X^n - 1$ と定める。生成多項式の一意性は 33.4 で示す。□

例 33.3. 31.2 の例で扱った巡回 RS 符号 C の符号語をリストすると

```
([00][00][00]),([10][10][10]),([01][01][01]),([11][11][11]),
([10][01][11]),([00][11][01]),([11][00][10]),([01][10][00]),
([01][11][10]),([11][01][00]),([00][10][11]),([10][00][01]),
([11][10][01]),([01][00][11]),([10][11][00]),([00][01][10])
```

となる。これより、C の生成多項式は、

$$g(X) = \boxed{[01] + [10]X}$$

である。他の符号語で生成多項式となるものはないので、生成多項式は唯一である。 □

定理 33.4. $\mathbb{F}$ 上の $[n,k]$ 巡回符号 C と生成多項式 $g(X)$ に対して次が成り立つ。

1. $g(X)$ は $C(\mathbb{F}[X]/\langle X^n-1\rangle$ のイデアルとみなした) の生成元である.

   証明. 33.1 の $[g(X)]$ の定義より明らか. □

2. $g(X)$ は X^n-1 を割り切る。

   証明. 33.1 の 1 より明らか. □

3. $g(X)$ は C の非零符号語である。

   証明. 生成多項式の定義より明らか。 □

4. C に対して $g(X)$ は一意に決まる。

   証明. 生成多項式が一意でないと仮定する。すなわち $g(X)\neq g'(X)$ なる生成多項式 $g(X), g'(X)$ が存在する。C が線形符号であることから $g(X)-g'(X)\neq 0$ は符号語であり、生成多項式のモニック性から $g(X)-g'(X)$ の次数は $g(X), g'(X)$ より次数が少なくなる。さらに、$g(X)-g'(X)$ を適当に非零定数倍するとモニックになる。これは、生成多項式の次数の最小性に矛盾する。□

5. 任意の符号語 $c(X) \in C$ は $g(X)$ で割り切れる[25]。

証明. ある符号語 $c(X)$ が $g(X)$ で割り切れないと仮定する。すると、

$$\begin{aligned} c(X) &= q(X)g(X) + r(X), \\ \deg r(X) &< \deg g(X) \end{aligned} \tag{33.5}$$

となる、商と余り $q(X), r(X)(\neq 0) \in \mathbb{F}[X]$ が存在する。$\deg c(X) < n$ であるから、$\deg(q(X)g(X)) < n$ となる。したがって,

$$\begin{aligned} q(X)g(X) &= q(X)g(X) \bmod X^n - 1 \\ &\overset{23.5}{=} [q(X)g(X)] \overset{23.1}{=} [q(X)][g(X)] \in C \end{aligned}$$

となる。ここで，$[g(X)]$ が C の生成元であることを使った．したがって、

$$r(X) = c(X) - q(X)g(X) \in C$$

となり、$0 \neq r(X) \in C$ を得るが、(33.5) は $g(X)$ の次数の最小性に矛盾する。 □

6. C は以下のように表せる。

$$C = \{u(X)g(X) \mid u(X) \in \mathbb{F}[X; n - \deg g(X)]\}$$

[25] 教員用メモ：これも多項式剰余類環のイデアルの性質だけで示したい.

これにより、C の符号語多項式は $g(X)$ に $n - \deg g(X)$ 次未満の情報多項式を乗じることで生成されることがわかる。これが $g(X)$ が生成多項式と呼ばれる理由である。

証明. 5 より，符号語 $c(X) \in C$ に対して，$c(X) = u(X)g(X)$ となる $u(X) \in \mathbb{F}[X; n - \deg g(X)]$ が存在する。逆に、$u(X) \in \mathbb{F}[X; n - \deg g(X)]$ に対して、$u(X)g(X)$ の次数は n 次未満なので,

$$\begin{aligned} u(X)g(X) &= u(X)g(X) \bmod X^n - 1 \\ &= [u(X)g(X)] \\ &= [u(X)][g(X)] \overset{\text{(a)}}{\in} C \end{aligned}$$

となる。(a) では 1 の $[g(X)]$ がイデアル C の生成元であることを使った. □

7. $k = n - \deg g(X)$ である.

証明. 異なる $u(X), u'(X) \in \mathbb{F}[X; n - \deg g(X)]$ に対して，$c(X) = u(X)g(X)$, $c'(X) = u'(X)g(X)$ とすると，$c(X) \neq c'(X)$ となるはずである．なぜなら，$c(X) = c'(X)$ と仮定すると，$(u(X) - u'(X))g(X) = 0$ となり $g(X) \neq 0$ に矛盾する．したがって，このような $u(X)$ をすべて動かすことで，C の符号語をすべて生成することができる: $|C| = |\mathbb{F}|^{n - \deg g(X)}$ となる．一方，C は $\mathbb{F}$ を

スカラとする k 次元線形符号であるから，$|C| = |\mathbb{F}|^k$ となる．これらより，$k = n - \deg g(X)$ を得る． □

□

この定理 33.4 は，巡回符号の生成多項式が満たすべき性質を与えてくれた．次の 33.6 は逆にこの性質を備えた多項式から生成される多項式集合は巡回符号になることを主張している．

命題 33.6. $g(X) \mid X^n - 1, \deg g(X) = n - k$ を満たすモニックな非零多項式 $g(X) \in \mathbb{F}[X]$ を用いて定義される

$$C = \{u(X)g(X) \mid u(X) \in \mathbb{F}[X; k]\} \subset \mathbb{F}[X; n]$$

は、$\mathbb{F}$ 上の $[n, k]$ 巡回符号となる。 □

証明. 演習問題で証明する。 □

命題 33.7 (巡回符号は割り算を用いて簡単に組織的に符号化できる)**.** C を $\mathbb{F}$ 上の $[n, k]$ 巡回符号とする。C の生成多項式を $g(X) \in \mathbb{F}[X, n - k]$ とする。下記のアルゴリズムは、情報多項式 $u(X) \in \mathbb{F}[X; k]$ を入力とし、1 対 1 に対応する符号語 $c(X)$ を出力する線形な符号化アルゴリズムであり、組織的な符号化になっている。ここで言う組織的符号化とは、対応する符号語ベクトル $\vec{c}$ に、情報ベクトル $\vec{u}$ が部分ベクトルとして現れることを意味している。

1. $u(X)X^{n-k}$ を $g(X)$ で割った商と剰余をそれぞれ $q(X), r(X)$ と書く。

$$u(X)X^{n-k} = q(X)g(X) + r(X),$$
$$\deg r(X) < \deg g(X) = n-k \tag{33.8}$$

が成り立つ。

2. これを移項して、

$$u(X)X^{n-k} - r(X) = q(X)g(X) =: c(X) \tag{33.9}$$

を符号語として出力する。

□

証明. (33.9) の右辺は $g(X)$ の倍多項式になっているので、左辺は C の符号語となっていることが分かる。

$$u(X)X^{n-k} - r(X) \in C \text{ with } r(X) \in \mathbb{F}[X; n-k]$$

$u(X) \mapsto u(X)X^{n-k}$ は、右に $n-k$ 回シフトする操作なので、30.2 より線形写像である。後で示す 33.10 から $u(X) \mapsto r(X)$ も線形写像であることがわかる。さらに、(33.8) より、$r(X)$ と $u(X)X^{n-k}$ の共通する次数に非ゼロ係数を持たないので、対応する符号語ベクトルは $\vec{c} = (-\vec{r}|\vec{u})$ となる。これより、$\vec{c}$ は $\vec{u}$ を一部に含んでおり組織的であることと、$u(X) \mapsto c(X)$ は一対一であることが分かる。 □

補題 33.10 (剰余の線形性)**.** $n \geq m$ とする．$m = \deg g(X)$ なる非零多項式 $d(X) \in \mathbb{F}[X;n]$ に対して、以下で定義される写像 $\phi : \mathbb{F}[X;n] \ni f(X) \mapsto \phi(f) \in \mathbb{F}[X;m]$ は線形写像である。

$$\phi(f) := f(X) \bmod d(X)$$

ただし、$f(X) \bmod d(X)$ は $f(X)$ を $d(X)$ で割った剰余多項式である。

証明. 表記を簡単にするために、多項式 $f(X)$ を f と書く。

$$\begin{aligned}\phi(f+g) &= \phi(f) + \phi(g),\\ \phi(cf) &= c\phi(f)\end{aligned}$$

を示せばよい。多項式 f, g に対して、$f/d, g/d$ の商と剰余が剰余定理 24.1 よりそれぞれ以下の通り与えられるとする。

$$\begin{aligned}f &= q_f d + r_f,\ \deg r_f < \deg d\\ g &= q_g d + r_g,\ \deg r_g < \deg d\end{aligned}$$

このとき、

$$\begin{aligned}f + g &= (q_f + q_g)d + (r_f + r_g),\\ \deg(r_f + r_g) &< \deg d\end{aligned}$$

[26]教員用メモ: ここに符号化の例を与えたい.

となる。したがって、

$$\phi(f+g) = r_f + r_g = \phi(f) + \phi(g)$$

となる。スカラー $c \in \mathbb{F}$ に対して、

$$cf = cq_f d + cr_f,\ \deg cr_f < \deg d$$

となるので、剰余定理 24.1 より $\phi(cf) = c\phi(f)$ も言えて、主張が導けた。 □

34 @10 巡回符号の生成行列とパリティ検査行列

この節では，巡回符号の生成行列，パリティ検査行列を与える．また，符号語多項式とかけると零多項式になるパリティ検査多項式を与える．

命題 34.1 (巡回符号の生成行列). $\mathbb{F}_q$ 上の $[n,k]$ 巡回符号 C の生成多項式が $g(X)$ で与えられるとする。33.4 の 7 より，$\deg g(X) = n-k$ である。つまり、

$$g(X) = g_0 + g_1 X + \cdots + g_{n-k-1}X^{n-k-1} + \underbrace{g_{n-k}}_{=1} X^{n-k}$$

と書ける．ここで $g(X)$ を，それぞれ $0, 1, \ldots, k-1$ 回，右シフトした $g(X)$, $Xg(X)$, $\ldots$, $X^{k-1}g(X)$ に対応する k 個の符号語は

$$\begin{aligned}
g(X) &\leftrightarrow (g_0, g_1, \ldots, g_{n-k-1}, g_{n-k}, 0, \cdots, 0) \\
Xg(X) &\leftrightarrow (0, g_0, g_1, \ldots, g_{n-k-1}, g_{n-k}, 0, \cdots, 0) \\
&\vdots \\
X^{k-2}g(X) &\leftrightarrow (0, \ldots, 0, g_0, g_1, \ldots, g_{n-k-1}, g_{n-k}, 0) \\
X^{k-1}g(X) &\leftrightarrow (0, \ldots, \ldots, 0, g_0, g_1, \ldots, g_{n-k-1}, g_{n-k})
\end{aligned}$$

となる．これらは一番右にある非ゼロ成分 $g_{n-k} = 1$ の位置がすべて異なるから線形独立である。または、$g_0 \neq 0$ であるこ

と（証明は演習で行う）からも分かる。またベクトルの数 k は C の次元 k に等しいからこれらのベクトルは基底を構成している。従ってこれらのベクトルを縦に並べた $\mathbb{F}_q$ 値 $k \times n$ 行列

$$G = \begin{pmatrix} g_0 & g_1 & \cdots & g_{n-k-1} & g_{n-k} & 0 & \cdots & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & g_{n-k-1} & g_{n-k} & 0 & \cdots & 0 \\ & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \\ 0 & \cdots & 0 & g_0 & g_1 & \cdots & g_{n-k-1} & g_{n-k} & 0 \\ 0 & \cdots & \cdots & 0 & g_0 & g_1 & \cdots & g_{n-k-1} & g_{n-k} \end{pmatrix}$$

が C の生成行列になる。 □

定義 34.2 (パリティ検査多項式)**.** 符号長 n の巡回符号 C の生成多項式 $g(X)$ に対して、

$$h(X) := (X^n - 1)/g(X) \tag{34.3}$$

を C のパリティ検査多項式という。(34.3) の割り算が割り切れることは、33.4 の 2 で示した。 □

7.7 を思い出そう．パリティ検査行列は符号語と掛けるとゼロベクトルとなる行列であった．パリティ検査多項式は，符号語多項式に掛けて $X^n - 1$ で割ったあまりが零多項式になる多項式である．

命題 34.4 (巡回符号のパリティ検査行列)**.** 符号長 n の $\mathbb{F}$ 上の巡回符号 C のパリティ検査多項式を $h(X) = \sum_{i=0}^{k} h_i X^i$ とする。以下が成り立つ。

1. $\deg h(X) = k, h_k = 1$ である。

2. $c(X) \in \mathbb{F}[X;n]$ に対して、$c(X) \in C$ であることと、$c(X)h(X) \equiv 0 (\mathrm{mod} X^n - 1)$ であることは同値である。

3. 以下の H は C のパリティ検査行列である。

$$H = \begin{pmatrix} h_k & h_{k-1} & \dots & h_1 & h_0 & 0 & \cdots\cdots & 0 \\ 0 & h_k & h_{k-1} & \dots & h_1 & h_0 & 0 \cdots & 0 \\ & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots \\ 0 & \dots & 0 & h_k & h_{k-1} & \dots & h_1 & h_0 & 0 \\ 0 & \dots & \dots & 0 & h_k & h_{k-1} & \dots & h_1 & h_0 \end{pmatrix}$$

□

証明. 1. $\deg g(X) = n-k, g_{n-k} = 1$ であったから、(34.3) より明らか。

2. $c(X)$ が C の符号語であるとすると、33.4 の 6 より生成多項式 $g(X)$ と情報多項式 $u(X) \in \mathbb{F}[X;k]$ を用いて、$c(X) = u(X)g(X)$ と書ける。これより，次が成り立つ.

$$\begin{aligned} c(X)h(X) &= u(X)g(X)h(X) \\ &\overset{(34.3)}{=} u(X)(X^n - 1) \\ &\equiv 0 (\mathrm{mod}\ X^n - 1) \end{aligned} \tag{34.5}$$

逆に $c(X) \in \mathbb{F}[X;n]$ に対して $c(X)h(X) \equiv 0$ とすると、

$$c(X)h(X) = u(X)(X^n - 1) = u(X)g(X)h(X)$$

なる多項式 $u(X) \in \mathbb{F}[X;k]$ が存在する。これより

$$\big(c(X) - g(X)u(X)\big)h(X) = 0$$

となるが、非ゼロ多項式どうしの積はゼロにはならないのと第 2 因子 $h(X)$ は非ゼロなので、第一因子がゼロ、すなわち $c(X) = u(X)g(X)$ となるはずである。これより、$c(X)$ が C の符号語であることがわかる。

3. まず、$H\vec{c} = \vec{0}$ であることを示す。(34.5) の右辺 $u(X)X^n - u(X)$ の第 1 項は j 次 $(n \le j < n+k)$ 以外の係数はゼロであり第 2 項は j 次 $(0 \le j < k)$ 以外の係数はゼロである。よって、$u(X)X^n - u(X)$ の j $(k \le j \le n-1)$ 次の係数は 0 である。したがって、(34.5) の左辺を展開した多項式

$$c(X)h(X) = \sum_{j \ge 0} (\sum_{i=0}^{j} c_i h_{j-i}) X^j$$

の j $(k \le j \le n-1)$ 次の係数も 0 となる。

$$\sum_{i=0}^{j} c_i h_{j-i} = 0 \text{ for } j = k, k+1, \ldots, n-1$$

これを行列で表すと $H\vec{c} = \vec{0}$ である。これは、$GH^T = 0$ を意味する。つぎに、対角成分に $h_k = 1$ が並んでいることからフルランクである $\mathrm{rank}(H) = n - k$ となる。したがって、7.13 より、H は C のパリティ検査行列となる。

□

例 34.6. 31.2 の例で扱った $[n=3,k=2]$ 巡回 RS 符号 C の符号語を列挙すると

```
([00][00][00]),([10][10][10]),([01][01][01]),([11][11][11]),
([10][01][11]),([00][11][01]),([11][00][10]),([01][10][00]),
([01][11][10]),([11][01][00]),([00][10][11]),([10][00][01]),
([11][10][01]),([01][00][11]),([10][11][00]),([00][01][10])
```

となる。これより、C の生成多項式は、

$$g(X) = \boxed{[01] + [10]X}$$

であった。パリティ検査多項式は、

$$h(X) = (X^n - 1)/\boxed{([01] + [10]X)} = \boxed{[11] + [01]X + X^2}$$

となる。TODO:$h(X)c(X) \equiv 0$ となる例を与える。 □

35 巡回符号の双対符号

線形符号一般では，主符号のパリティ検査行列が双対符号の生成行列となり，主符号の生成行列が双対符号のパリティ検査行列となるという，いわゆる「双対性」が成立する．すなわち，C と $C^\perp$ の間には役割が反転する対称的な対応がある。

しかし，巡回符号の場合，生成多項式 $g(X)$ とパリティ検査多項式 $h(X)$ の間には，このような単純な「役割の反転」は生じない。実際，$g(X)$ をそのまま「反転」させて $C^\perp$ のパリ

ティ検査多項式や生成多項式を得ることはできず，一般の線形符号で見られるような形式的な双対性は，多項式表現のレベルでは成立しない。

したがって，巡回符号の双対符号がどのような生成多項式を持つのかは，一般の線形符号とは別に，巡回構造に基づいた特有の議論を必要とする。この節では，巡回符号の双対符号もまた巡回符号になること，およびその生成多項式を具体的に決定する方法を明らかにする。

定理 35.1 (巡回符号の双対符号は巡回符号)**.** 非自明な体 $\mathbb{F} \neq \{0\}$ 上の $[n,k]$ 巡回符号 C は，生成多項式 $g(X) = \sum_{i=0}^{n-k} g_i X^i$ とパリティ検査多項式 $h(X) = \sum_{i=0}^{k} h_i X^i$ を有しているとする．k 次の多項式 $g^{\perp}(X) \in \mathbb{F}[X;k]$ を定義する．

$$\begin{aligned} g^{\perp}(X) &\stackrel{\text{def}}{=} h_0^{-1} X^k h(1/X) \\ &= h_0^{-1}(h_k + h_{k-1}X + \cdots + h_1 X^{k-1} + h_0 X^k) \end{aligned}$$

$g^{\perp}(X)$ は，$h(X)$ の係数 $h_0, \ldots, h_k$ を逆順に並べた k 次多項式をモニック化したものである．このとき，以下が成り立つ。

1. $h_0 \neq 0$
2. $g^{\perp}(X) \mid X^n - 1$ である．これと 33.6 により，$g^{\perp}(X)$ はある巡回符号 C' の生成多項式となることが分かる．
3. $C' = C^{\perp}$ である．したがって，双対符号 $C^{\perp}$ は巡回符号である．$g^{\perp}(X)$ は双対符号 $C^{\perp}$ の生成多項式である．

C の双対符号 $C^\perp$ は巡回符号であり、$g^\perp(X)$ は $C^\perp$ の生成多項式である. □

証明. 1. まず、$h_0 \neq 0$ であることを示す。$h_0 = 0$ と仮定すると $h(0) = 0$ となる。一方、$X^n - 1 = g(X)h(X)$ である。これから、左辺 $|_{X=0} = -1$ で 右辺 $|_{X=0} = 0$ となることになるが、$-1 \neq 0$ なので[27]、矛盾する。

2. 次に，$g^\perp(X) \mid X^n - 1$ を示す. $h(X)$ はパリティ検査多項式であったから、$g(X)h(X) = X^n - 1$ が成り立つ。X を $1/X$ に置き換えることで、多項式でなくなるが形式的に

$$g(1/X)h(1/X) = (1/X)^n - 1$$

が成り立つ。$\deg g(X) = n - k, \deg h(X) = k$ であった。これらが多項式になるように、両辺に X^n を乗じて、多項式の等式

$$\underbrace{X^{n-k}g(1/X)}_{\in \mathbb{F}[X]} \underbrace{X^k h(1/X)}_{= h_0 g(X)^\perp \in \mathbb{F}[X]} = 1 - X^n$$

を得る。これは、$g^\perp(X) := h_0^{-1} X^k h(1/X)$ が $X^n - 1$ を割り切ることを意味している。

3. 34.1 と 34.4 から，C の生成行列 G とパリティ検査行列

[27] $0 = 1$ だと仮定すると $x = x \cdot 1 = x \cdot 0 = 0$ for $x \in \mathbb{F}$ となり自明な体 $\mathbb{F} = \{0\}$ となる。

H はそれぞれ $g(X), h(X)$ を用いて,

$$G = \begin{pmatrix} g_0 & g_1 & \cdots & g_{n-k-1} & g_{n-k} & 0 & \cdots & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & g_{n-k-1} & g_{n-k} & 0 & \cdots & 0 \\ & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \\ 0 & \dots & 0 & g_0 & g_1 & \cdots & g_{n-k-1} & g_{n-k} & 0 \\ 0 & \dots & \dots & 0 & g_0 & g_1 & \cdots & g_{n-k-1} & g_{n-k} \end{pmatrix}$$

$$H = \begin{pmatrix} h_k & h_{k-1} & \dots & h_1 & h_0 & 0 & \cdots & \cdots & 0 \\ 0 & h_k & h_{k-1} & \dots & h_1 & h_0 & 0 & \cdots & 0 \\ & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \\ 0 & \dots & 0 & h_k & h_{k-1} & \dots & h_1 & h_0 & 0 \\ 0 & \dots & \dots & 0 & h_k & h_{k-1} & \dots & h_1 & h_0 \end{pmatrix}$$

と構成できた。$g^{\perp}(X)$ を生成多項式とする巡回符号 C' の生成行列は $\frac{1}{h_0}H$ で与えられることが分かる．一方，7.7 から，C のパリティ検査行列 $\frac{1}{h_0}H$ は双対符号 $C^{\perp}$ の生成行列になる。したがって，$g^{\perp}(X)$ を生成多項式とする巡回符号 C' は $C^{\perp}$ であることがわかった. □

36 体の元の位数に関する性質

次の節で学習する有限体の便利な性質「原始元が存在する」ことの証明に使用するいくつかの補題を導く.[28]

定義 36.1 (位数). 体 $\mathbb{F}$ の非零元 $\alpha \in \mathbb{F}$ に対して、

$$\alpha^1, \alpha^2, \dots,$$

[28] 教員用メモ：証明は直感的に説明しにくいので、証明は概要を述べるだけにする。

と並べたときに初めて単位元 1 になる $\alpha^i = 1$ に対して、i を α の位数といい、$\mathrm{ord}(\alpha)$ と書く。$\mathrm{ord}(1) = 1$ である。 □

補題 36.2 (36.5, 36.6 で使用する)**.** 有限体の非零の元 α に対して、$i := \mathrm{ord}(\alpha)$ とする。このとき、以下が成り立つ。

$$\alpha^j = 1 \Leftrightarrow i \mid j$$

証明. ($\Leftarrow$ の証明)$i \mid j$ ならば $j = ih$ となる整数 h が存在する。$\alpha^j = \alpha^{ih} = (\alpha^i)^h = 1^h = 1$ となる。
($\Rightarrow$ の証明)

$$j/i = \text{商 } q \text{ 余り } r \tag{36.3}$$

とする。$0 \leq r < i$ である。$\alpha^j = 1$ ならば、

$$1 = \alpha^j = \alpha^{iq+r} = (\alpha^i)^q \alpha^r \overset{[i=\mathrm{ord}(\alpha)]}{=\!=} \alpha^r$$

となる。$r \neq 0$ つまり $r > 0$ を仮定すると、位数 $i := \mathrm{ord}(\alpha)$ の定義の最小性に矛盾する。したがって、$r = 0$ となる。これを (36.3) に代入して $i \mid j$ を得る。 □

定義 36.4. 自然数 n の素因数の重複を許した集合を (n) と書く。例えば、$(72) = \{2, 2, 2, 3, 3\}$ である。この表記を用いい

ると次が成り立つ。

$$
\begin{aligned}
&(1) = \text{空集合} \\
&n \mid m \Leftrightarrow (n) \subset (m) \\
&(\gcd(n,m)) = (n) \cap (m), \\
&\gcd(n,m) = 1 \Leftrightarrow (n) \text{ と } (m) \text{ に交わりはない} \\
&(nm) = (n) \cup (m), \\
&(n/m) = (n) \setminus (m) \text{ for } m \mid n \\
&n = \prod_{p \in (n)} p
\end{aligned}
$$

となる。 □

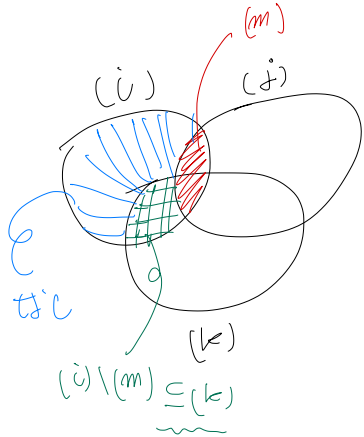
補題 36.5 (ベキの位数の評価、37.4 と 40.5 で使用する)**.** 有限体の非零の元 α に対して、以下が成り立つ。

$$\operatorname{ord}(\alpha^j) = \operatorname{ord}(\alpha) / \gcd\bigl(\operatorname{ord}(\alpha), j\bigr)$$

この命題は、元 α の j 乗の位数がどうなるかを教えてくれています。

証明. $k := \operatorname{ord}(\alpha^j), i := \operatorname{ord}(\alpha), m := \gcd(\operatorname{ord}(\alpha), j)$ として、$k = i/m$ を示す。

【$i/m \mid k$ を示す】$k = \operatorname{ord}(\alpha^j)$ より、$1 = (\alpha^j)^k = \alpha^{jk}$ となる。36.2 より $i \mid jk$ を得る。これと $\gcd(i,j) = m$ から $i/m \mid k$ を得る。実際、$(i) \subset (j) \cup (k)$ と $(i) \cap (j) = (m)$ より、$(i) \setminus (m) \subset (k)$ はベン図を書けば明らかに成り立つ。



【$k \mid i/m$ を示す】$i = \mathrm{ord}(\alpha)$ より、$(\alpha^j)^{i/m} = (\alpha^i)^{j/m} = 1$ である。36.2 より、$k \mid i/m$ を得る。 □

補題 36.6 (互いに素な位数を有する 2 つ元の積の位 数は、それらの位数の積になる．37.4 で使用する)**.** 有限体 $\mathbb{F}$ の非零の元 $\alpha, \beta \in \mathbb{F}$ に対して、$i := \mathrm{ord}(\alpha), j := \mathrm{ord}(\beta)$ とする。以下が成り立つ。

$$\gcd(i, j) = 1 \Rightarrow \mathrm{ord}(\alpha\beta) = ij$$

37.14 で、有限体の非零元は周期性を持つ巡回群となることを学ぶ。この命題は、周期が互いに素な 2 つの回転（元）を組

み合わせると、その合成の周期は単純にかけ算になることを教えてくれている。

証明.

$$(\alpha\beta)^{ij} = \alpha^{ij}\beta^{ij} = (\alpha^i)^j(\beta^j)^i = 1 \times 1 = 1$$

となる。36.2 より、

$$\mathrm{ord}(\alpha\beta) \mid ij$$

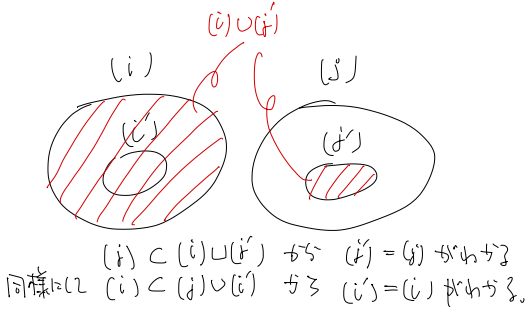
を得る。これと $\gcd(i,j) = 1$ から、$i' \mid i, j' \mid j$ となる整数 i', j' が存在して、

$$\mathrm{ord}(\alpha\beta) = i'j' \tag{36.7}$$

となることを意味する。あとは、$\gcd(i,j) = 1 \Rightarrow i = i', j = j'$ を示せば十分である。(36.7) より、$(\alpha\beta)^{i'j'} = 1$ である。

$$1 = \left((\alpha\beta)^{i'j'}\right)^{i/i'} = \alpha^{ij'}\beta^{ij'} = 1 \times \beta^{ij'} = \beta^{ij'}$$
$$1 = \left((\alpha\beta)^{i'j'}\right)^{j/j'} = \alpha^{i'j}\beta^{i'j} = \alpha^{i'j} \times 1 = \alpha^{i'j}$$

となる。これらと 36.2 より、それぞれ $j \mid ij', i \mid i'j$ を得る。これらと $i' \mid i, j' \mid j$ と $\gcd(i,j) = 1$ から、$j = j', i = i'$ を得る。



□

37　体の原始元

この節では，有限体の元を表現するのにとても便利な原始元を学ぶ.

定義 37.1 (原始元)**.** サイズ q の有限体 $\mathbb{F}_q$ の元 $\alpha \in \mathbb{F}_q$ の位数が $q-1$、言い換えると

$$q - 1 = \mathrm{ord}(\alpha)$$

であるとき、α は $\mathbb{F}_q$ の原始元であるという。原始元 $\alpha \in \mathbb{F}_q$ を用いて、$\mathbb{F}_q$ を、α のべきの形で網羅的に列挙したものにゼロ

を付け加えた集合

$$\mathbb{F}_q = \{0, \alpha^0 = \alpha^{q-1} = 1, \alpha^1, \ldots, \alpha^{q-2}\}$$

と表すことができる。原始元が存在することは、定理 37.4 で証明する。 □

例 37.2. 既約多項式 $1 + X + X^2$ によって構成された $\mathbb{F}_4 := \mathbb{F}_2[X]/\langle 1 + X + X^2 \rangle = \{[00], [10], [01], [11]\}$ に対して、位数を計算して原始元を見つよう。

$[10] = 1$ なので $\mathrm{ord}([10]) = \boxed{1}$,
$[01]^2 = [11], [01]^3 = [11] \times [01] = [10]$ なので $\mathrm{ord}([01]) = \boxed{3}$,

$[11]^2 = [01], [11]^3 = [01] \times [11] = [10]$ なので $\mathrm{ord}([11]) = \boxed{3}$

となり、$[01], [11]$ のふたつは $\mathbb{F}_4$ の原始元である。 □

例 37.3. $\mathbb{F}_{11} := \mathbb{Z}/11\mathbb{Z}$ の演算表を示す。

x	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]
[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]
[2]	[0]	[2]	[4]	[6]	[8]	[10]	[1]	[3]	[5]	[7]	[9]
[3]	[0]	[3]	[6]	[9]	[1]	[4]	[7]	[10]	[2]	[5]	[8]
[4]	[0]	[4]	[8]	[1]	[5]	[9]	[2]	[6]	[10]	[3]	[7]
[5]	[0]	[5]	[10]	[4]	[9]	[3]	[8]	[2]	[7]	[1]	[6]
[6]	[0]	[6]	[1]	[7]	[2]	[8]	[3]	[9]	[4]	[10]	[5]
[7]	[0]	[7]	[3]	[10]	[6]	[2]	[9]	[5]	[1]	[8]	[4]
[8]	[0]	[8]	[5]	[2]	[10]	[7]	[4]	[1]	[9]	[6]	[3]
[9]	[0]	[9]	[7]	[5]	[3]	[1]	[10]	[8]	[6]	[4]	[2]
[10]	[0]	[10]	[9]	[8]	[7]	[6]	[5]	[4]	[3]	[2]	[1]

$$[2]^0 = [1], [2]^1 = [2], [2]^2 = [4], [2]^3 = [8],$$
$$[2]^4 = [5], [2]^5 = [10], [2]^6 = [9], [2]^7 = [7],$$
$$[2]^8 = [3], [2]^9 = [6], [2]^{10} = [1]$$

となり、$[2] \in \mathbb{F}_{11}$ は $\mathbb{F}_{11}$ の原始元であることが分かる。 □

定理 37.4 (原始元の存在)**.** サイズ q の有限体 $\mathbb{F}_q$ には原始元が存在する。$\mathbb{F}_q$ に存在する原始元の数はオイラー関数 $\phi(q-1)$ で与えられることは、演習で扱う。 □

証明. 位数が最大となる $\mathbb{F}_q$ の非零元を $\alpha \neq 0$ と書く。$i := \mathrm{ord}(\alpha)$ とする。最大位数元 α が定義できるためには、すべての非零元の位数が有限でなければならない。これは演習で証明する。この最大位数元 α が原始元であることを主張する。$i = q-1$ であることを示せば十分である。

【$i \leq q-1$ であること】$\alpha^1, \alpha^2, \ldots, \alpha^i = 1 \in \mathbb{F}_q \setminus \{0\}$ はすべ

て異なることを主張する。すべて異なるわけではない、つまり

$$\alpha^{i_1} = \alpha^{i_2} \text{ with } 0 \leq i_1 < i_2 \leq i$$

と仮定すると、$\alpha^{i_2 - i_1} = 1$ with $0 < i_2 - i_1 < i$ となり、$i = \mathrm{ord}(\alpha)$ であることに矛盾する。これより、$\alpha^1, \alpha^2, \ldots, \alpha^i = 1 \in \mathbb{F}_q$ は全て異なっていることがわかる。非ゼロ元のべきは非ゼロになることと、$\mathbb{F}_q$ の非ゼロ元は $q-1$ 個あることから、$i \leq q-1$ が導ける。

【$i \geq q-1$ であること】非零元 $\beta (\neq 0) \in \mathbb{F}_q$ に対して、$j := \mathrm{ord}(\beta)$ とする。非零元位数 j と最大位数 i に対して、

$$j \mid i \tag{37.5}$$

であることを主張する。$j \mid i$ でないと仮定する。すると、$(j) \not\subset (i)$ であるから、(j) はある素因子 $p \in (j)$ を (i) より多く含んでいるはずである。この数をそれぞれ k, l とすると、

$$\begin{aligned} i &= p^k i', \\ j &= p^l j', \\ &\text{with } l > k, && (37.6) \\ &\gcd(p, i') = 1 && (37.7) \\ &\gcd(p, j') = 1 && (37.8) \end{aligned}$$

と書けるはずである。36.5 より、以下が成り立つ。i は α の

位数。

$$\mathrm{ord}(\alpha^{p^k}) \overset{36.5}{=} i/\gcd(i,p^k) = p^k i'/p^k = i'$$
$$\mathrm{ord}(\beta^{j'}) \overset{36.5}{=} j/\gcd(j,j') = p^l j'/j' = p^l$$

(37.7) と (37.8) より、これらの位数は互いに素:$\gcd(i',p^l)=1$ となる。これと 36.6[互いに素な位数を有する 2 つ元の積の位数は、それらの位数の積になる] より、

$$\mathrm{ord}(\alpha^{p^k}\times\beta^{j'}) \overset{36.6}{=} \mathrm{ord}(\alpha^{p^k})\mathrm{ord}(\beta^{j'}) = p^l i' \overset{(37.6)}{>} p^k i' = i$$

となる。i より大きな位数の元 $\alpha^{p^k}\times\beta^{j'}\in\mathbb{F}$ が存在することになり α が最大位数元であることに矛盾するので、結局 $j \mid i$ となる。これを用いて、

$$\beta^i = \beta^{ji/j} = (\beta^j)^{i/j} = 1$$

となる。非ゼロ要素 $\beta\in\mathbb{F}_q$ は任意に選ばれたことを思い出すと、$\mathbb{F}_q$ の $q-1$ 個の非零元 β はすべて $-1+X^i$ の根である、正確に述べると

$$\beta\in\mathbb{F}_q, \beta\neq 0 \Longrightarrow -1+\beta^i = 0 \tag{37.9}$$

であることが分かる。代数の基本定理により、次数 i の多項式は高々i 個の根しかもたないので、$-1+X^i$ の根の個数 $= q-1 \leq i$ となる。

【まとめ】まとめると、最大位数元 $\alpha\in\mathbb{F}_q$ の位数 i は $q-1$ に一致し、α は原始元になることが分かる。 □

定理 37.10 (一般化されたフェルマーの小定理)**.** サイズ q の有限体の任意の元 α は、$f(X) := X^q - X$ に対して $f(\alpha) = 0$ を満たす。[29] これより、$\alpha^q = \alpha$ となることが分かる。さらに,

$$\left.\begin{aligned} \prod_{\alpha \in \mathbb{F}_q} (X - \alpha) &= X^q - X, \\ \prod_{\alpha \in \mathbb{F}_q^\times} (X - \alpha) &= X^{q-1} - 1 \end{aligned}\right\} \tag{37.11}$$

が成り立つ. □

証明. $\alpha = 0$ に対しては、明らか。(37.9) より、非零元 $\alpha \in \mathbb{F}_q$ に対して、$\alpha^{q-1} = 1$ であったから、$f(\alpha) = \alpha^q - \alpha = 0$ は成り立つ。$X^q - X$ は $\mathbb{F}_q$ の元をすべて根に持つ。代数の基本定理から $X^q - X$ は高々$q - 1$ 個の異なる元を有するので、これ以外の根は持たいない。これより，(37.11) が分かる. □

系 37.12. 有限体 $\mathbb{F}_q$ の非零元の位数は $q - 1$ を割り切る。

証明. (37.5) より分かる。 □

定義 37.13 (巡回群 (cyclic group))**.** ある群 G が一つの元 $g \in G$ を用いて、

$$G = \{g^n \mid n \in \mathbb{Z}, n \geq 0\}$$

[29] q が素数 p の場合にはフェルマーの小定理 $a^{p-1} \equiv 1 \pmod{p}$http://bit.ly/2Rm56Ww として知られている。

と書けるとき、G は g によって生成される巡回群であるといい、$G = \langle g \rangle$ と書く。G のサイズを G の位数という。 □

命題 37.14 (有限体の乗法群は巡回群になる)**.** 有限体 $\mathbb{F}_q$ の非零の元の集合 $\mathbb{F}_q^\times$ は乗法に関して位数 $q-1$ 巡回群をなす。□

証明. 非零の元の集合は、原始元 α によって、

$$\mathbb{F}_q^\times = \{\alpha^1, \ldots, \alpha^{q-1}(=1)\}$$

と書けた。任意の $n \in \mathbb{Z}$ に対して、

$$\alpha^n = \alpha^{n \bmod q-1} \in \mathbb{F}_q^\times$$

である。これから、主張が正しいことが分かる。 □

命題 37.15 (有限体上のべき乗計算の効率的な方法)**.** 非零元 $\beta \in \mathbb{F}_q$ に対して、べき乗 β^n を大きな $n \gg 1$ でも高速に計算したい。以下のようにして原始元 $\alpha \in \mathbb{F}_q$ を用いて効率的に計算することができる。

1. $1, \alpha, \alpha^2, \ldots, \alpha^{q-2}$ の順で $\mathbb{F}_q^\times$ の要素を列挙する。
2. $\alpha^k = \beta$ となる $k \in \{0, 1, \ldots, q-2\}$ を求める。
3. $j := kn \bmod q-1$ を求める。
4. $\beta^n = \alpha^j$ として、出力する。

□

証明. $kn/(q-1)$ = 商 a 余り j とすると、$\beta^n = (\alpha^k)^n = \alpha^{kn} = \alpha^{a(q-1)+j} = \alpha^{a(q-1)}\alpha^j = (\alpha^{(q-1)})^a\alpha^j = \alpha^j$ となる。□

38 原始元による有限体の表現 @11

例 38.1. 既約多項式 $f(X) = 1 + X + X^6 \in \mathbb{F}_2[X]$ で定義される $\mathbb{F}_{64} = \mathbb{F}_2[X]/\langle f(X)\rangle$ に対して、$\alpha := [X]$ は原始元である。$[1 + X + X^6] = [0]$ なので、

$$1 + \alpha + \alpha^6 = 0 \tag{38.2}$$

となる。これを利用して、べき表現と 6 次未満の α の多項式表現またはそれと等価な長さ 6 のベクトル表現を 38.3 のよう

に得ることができる。例えば、

$$\alpha^1 = [010000] \quad \alpha^2 = [001000] \quad \alpha^3 = [000100]$$
$$\alpha^4 = [000010] \quad \alpha^5 = [000001]$$
$$\alpha^6 \overset{(38.2)}{=} 1 + \alpha = [110000]$$
$$\alpha^7 = \alpha \times \alpha^6 = \alpha(1 + \alpha) = \alpha + \alpha^2 = [0110000]$$
$$\alpha^8 = \alpha \times \alpha^7 = \alpha(\alpha + \alpha^2) = \alpha^2 + \alpha^3 = [0011000]$$
$$\vdots$$
$$\alpha^{54} = \alpha \times \alpha^{53} = \alpha \times (\boxed{\alpha + \alpha^3 + \alpha^5}) = \boxed{\alpha^2 + \alpha^4 + \alpha^6}$$
$$\overset{(38.2)}{=} \boxed{1 + \alpha + \alpha^2 + \alpha^4} = [\boxed{111010}]$$

である。この表を用いて、乗算はべき表現によって、加算はベクトル表現によって、簡単に行うことができる。上記の議論は、原始多項式の定義をしたあとで一般的に 40.7 でもう一度議論する。

注意：任意の既約多項式 $f(X)$ に対して、$[X] \in \mathbb{F}_p[X]/\langle f(X)\rangle$ が原始元になるとは限らないので注意しよう。例えば、$1 + X + X^2 + X^3 + X^4 \in \mathbb{F}_2[X]$ は既約多項式だが $[X] \in \mathbb{F}_2[X]/\langle 1 + X + X^2 + X^3 + X^4\rangle$ は下記の計算により $[X]^5 = 1$ となり、15 乗する前に 1 になってしまうので、原始元ではない。$[X]^4 = 1 + X + X^2 + X^3, [X]^5 = XX^4 = X(1 + X + X^2 + X^3) = X((1 + X + X^2) + X^3) = (X + X^2 + X^3) + X^4 = (X + X^2 + X^3) + 1 + X + X^2 + X^3 = 1$

□

$\alpha^{1} = [010000]$ $\alpha^{22} = [101011]$ $\alpha^{43} = [111011]$
$\alpha^{2} = [001000]$ $\alpha^{23} = [100101]$ $\alpha^{44} = [101101]$
$\alpha^{3} = [000100]$ $\alpha^{24} = [100010]$ $\alpha^{45} = [100110]$
$\alpha^{4} = [000010]$ $\alpha^{25} = [010001]$ $\alpha^{46} = [010011]$
$\alpha^{5} = [000001]$ $\alpha^{26} = [111000]$ $\alpha^{47} = [111001]$
$\alpha^{6} = [110000]$ $\alpha^{27} = [011100]$ $\alpha^{48} = [101100]$
$\alpha^{7} = [011000]$ $\alpha^{28} = [001110]$ $\alpha^{49} = [010110]$
$\alpha^{8} = [001100]$ $\alpha^{29} = [000111]$ $\alpha^{50} = [001011]$
$\alpha^{9} = [000110]$ $\alpha^{30} = [110011]$ $\alpha^{51} = [110101]$
$\alpha^{10} = [000011]$ $\alpha^{31} = [101001]$ $\alpha^{52} = [101010]$
$\alpha^{11} = [110001]$ $\alpha^{32} = [100100]$ $\alpha^{53} = [010101]$
$\alpha^{12} = [101000]$ $\alpha^{33} = [010010]$ $\alpha^{54} = [111010]$
$\alpha^{13} = [010100]$ $\alpha^{34} = [001001]$ $\alpha^{55} = [011101]$
$\alpha^{14} = [001010]$ $\alpha^{35} = [110100]$ $\alpha^{56} = [111110]$
$\alpha^{15} = [000101]$ $\alpha^{36} = [011010]$ $\alpha^{57} = [011111]$
$\alpha^{16} = [110010]$ $\alpha^{37} = [001101]$ $\alpha^{58} = [111111]$
$\alpha^{17} = [011001]$ $\alpha^{38} = [110110]$ $\alpha^{59} = [101111]$
$\alpha^{18} = [111100]$ $\alpha^{39} = [011011]$ $\alpha^{60} = [100111]$
$\alpha^{19} = [011110]$ $\alpha^{40} = [111101]$ $\alpha^{61} = [100011]$
$\alpha^{20} = [001111]$ $\alpha^{41} = [101110]$ $\alpha^{62} = [100001]$
$\alpha^{21} = [110111]$ $\alpha^{42} = [010111]$ $\alpha^{63} = [100000]$

図 38.3: $\mathbb{F}_{64}$ の原始元のべき表現とベクトル表現

39　標数と有限体の要素数

これまでに、素数のべきのサイズで表される有限体を構成する方法を学んだ。この節では、この方法で与えられたとは限らない任意の有限体のサイズは、素数のべきで与えられること 39.5 を学ぶ。

定義 39.1 (標数 (characteristic))**.** 体 $\mathbb{F}$ において乗法単位元 1 を m 回足したものを

$$m_{\mathbb{F}} := \overbrace{1 + \cdots + 1}^{m \text{ 回}}$$

と書く。$m_{\mathbb{F}} = 0$ となる最小の $m > 0$ を $\mathbb{F}$ の標数という。$\mathbb{F}$ の標数が存在しない場合には、$\mathbb{F}$ の標数は 0 と定義される。$0_{\mathbb{F}} = 0, 1_{\mathbb{F}} = 1$ である。 □

命題 39.2. 有限体 $\mathbb{F}$ の標数は素数である。 □

証明. $\mathbb{F}$ の標数 m が合成数であると仮定する。

$$m = i \times j, \text{ with } 1 < i, j < m \tag{39.3}$$

m が標数であることから,

$$0_{\mathbb{F}} = m_{\mathbb{F}} = (i \times j)_{\mathbb{F}} = i_{\mathbb{F}} \times j_{\mathbb{F}}$$

が成り立つ。これより、$i_{\mathbb{F}} = 0$ or $j_{\mathbb{F}} = 0$ であるが、(39.3) から標数 m の最小性に矛盾する。 □

命題 39.4. 標数 p の有限体 $\mathbb{F}$ に対して、

$$\mathbb{F}^{(p)} := \{0_{\mathbb{F}}, 1_{\mathbb{F}}, \ldots, (p-1)_{\mathbb{F}}\}$$

は $\mathbb{F}$ と同じ演算によって位数 p の体となる。 □

証明. ここで、要素数 p の有限体

$$\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z} = \{[0], [1], \ldots, [p-1]\}$$

に対して、全単射

$$\phi : i_{\mathbb{F}} \in \mathbb{F}^{(p)} \mapsto [i] \in \mathbb{F}_p$$

を考える。この対応によって、演算結果も対応する（同型となる）。

$$i_{\mathbb{F}} + j_{\mathbb{F}} \mapsto [i+j] = [i] + [j]$$
$$i_{\mathbb{F}} \times j_{\mathbb{F}} \mapsto [i \times j] = [i] \times [j]$$

したがって、$\mathbb{F}^{(p)} \subset \mathbb{F}$ は体となることが分かる。 □

定理 39.5. 要素数 q で標数 p の有限体 $\mathbb{F}$ に対して、要素数 q は標数 p のべき乗で表される。正確に述べると、ある整数 $u \geq 1$ が存在して、以下が成り立つ。

$$q = p^u$$

□

証明. まず、有限体 $\mathbb{F}$ を $\mathbb{F}^{(p)}$ 上の線形空間とみなすことができることを示す。$\mathbb{F}$ の要素 x, y は

$$\begin{aligned} x+y &\in \mathbb{F}, \\ i_{\mathbb{F}}(x+y) &= i_{\mathbb{F}}x + i_{\mathbb{F}}y \in \mathbb{F} \end{aligned}$$

を満たすから、$\mathbb{F}$ は体 $\mathbb{F}^{(p)}$ 上の線形空間となる。この線形空間の次元を u とする。もし u が無限ならば $\mathbb{F}$ が無限集合になってしまうから、u は有限でなければならない。$\mathbb{F}^{(p)}$ 上の u 次元線形空間はサイズ u の基底によって張られるので、$\mathbb{F}$ の要素数は $|\mathbb{F}^{(p)}|^u = p^u$ となる。 □

この節の残りでは、次の節で必要ないくつかの補題を与える。

命題 39.6 (フロベニウスの恒等式)**.** 標数 p の体 $\mathbb{F}$ の要素 α, β と $n > 0$ に対して、

$$(\alpha+\beta)^{p^n} = \alpha^{p^n} + \beta^{p^n} \tag{39.7}$$

が成立する[30]。 □

証明. まず、$n = 1$ の場合の以下を示す。

$$(\alpha+\beta)^{p} = \alpha^{p} + \beta^{p} \tag{39.8}$$

[30] 教員用メモ：$n = 1$ だけで十分なのでは？

2 項展開すると

$$
\begin{aligned}
(\alpha+\beta)^p &= \sum_{k=0}^{p} \overbrace{\alpha^{p-k}\beta^k + \cdots + \alpha^{p-k}\beta^k}^{\binom{p}{k}\text{個}} \\
&= \sum_{k=0}^{p} \overbrace{1_{\mathbb{F}}\alpha^{p-k}\beta^k + \cdots + 1_{\mathbb{F}}\alpha^{p-k}\beta^k}^{\binom{p}{k}\text{個}} \\
&= \sum_{k=0}^{p} (\overbrace{1_{\mathbb{F}} + \cdots + 1_{\mathbb{F}}}^{\binom{p}{k}\text{個}})\alpha^{p-k}\beta^k \\
&= \sum_{k=0}^{p} \binom{p}{k}_{\mathbb{F}} \alpha^{p-k}\beta^k \\
&= \binom{p}{0}_{\mathbb{F}} \alpha^p\beta^0 + \sum_{k=1}^{p-1} \binom{p}{k}_{\mathbb{F}} \alpha^{p-k}\beta^k + \binom{p}{p}_{\mathbb{F}} \alpha^0\beta^p \\
&\overset{\text{(a)}}{=} \binom{p}{0}_{\mathbb{F}} \alpha^p\beta^0 + \sum_{k=1}^{p-1} \binom{p}{k}_{\mathbb{F}} 0 \times \alpha^{p-k}\beta^k + \binom{p}{p}_{\mathbb{F}} \alpha^0\beta^p \\
&= \alpha^p + \beta^p
\end{aligned}
$$

である。(a) が成り立つことは $\binom{p}{k}$ は p で割り切れることと $\binom{p}{0} = \binom{p}{p} = 1$ であることを利用している。実際、$0 < k < p$

に対して、

$$\binom{p}{k} = \frac{p \times (p-1) \times \cdots \times (p-k+1)}{k \times (k-1) \times \cdots \times 2 \times 1}$$

となるが、分子には因子 p を含むが因子が分母には含まないので、$p|\binom{p}{k}$ となる。従って、$\binom{p}{k}_{\mathbb{F}} = 0$ となる。

次に帰納的に、(39.7) が成り立っているときに $n+1$ は、

$$\begin{aligned}(\alpha+\beta)^{p^{n+1}} &= ((\alpha+\beta)^{p^n})^p \\ &= (\alpha^{p^n} + \beta^{p^n})^p \\ &\overset{(39.8)}{=} (\alpha^{p^{n+1}} + \beta^{p^{n+1}})\end{aligned}$$

となる。第 2 等号では、帰納法の仮定を使った。これより、証明が完成する。 □

補題 39.9 (39.12 で使う)**.** 標数 p の有限体 $\mathbb{F}_q$ と次数 d の $\mathbb{F}_q$ 係数多項式

$$f(X) = \sum_{j=0}^{d} f_j X^j \in \mathbb{F}_q[X]$$

に対して以下が成り立つ。

$$\big(f(X)\big)^p = \sum_{j=0}^{d} f_j^p X^{jp} \tag{39.10}$$

特に、$q = p$ の場合には、37.10 より $f_j^p = f_j$ が成り立つので、

$$\big(f(X)\big)^p = \sum_{j=0}^{d} f_j X^{jp} = f(X^p) \tag{39.11}$$

が成り立つ。

証明. [31]最大次数とそれ以外の項に分けて、2 項展開すると、

$$\begin{aligned}
\big(f(X)\big)^p &= \Big(f_d X^d + \sum_{j=0}^{d-1} f_j X^j\Big)^p \\
&= \sum_{i=0}^{p} \binom{p}{i}_{\mathbb{F}_p} (f_d X^d)^i \Big(\sum_{j=0}^{d-1} f_j X^j\Big)^{p-i} \\
&= (f_d X^d)^p + \Big(\sum_{j=0}^{d-1} f_j X^j\Big)^p \\
&= f_d^p X^{dp} + \Big(\sum_{j=0}^{d-1} f_j X^j\Big)^p
\end{aligned}$$

となる。第 3 等号では、フロベニウスの恒等式 39.6 の証明で示したことと同じであるが $0 < i < p$ なる i に対して $\binom{p}{i}_{\mathbb{F}_p} = 0$ となることを使った。同様にして、$\Big(\sum_{j=0}^{d-1} f_j X^j\Big)^p = f_{d-1}^p X^{(d-1)p} + \Big(\sum_{j=0}^{d-2} f_j X^j\Big)^p$ を得る。これを繰り返して、(39.10) を得る。 □

[31]教員メモ：フロベニウスの恒等式 39.6 と証明は同じなので、説明は省略する

補題 39.12 (40.3 で使う)**.** 標数が p である有限体 $\mathbb{F}_q$ において、$f(X) \in \mathbb{F}_p[X]$ とその根 $\beta \in \mathbb{F}_q$ に対して以下が成り立つ。根 β は標数乗してもまた f の根になる。

$$f(\beta) = 0 \Longrightarrow f(\beta^p) = 0$$

これを続けていくと、β^p,β^{p^2}, β^{p^3},... も f の根となることがわかる。

証明. (39.11) より、$\big(f(X)\big)^p = f(X^p)$ である。これに $X = \beta$ を代入すれば明らか。 □

40 最小多項式、原始多項式

次の節で学習する予定の BCH 符号の性質を知るために必要な最小多項式と原始多項式を学ぶ。

定義 40.1 (部分体、拡大体)**.** $\mathbb{F} \subset \mathbb{E}$ に関して、$\mathbb{F}, \mathbb{E}$ が同じ演算で体となるとき $\mathbb{F}$ を $\mathbb{E}$ の部分体、$\mathbb{E}$ を $\mathbb{F}$ の拡大体という。□

定義 40.2 (最小多項式、原始多項式)**.** 素数 p と m 次の既約多項式 $f(X) \in \mathbb{F}_p[X]$ によって定義される有限体 $\mathbb{F}_q = \mathbb{F}_p[X]/\langle f(X)\rangle$ を考えよう。p は $\mathbb{F}_q$ の標数で $q = p^m$ である。以下を定義する。

$\beta \in \mathbb{F}_q$ を根として有する $(M_\beta(\beta) = 0)$ である次数が $\mathbb{F}_p$ 係数の最小のモニック多項式を、$\beta \in \mathbb{F}_q$ の $\mathbb{F}_p$ 上の最小多項式であるといい、$M_\beta(X)$ と書く。

原始元 $\beta \in \mathbb{F}_q$ の $\mathbb{F}_p$ 上の最小多項式は β の原始多項式と呼ばれる。 □

定理 40.3 (最小多項式の構成法、共役根)**.** 40.2 と同じ設定において、$\ell > 0$ を $\beta^{p^\ell} = \beta$ を満たす最小の正数とする。β の最小距離は次のように構成することができる。

$$M_\beta(X) = \prod_{i=0}^{\ell-1}(X - \beta^{p^i})$$

$\deg M_\beta(X) = \ell$ であることがわかる。

定義から $M_\beta(X) \in \mathbb{F}_p[X]$ である。この定理は、右辺も $\mathbb{F}_p$ 係数の多項式となることを主張していることに注意しよう。

このとき、$\beta, \beta^p, \beta^{p^2}, \ldots, \beta^{p^{\ell-1}}$ を最小多項式 $M(X)$ の共役根であるという。特に β が原始元ならば $\ell = m$ である。 □

証明. 右辺を $M(X) := \prod_{i=0}^{\ell-1}(X - \beta^{p^i}) \in \mathbb{F}_q[X]$ と書く。$M(X) = M_\beta(X)$ であること、つまり $M(X)$ が次の 2 つを満たすことを示す。

1. β を根に持つ次数最小のモニック多項式であること
2. $\mathbb{F}_p$ 係数多項式であること:$M(X) \in \mathbb{F}_p[X]$

【1. の証明】β の $\mathbb{F}_p$ 上の最小多項式 $M_\beta(X)$ は、39.12 よりそ

の根の p 乗をまた根に持つので、

$$\begin{aligned}
&\beta,\\
&\beta^{p},\\
&\beta^{p^2} = (\beta^{p})^{p},\\
&\vdots\\
&\beta^{p^{\ell-1}} = (\cdots(\beta^{\overbrace{p)^{p}\cdots)^{p}}^{\ell-1}}
\end{aligned}$$

を根として有するはずである。$M(X)$ はこれらを根に持つので、β を根に持つ次数が最小のモニック多項式であることがわかった。

【2. の証明】まず $(M(X))^p = M(X^p)$ を[32]示す。

$$\begin{aligned}
(M(X))^{p} &= \prod_{i=0}^{\ell-1}(X-\beta^{p^i})^{p}\\
&= \prod_{i=0}^{\ell-1}(X^{p}+(-\beta^{p^i})^{p}) \qquad (40.4)
\end{aligned}$$

第 2 等号ではフロベニウスの恒等式 39.6 または 39.9 の証明と

[32](39.11) から、$M(X) \in \mathbb{F}_p[X]$ ならばこれが成り立つ事が分かる。

同じ議論を使った。ここで、

$$
\begin{aligned}
(-\beta^{p^i})^p &= ((-1)\times\beta^{p^i})^p \\
&= (-1)^p\times(\beta^{p^i})^p \\
&= (-1)^p\times\beta^{p^{i+1}} \\
&= \begin{cases} \beta^{p^{i+1}} = -\beta^{p^{i+1}} & (p\text{ は偶素数：}p=2) \\ -\beta^{p^{i+1}} & (p\text{ は奇素数}) \end{cases}
\end{aligned}
$$

となり、どちらの場合でも $(-\beta^{p^i})^p = -\beta^{p^{i+1}}$ である。これを (40.4) に代入して、

$$
\begin{aligned}
&\big(M(X)\big)^p \\
&= \prod_{i=0}^{\ell-1}(X^p-\beta^{p^{i+1}}) \\
&= (X^p-\beta^{p^1})(X^p-\beta^{p^2})\cdots(X^p-\beta^{p^{\ell-1}})(X^p-\beta^{p^\ell}) \\
&\overset{\text{(a)}}{=} (X^p-\beta^{p^0})(X^p-\beta^{p^1})\cdots(X^p-\beta^{p^{\ell-2}})(X^p-\beta^{p^{\ell-1}}) \\
&= \prod_{i=0}^{\ell-1}(X^p-\beta^{p^i}) \\
&= M(X^p)
\end{aligned}
$$

を得る。(a) では定理の前提 $\beta^{p^\ell}=\beta$ を用いた。

次に、$M(X) =: \sum_{j=0}^{d} f_j X^j \in \mathbb{F}_q[X]$ と係数に名前をつけ

る。次が成り立つ。

$$(M(X))^p \overset{(39.10)}{=} \sum_{j=0}^{d} (f_i X^i)^p = \sum_{j=0}^{d} f_i^p X^{ip}$$

$$M(X^p) = \sum_{j=0}^{d} f_i X^{pi}$$

上で導出した $M(X) = M(X^p)$ からこれらの係数は一致するはずなので、

$$f_i = f_i^p \text{ for } i = 0, \ldots, d$$

が成り立つ。これは、37.10 の証明の議論と同じことだが、以下に示す理由により $f_i \in \mathbb{F}_p$ を意味し、$M(X) \in \mathbb{F}_p[X]$ となり証明が完了する。

$f_i \in \mathbb{F}_p$ を示す。フェルマーの小定理 37.10 より $\mathbb{F}_p$ の p 個の元は $X^p - X = 0$ の根である。$f_i \notin \mathbb{F}_p$ と仮定して矛盾を導こう。代数の基本定理より $X^p - X = 0$ の根は高々 p 個のはずである。$\mathbb{F}_p$ に含まれない $f_i \notin \mathbb{F}_p$ が $f_i = f_i^p$ となったと仮定すると、上記の p 個の元に加えて f_i が根になるので、根が p 個より多く存在してしまうので矛盾となる。 □

定理 40.5 (原始多項式の根はすべて原始元になる)**.** $q = p^m$ として、原始元 $\alpha \in \mathbb{F}_q$ の $\mathbb{F}_p$ 上の最小多項式 (つまり原始多項式) を $M_\alpha(X)$ とする。原始多項式 $M_\alpha(X)$ の任意の根 $\beta \in \mathbb{F}_q$ は、$\mathbb{F}_q$ の原始元となる。 □

証明. 原始元 α の定義 37.1 より、m は $\alpha^{p^m} = \alpha$ を満たす最小の正数である。原始多項式 (原始元 α の最小多項式)$M_\alpha(X) \in \mathbb{F}_p[X]$ の根は、40.3 から α^{p^i} with $0 \leq i < m$ の形をしていることが分かる。各根 α^{p^i} が現資源になっているためには、

$$\mathrm{ord}(\alpha^{p^i}) = q - 1 \tag{40.6}$$

であることを示せば十分である。36.5 と原始元の定義 $\mathrm{ord}(\alpha) = q - 1 = p^m - 1$ より、

$$\begin{aligned} \mathrm{ord}(\alpha^{p^i}) &\overset{36.5}{=} \mathrm{ord}(\alpha)/\gcd(\mathrm{ord}(\alpha), p^i) \\ &= (p^m - 1)/\gcd(p^m - 1, p^i) \end{aligned}$$

である。$\gcd(p^m - 1, p^i) = 1$ であることは、下記のユークリッドの互除法 25 による計算で分かるので (40.6) が示された。

$$\begin{aligned} &(p^m - 1) \div p^i = \text{商 } p^{m-i} \text{あまり } p^i - 1 \\ &p^i \div (p^i - 1) = \text{商 } 1 \text{ あまり } 1 \\ &(p^i - 1) \div 1 = \text{商 } (p^i - 1) \text{ あまり } 0 \end{aligned}$$

□

議論 40.7. 素数 p に対して $q := p^m$ とする。これまでの議論では、有限体を既約多項式 $M_\alpha(X) \in \mathbb{F}_p[X]$ を用いて剰余類環 $\mathbb{F}_p[X]/\langle M_\alpha(X)\rangle$ として代数的に構成してきた。この議論をせずに、38.1 で見たように、原始元 α と原始多項式 $M_\alpha(X)$ が

満たす式 $M_\alpha(X)|_{X=\alpha}=0$ を用いて、有限体を $\mathbb{F}_q$ の計算法と構成を定めることができる。

$\mathbb{F}_p[X]/\langle M_\alpha(X)\rangle$ を考えよう。原始元 α は、$\alpha^1,\alpha^2,\ldots,\alpha^{q-1}$ と計算したときに $\alpha^{q-1}=1$ ではじめて 1 となる。$M_\alpha(\alpha)=0$ であるのと対応して $[X]\in\mathbb{F}_p[X]/\langle M_\alpha(X)\rangle$ は $M_\alpha([X])=0$ を満たす非ゼロ元であるから、$[X]\in\mathbb{F}_p[X]/\langle M_\alpha(X)\rangle$ は、$[X]^{q-1}=1$ ではじめて 1 となる。つまり $[X]$ は $\mathbb{F}_p[X]/\langle M_\alpha(X)\rangle$ の原始元である。

37.1 では、α のべきと 0 によって $\mathbb{F}_q$ が構成されることを学んだ。

$$\mathbb{F}_q=\{0,1,\alpha,\alpha^2,\ldots,\alpha^{q-2}\}$$

これは乗算と除算を行うときに便利な表現となっている。さらに、$M_\alpha(\alpha)=0$ の関係を使って、α の m 次未満の多項式表現によって表すことができる。

$$\mathbb{F}_q=\{f_0+f_1\alpha+f_2\alpha^2+\cdots+f_{m-1}\alpha^{m-1}\mid f_i\in\mathbb{F}_p\}$$

これは加算と減算を行うときに便利な表現となっている。

例 **40.8** (最小多項式の計算の仕方)**.** 原始多項式 $1+X+X^6\in\mathbb{F}_2[X]$ の根 α を用いて定義される $\mathbb{F}_{64}$ に対して、標数は $p=2$ である。40.3 にしたがって $\beta=\alpha^3\in\mathbb{F}_{64}$ の最小多項式 $M_\beta(X)\in\mathbb{F}_2[X]$ を求めてみよう。β の位数は 21 である:$\beta^{21}=(\alpha^3)^{21}=$

$\alpha^{63} = 1$ であった。これをつかって、

$$\beta^{2^5} = \beta^{32} = \beta^{11}$$
$$\beta^{2^6} = \beta^{64} = \beta$$

から $\ell = 6$ がわかる。これらより、β の最小多項式 $M_\alpha(X) \in \mathbb{F}_2[X]$ は以下で与えられる。

$$\begin{aligned}
M_\beta(X) &= \prod_{i=0}^{\ell-1}(X - \beta^{p^i}) \\
&= (X-\beta)(X-\beta^2)(X-\beta^{2^2})(X-\beta^{2^3})(X-\beta^{2^4})(X-\beta^{2^5}) \\
&= (X-\beta)(X-\beta^2)(X-\beta^4)(X-\beta^8)(X-\beta^{16})(X-\beta^{32}) \\
&= (X-\alpha^3)(X-\alpha^6)(X-\alpha^{12})(X-\alpha^{24})(X-\alpha^{48})(X-\alpha^{96}) \\
&= (X-\alpha^3)(X-\alpha^6)(X-\alpha^{12})(X-\alpha^{24}) \\
&\quad \times (X-\alpha^{48})(X-\alpha^{33=96 \bmod 63})
\end{aligned}$$

これより、$M_\beta(X) = M_{\alpha^i}(X)$ for $i = 3, 6, 12, 24, 48, 33$ であることも分かる。$1 + \alpha + \alpha^6 = 0$ となることを利用すると、

$$M_\beta(X) = 1 + X + X^2 + X^4 + X^6$$

を得る。例えば、0 次の係数が 1 となることは、

$$\begin{aligned}
&\alpha^3 \times \alpha^6 \times \alpha^{12} \times \alpha^{24} \times \alpha^{48} \times \alpha^{33} \\
&= \alpha^{45+81} = \alpha^{126 \bmod 63} = \alpha^0 = 1
\end{aligned}$$

と確かめられる。5 次の係数が 0 となることは、

$$\begin{aligned}
&\alpha^3+\alpha^6+\alpha^{12}+\alpha^{24}+\alpha^{48}+\alpha^{33}\\
=&+[000100]\\
&+[110000]\\
&+[101000]\\
&+[100010]\\
&+[101100]\\
&+[010010]\\
&=[000000]=0
\end{aligned}$$

から分かる。 □

定理 40.9 (最小多項式の性質)**.** 素数 p に対して $q=p^m$ とする。原始元とは限らない $\alpha\in\mathbb{F}_q$ の $\mathbb{F}_p$ 上の最小多項式 $M_\alpha(X)$ に対して、次が成り立つ。

1. モニック既約多項式 $f(X)\in\mathbb{F}_p[X]$ に対して、$\alpha\in\mathbb{F}_q$ が $f(X)$ の根ならば、$f(X)$ は α の $\mathbb{F}_p$ 上の最小多項式であることを示せ。

   証明. 演習で扱います。 □

2. $M_\alpha(X)$ は唯一存在する。$M_\alpha(X)$ は既約である。

証明. (存在性：) 最小多項式の構成法 40.3 より明らかあるが、簡単に次のようにも示せる。$f(\alpha)=0$ となるモニック多項式 $f(X)\in\mathbb{F}_p[X]$ がひとつでもあれば、そのうち次数が最小のものは存在するはずなので、あるモニック多項式 $f(X)\in\mathbb{F}_p[X]$ に対して $f(\alpha)=0$ が満たされることを示せば十分である。$f(X)=X^q-X\in\mathbb{F}_p[X]$ と選べばフェルマーの小定理 37.10 より $f(\alpha)=0$ が満たされる。

(既約性：) 既約でないと仮定する。即ち、

$$\begin{aligned} &M_\alpha(X)=f(X)g(X),\\ &0<\deg f(X)<\deg M_\alpha(X),\\ &0<\deg g(X)<\deg M_\alpha(X) \end{aligned}$$

が成り立つ。$M_\alpha(\alpha)=f(\alpha)g(\alpha)=0$ となり $f(\alpha)=0$ or $g(\alpha)=0$ となるが[33]、これは $M_\alpha(X)$ の次数が最小であることに矛盾する。

(唯一性：) 唯一でないと仮定する。異なる 2 つの最小多項式を $M_\alpha(X)\neq M'_\alpha(X)$ と書く。次数の最小性から、項式は次数が同じはずである。

$$f(X):=M_\alpha(X)-M'_\alpha(X)\in\mathbb{F}[X]$$

[33] 対偶：非零元 $x,y\in\mathbb{F}$ に対して $xy\neq 0$ である。実際、$xy=0$ だと仮定すると、右から y^{-1} を書けて $x=0$ となり矛盾する。

は非零多項式になり、

$$f(\alpha) = 0$$
$$\deg f(X) < \deg M_\alpha(X) = \deg M'_\alpha(X)$$

が成り立つ。$f(X)$ は定数倍することでモニックにすることができるので、最小多項式の次数最小性に矛盾する。□

3. α の最小多項式は、α を根として有する多項式を割り切る。正確に述べると、$f(X) \in \mathbb{F}_p[X]$ に対して、$f(\alpha) = 0$ ならば $M_\alpha(X) | f(X)$ である。

証明. $f(X)$ を $M_\alpha(X)$ で割って、

$$f(X) = M_\alpha(X)q(X) + r(X), \qquad (40.10)$$
$$\deg r(X) < \deg M_\alpha(X)$$

だとする。割り切れないと仮定すると、$r(X) \neq 0$ であるが、(40.10) の X に α を代入して、$0 = r(\alpha)$ となる。$r(X)$ を定数倍してモニックにできるので、$M_\alpha(X)$ の次数の最小性に矛盾する。□

4. $M_\alpha(X) \mid X^q - X$

証明. フェルマーの小定理 37.10 より $\alpha^q - \alpha = 0$ であるから、α は $X^q - X$ の根である。3 より、$M_\alpha(X) \mid X^q - X$ が成り立つ。□

5. 非ゼロ元 $\beta \in \mathbb{F}_q^\times$ に対して、最小多項式 $M_\beta(X) \in \mathbb{F}_p[X]$ の集合を $\mathcal{M}$ と書く。

$$\mathcal{M} = \{M_\beta(X) \mid \beta \in \mathbb{F}_q^\times\}$$

$M_\beta(X) \in \mathcal{M}$ に対して、$M_\beta(X)$ の根の集合を $[\beta]$ と書く。40.3 より

$$[\beta] = \{\beta^{p^0}, \beta^{p^1}, \beta^{p^2}, \ldots\}$$

となる。次が成り立つ。

(a) 異なる $[\beta], [\beta']$ は互いに素である。

(b) $\bigcup_{\beta \in \mathbb{F}_q^\times} [\beta] = \mathbb{F}_q^\times$

(c) $\prod_{M(X) \in \mathcal{M}} M(X) = X^{q-1} - 1$

具体例を 41.4 で与える。

証明. 非ゼロ元集合 $\mathbb{F}_q^\times$ の上で、$\beta, \beta' \in \mathbb{F}_q$ が非負整数 i を用いて $\beta^{p^i} = \beta'$ と書ける関係 $\beta \sim \beta'$ は同値関係になる[34]。この同値関係は $\mathbb{F}_q^\times$ 上で商集合 $\mathbb{F}_q^\times / \sim$ を与える。40.3 より β を含む同値類 $\{\beta^{p^0}, \beta^{p^1}, \beta^{p^2}, \ldots, \beta^{p^{\ell-1}}\}$ は $M_\beta(X)$ の根の集合 $[\beta]$ と一致する。ただし、ℓ は $\beta^{p^\ell} = \beta$ となる

[34] $\mathbb{F}_q^\times$ が位数が $p^m - 1$ の巡回群になることと、フェルマーの小定理と、https://bit.ly/49iuHsv から分かる。

最小の正整数 ℓ である。同値類は分割を与えること 9.7 から、5a と 5b は明らか。5b から、次が成り立つ:

$$\prod_{M(X)\in\mathcal{M}} M(X) = \prod_{\beta\in\mathbb{F}_q^\times} (X-\beta)$$

一方、$\prod_{\beta\in\mathbb{F}_q^\times}(X-\beta) \overset{37.10}{=} X^{q-1}-1$ が成り立つことから 5c は証明される。 □

6. $\deg M_\alpha(X) \leq m$

証明. フェルマーの小定理 $\alpha^{p^m}=\alpha$ から、$\alpha^{p^\ell}=\alpha$ を満たす最小の正数 $\ell>0$ は $\ell\leq m$ となる。最小多項式の構成法 40.3 から $\ell=\deg M_\alpha(X)\leq m$ は明らか。次のようにも証明できる。

38.1 でみたように、$\mathbb{F}_q$ は $\mathbb{F}_p$ 上の m 次元線形空間と見なせた。$m+1$ 個の元 $1,\alpha,\alpha^2,\ldots,\alpha^m$ は線形従属となる。言い換えると $(0,\ldots,0)\neq(f_0,\ldots,f_m)\in\mathbb{F}_p^{m+1}$ が存在して

$$\sum_{i=0}^{m} f_i\alpha^i = 0$$

となる。即ち、多項式

$$f(X) := \sum_{i=0}^{m} f_i X^i \in \mathbb{F}_p[X]$$

は次数が m 以下で、α を根として有する。したがって、3 から $M_\alpha(X)|f(X)$ となり、これは $\deg M_\alpha(X) \leq \deg f(X) \leq m$ を意味する。 □

7. 原始元 $\alpha \in \mathbb{F}_q$ の原始多項式 $M_\alpha(X)$ に対して、$\deg M_\alpha(X) = m$ を得る。

   証明. 原始元 α に対して $\alpha^{p^\ell} = \alpha$ を満たす最小の正数 $\ell > 0$ は $\ell = m$ となる。最小多項式の構成法 40.3 から $\ell = \deg M_\alpha(X) = m$ となる。 □

8. 最小多項式 $M_\alpha(X)$ の根は全て同じ位数を有する。

   証明. 証明は演習問題で扱う。 □

□

41 BCH 符号 @12

令和 7 年度の期末試験、12 月 27 日 (木)M-B104(H103)
https://bit.ly/488Hmy0
【学修アンケートに答えてもらう】この節では、素数 p に対して訂正能力が $t > 0$ 以上の $\mathbb{F}_p$ 上の巡回符号を構成する。

定義 41.1 (ヴァンデルモンド行列)**.** 体 $\mathbb{F}$ の元 $x_1, \ldots, x_n$ に対して、$\mathbb{F}$ 上の $n \times n$ 行列

$$V(x_1, \ldots, x_n) := \begin{pmatrix} x_1^0 & x_1^1 & x_1^2 & \cdots & x_1^{n-1} \\ x_2^0 & x_2^1 & x_2^2 & \cdots & x_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ x_n^0 & x_n^1 & x_n^2 & \cdots & x_n^{n-1} \end{pmatrix}$$

を $x_1, \ldots, x_n$ で定義されるヴァンデルモンド行列という。ただし、$0^0 = 1$ とする。 □

補題 41.2 (ヴァンデルモンド行列の行列式)**.** $x_1, \ldots, x_n$ で定義されるヴァンデルモンド行列 $V(x_1, \ldots, x_n)$ の行列式は次で与えられる。

$$\begin{aligned} \det V(x_1, \ldots, x_n) &= \prod_{1 \le i < j \le n} (x_j - x_i) \\ &= (-1)^{n(n-1)/2} \prod_{1 \le i < j \le n} (x_i - x_j) \end{aligned}$$

特に、$x_1, \ldots, x_n$ が互いに異なっていれば、行列式 https://bit.ly/47NaM38 は非零となる。

証明. 線形代数の授業で学習しているはず。証明は、http://bit.ly/2AYOjU1 で見つけることができる。 □

定義 41.3 (BCH 符号)**.** $n := q-1 := p^m-1$ とする。$\alpha \in \mathbb{F}_q$ を原始元とする。$\alpha^{q-1}=1$ となる。$\hat{d} \leq q-1$ なる $\hat{d}$ に対して、

$$\alpha^1, \alpha^2, \alpha^3, \ldots, \alpha^{\hat{d}-1} \in \mathbb{F}_q$$

を根とする、$\mathbb{F}_p$ 上の次数が最小のモニック多項式を $g(X)$ と書く。$g(X)$ は X^n-1 を割り切る。証明は、演習問題で扱う。これより、$g(X)$ は長さ n の $\mathbb{F}_p$ 上の巡回符号 C の生成多項式となる。$g(X) \in \mathbb{F}_p[X]$ を生成多項式とする $\mathbb{F}_p$ 上の符号長 n の巡回符号を、設計距離 $\hat{d}$ の BCH 符号という[35]。 □

例 41.4. 原始多項式 $1+X+X^4 \in \mathbb{F}_{p=2}[X]$ によって定義される $\mathbb{F}_{16}$ の原始元を α とする。各非零元 $\alpha^i \in \mathbb{F}_{16}$ の $\mathbb{F}_2$ 上の最小多項式を $m_i(X)$ と書く。40.2 の表記を用いると、$m_i(X) = M_{\alpha^i}(X)$ である。$\beta = \alpha^i$ に対して、

$$\begin{aligned} M_{\alpha^i=\beta}(X) &= (X-\beta^{p^0})(X-\beta^{p^1})\cdots(X-\beta^{p^{\ell-1}}) \\ &= (X-\alpha^{ip^0})(X-\alpha^{ip^1})\cdots(X-\alpha^{ip^{\ell-1}}) \end{aligned}$$

とかける。40.8 と同様の方法で $m_i(X) \in \mathbb{F}_2[X]$ を計算したも

[35] 設計距離が最小距離の下界になっていることを 41.7 で示します。

のが以下の通りである。

α^i	$m_i(X)$
α^0	$1+X$
$\alpha, \alpha^2, \alpha^4, \alpha^8$	$1+X+X^4$
$\alpha^3, \alpha^{3\times 2=6}, \alpha^{6\times 2=12}, \alpha^{12\times 2=24=9}$	$1+X+X^2+X^3+X^4$
$\alpha^5, \alpha^{5\times 2=10}$	$1+X+X^2$
$\alpha^7, \alpha^{7\times 2=14}, \alpha^{14\times 2=13}, \alpha^{13\times 2=26=11}$	$1+X^3+X^4$

40.9 の 5 によると、$m_i(X), m_j(X)$ for $i \neq j$ は一致するか、そうでなければ共通の根をもたない。さらに、これら 5 つの最小多項式をすべてかけると $X^{15}-1$ となる。

$t=2$ ビットまでの誤りを訂正可能な設計距離 $2t+1=5=:\hat{d}$ の BCH 符号の生成多項式 $g(X)$ を構成してみよう。$g(X)$ は

$$\alpha^1, \alpha^2, \alpha^3, \alpha^{4=\hat{d}-1}$$

を根に含む次数が最小のモニック多項式である。$\alpha, \alpha^2, \alpha^4$ の最小多項式はすべて $1+X+X^4$ で、α^3 の最小多項式は $1+X+X^2+X^3+X^4$ である。したがって、

$$g(X) = \overbrace{(1+X+X^4)}^{\alpha,\alpha^2,\alpha^4\text{の最小多項式}} \overbrace{(1+X+X^2+X^3+X^4)}^{\alpha^3\text{の最小多項式}}$$

となる。

同様にして、$t=3$ ビットまでの誤りを訂正可能な設計距離 $2t+1=7=:\hat{d}$ の BCH 符号の生成多項式 $g(X)$ を求めよう。$g(X)$ は

$$\alpha^1,\alpha^2,\alpha^3,\ldots,\alpha^{6=\hat{d}-1}$$

を根に含む次数最小のモニック多項式である。

$$g(X)=\overbrace{(1+X+X^2+X^3+X^4)}^{\alpha^3,\alpha^6\text{の最小多項式}}\overbrace{(1+X+X^4)}^{\alpha,\alpha^2,\alpha^4\text{の最小多項式}}\times\overbrace{(1+X+X^2)}^{\alpha^5\text{の最小多項式}}$$

となることが分かる。$\deg g=8$ なので，C は $\mathbb{F}_2$ 上の $[n=15,k=7]$ 線形符号である。この巡回符号のパリティ検査多項式は

$$h(X):=\frac{X^{15}-1}{g(X)}=1+X^4+X^6+X^7$$

で与えられる。 □

定理 41.5 (BCH 符号の生成多項式)**.** $\mathbb{F}_p$ 上の符号長 $n:=q-1:=p^m-1$ の設計距離 $\hat{d}$ の BCH 符号の生成多項式 $g(X)\in\mathbb{F}_p[X]$ は次で与えられる。

$$g(X)=\mathrm{lcm}(m_1(X),m_2(X),\ldots,m_{\hat{d}-1}(X)) \quad (41.6)$$

ここで、$m_i(X)$ は α^i の $\mathbb{F}_p$ 上の最小多項式、lcm は最小公倍多項式を表す。 □

証明. (41.6) の右辺 $\mathrm{lcm}(\cdot)$ を考えよう。最小公倍多項式は各多項式 $m_i(X)$ の約多項式の和集合に含まれる多項式の積である。各 $m_i(X)$ は $\mathbb{F}_2[X]$ 上で既約 [40.9 の 2] なので、$m_i(X)$ の約多項式は $m_i(X)$ だけである。したがって、(41.6) の右辺 $\mathrm{lcm}(\cdot)$ は、異なる $m_i(X)$ の積である[36]。

一方、(41.6) の左辺である生成多項式 $g(X)$ は $\alpha^1, \alpha^2, \ldots, \alpha^{\hat{d}-1}$ を根に含む次数最小のモニック多項式である。$m_i(X)$ は α^i を根に含む既約多項式であったことを思い出そう。40.9 の 5 より、$m_i(X), m_j(X)$ for $i \neq j$ は一致するか、そうでなければ共通の根をもたない。これらのことより、$g(X)$ は異なる $m_i(X)$ for $i = 1, \ldots, \hat{d}-1$ の積である。こうして証明は完成する。 □

定理 41.7 (BCH 限界)**.** $\mathbb{F}_p$ 上の符号長 $n = p^m - 1$、設計距離 $\hat{d}$ の BCH 符号 C に対して、以下が成り立つ。

$$d_{\min}(C) \geq \hat{d}$$

これより、符号 C の訂正能力は $t := \lfloor (\hat{d}-1)/2 \rfloor$ 以上となり、半径 t の限界距離復号によって t 個以下の誤りを訂正できることが分かる。 □

[36] 最小公倍多項式は整数環における最小公倍数に対応するものである。各素数 p_i の最小公倍数 $\mathrm{lcm}(p_1, \ldots, p_k)$ が異なる p_i の積で表せるのと対応して、各既約多項式 $m_i(X)$ の最小公倍多項式 $\mathrm{lcm}(m_1(X), \ldots, p_k(X))$ は異なる $m_i(X)$ の積で表せる。

証明. 重みが $\hat{d}$ より小さい非ゼロ符号語はないことを示したい。$c(X)$ を符号語多項式としよう。$c(X)$ のハミング重みを w と書く。$w < \hat{d}$ であるなら $c(X) = 0$ であることを示せば十分である。非零係数重みの次数を $k_1 < \cdots < k_w$ とする。つまり、

$$c(X) = c_{k_1} X^{k_1} + \cdots + c_{k_w} X^{k_w}$$

である。このとき、$w = 0$ つまり $c(X) = 0$ を示す。BCH 符号の定義 41.3 から $\alpha, \alpha^2, \ldots, \alpha^w$ は生成多項式 $g(X)$ の根である。33.4 から符号語多項式 $c(X)$ は生成多項式 $g(X)$ の倍多項式なので、$g(X)$ の根は $c(X)$ の根でもある。これは、以下の方程式を満たすことを意味する。

$$\begin{aligned} c(\alpha^i) &= c_{k_1} \alpha^{ik_1} + c_{k_2} \alpha^{ik_2} + \cdots + c_{k_w} \alpha^{ik_w} \\ &= 0 \text{ for } i = 1, \ldots, w \end{aligned}$$

これを、行列とベクトルで表すと

$$\begin{bmatrix} \alpha^{1k_1} & \alpha^{1k_2} & \cdots & \alpha^{1k_w} \\ \alpha^{2k_1} & \alpha^{2k_2} & \cdots & \alpha^{2k_w} \\ \vdots & \vdots & & \vdots \\ \alpha^{wk_1} & \alpha^{wk_2} & \cdots & \alpha^{wk_w} \end{bmatrix} \begin{bmatrix} c_{k_1} \\ c_{k_2} \\ \vdots \\ c_{k_w} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}. \qquad (41.8)$$

となる。行列式は転置しても値を変えないこと、ある列または行を定数倍すると行列式もその定数倍になることを使って、

左辺の係数行列の行列式を評価すると以下の通りとなる。

$$\left(\prod_{i=1}^{w}\alpha^{k_i}\right)\det\begin{pmatrix}\alpha^{0\cdot k_1} & \alpha^{0\cdot k_2} & \cdots & \alpha^{0\cdot k_w}\\ \alpha^{1\cdot k_1} & \alpha^{1\cdot k_2} & \cdots & \alpha^{1\cdot k_w}\\ \vdots & \vdots & & \vdots\\ \alpha^{(w-1)\cdot k_1} & \alpha^{(w-1)\cdot k_2} & \cdots & \alpha^{(w-1)\cdot k_w}\end{pmatrix}$$
$$=\left(\prod_{i=1}^{w}\alpha^{k_i}\right)\det(V(\alpha^{k_1},\ldots,\alpha^{k_w})).$$

V はヴァンデルモンド行列 41.1 である。ここで、ヴァンデルモンド行列の性質 41.2 を使うと以下を得る。

$$\det(V)=\prod_{1\le i<j\le w}(\alpha^{k_j}-\alpha^{k_i}) \tag{41.9}$$

α が原始元で、$k_i \neq k_j$ for $i \neq j$ であることから、$\alpha^{k_i} \neq \alpha^{k_j}$ for $i \neq j$ となり、(41.9) は非零となる。したがって、線型方程式 (41.8) の解は $(c_{k_1},\ldots,c_{k_w})=(0,\ldots,0)$ のみとなり、結局 $c(X)=0$ となる。 □

42 BCH 符号と巡回 RS 符号の関係、BCH 符号の復号

本節では、巡回 RS 符号と BCH 符号の関係を明らかにし、RS 符号の復号が BCH 符号の復号に使えることを述べる。

補題 42.1 (巡回 RS 符号の生成多項式)**.** 31.1 で定義した $[n, k]$ 巡回 RS 符号 C は次であった。

$$C = \{\vec{c}(f) \mid f(X) \in \mathbb{F}_q[X; k]\}$$
$$\vec{c}(f) := \big(f(\beta^0), f(\beta^1), \ldots, f(\beta^{n-1})\big)$$

ただし、非ゼロ要素 $\beta \in \mathbb{F}_q$ は n 乗して始めて 1 に等しくなる。

このとき、次が成り立つ。

1. C の生成行列の一つ G は次で与えられる。

$$G = (\beta^{i\times j})_{0\le i\le k-1, 0\le j\le n-1}$$
$$= \begin{bmatrix} \beta^{0\times 0} & \beta^{0\times 1} & \ldots & \beta^{0\times(n-1)} \\ \beta^{1\times 0} & \beta^{1\times 1} & \ldots & \beta^{1\times(n-1)} \\ \vdots & \ddots & \ddots & \vdots \\ \beta^{(k-1)\times 0} & \beta^{(k-1)\times 1} & \ldots & \beta^{(k-1)\times(n-1)} \end{bmatrix}$$

証明. 28.4 の 3 より G は生成行列となる。 □

2. C のパリティ検査行列の一つ H は次で与えられる。

$$H = (\beta^{(i+1)\times j})_{0\le i\le k-1, 0\le j\le n-1}$$
$$= \begin{bmatrix} \beta^{1\times 0} & \beta^{1\times 1} & \ldots & \beta^{1\times(n-1)} \\ \beta^{2\times 0} & \beta^{2\times 1} & \ldots & \beta^{2\times(n-1)} \\ \vdots & \ddots & \ddots & \vdots \\ \beta^{(n-k)\times 0} & \beta^{(n-k)\times 1} & \ldots & \beta^{(n-k)\times(n-1)} \end{bmatrix}$$

証明. H の任意の $(n-k)\times(n-k)$ 部分行列は異なる $n-k$ 個の元で定義されるヴァンデルモンド行列となっているので、フルランクである。7.13 から、$GH^{\mathsf{T}}=0$ を示せば良いことがわかる。GH^{T} の第 (i,j) 成分 $(0\le i\le n-k-1, 0\le j\le n-1)$ は

$$\begin{aligned}\sum_{k=0}^{n-1} G_{i,k}H_{j,k} &= \sum_{k=0}^{n-1}\beta^{ik}\beta^{(j+1)k}\\ &= \sum_{k=0}^{n-1}\beta^{(i+j+1)k}\\ &= \sum_{k=0}^{n-1}(\beta^{i+j+1})^k\\ &\overset{\text{(a)}}{=} \left(1-(\beta^{i+j+1})^n\right)(1-\beta^{i+j+1})^{-1}\\ &\overset{\text{(b)}}{=} 0\end{aligned}$$

となる。ここで (a) では等比数列の和を求める方法[37]を適用した。$1-\beta^{i+j+1}$ の逆元が存在することを確かめないといけないが、$0\le i\le k-1, 0\le j\le n-k-1$ より $1\le i+j+1\le n-1$ となることと、β は n 乗してはじめて 1 になるので、$\beta^{i+j+1}\neq 1$ となることから、確かに逆元が存在する。(b) では、β の位数が n であることを用いた。 □

[37] http://bit.ly/2AYg676

3. C の生成多項式 $g(X)$ は次で与えられる。

$$g(X) = (X - \beta)(X - \beta^2) \cdots (X - \beta^{n-k})$$

証明. 33.4 の 5 から符号語多項式は生成多項式の倍多項式である。$[n, k]$ 巡回符号の生成多項式の次数は $n-k$ であるから、任意の符号語 $c(X)$ が $\beta, \beta^2, \ldots, \beta^{n-k}$ を根に持つことを示せば十分である。$c = (c_0, \ldots, c_{n-1})$ に対して、$Hc^{\mathsf{T}} = 0$ は

$$\sum_{j=0}^{n-1} \underbrace{H_{i,j}}_{=\beta^{(i+1)j}} c_j = 0 \text{ for } i = 0, \ldots, n-k-1$$

と等価でこれを多項式表現すると

$$0 = \sum_{j=0}^{n-1} c_j (\beta^{i+1})^j = c(\beta^{i+1}) \text{ for } i = 0, \ldots, n-k-1$$

$\beta^1, \beta^2, \ldots, \beta^{n-k}$ が $c(X)$ の根となることを意味する。□

定理 42.2 (BCH 符号と巡回 RS 符号の関係)**.** $n := q - 1 := p^m - 1$ とする。$\mathbb{F}_q$ の原始元 α を用いて $\beta := \alpha$ で定義される $\mathbb{F}_q$ 上の $[n, k]$ 巡回 RS 符号

$$C_q = \left\{ \vec{c}(f) \mid f(X) \in \mathbb{F}_q[X; k] \right\}$$
$$\vec{c}(f) := \left(f(\alpha^0), f(\alpha^1), \ldots, f(\alpha^{n-1}) \right)$$

に対して、C_q の符号語のうち全ての成分が $\mathbb{F}_p$ の元である符号語を集めた符号空間

$$C_p := C_q \cap \mathbb{F}_p^n$$

は設計距離 $\hat{d} := n - k + 1$ の $\mathbb{F}_p$ 上の BCH 符号となる。 □

証明. 次の 2 つを示せば十分である。

1. C_p が巡回符号になること
2. C_p の生成多項式 $g_p(X)$ が $\alpha^1, \alpha^2, \ldots, \alpha^{n-k}$ を根に持つ次数が最小のモニック多項式になること

1. $C_p \subset C_q$ である。C_p が $\mathbb{F}_p$ 上の巡回符号になることは、C_q の線形性と巡回性から明らか。
2. 42.1 の 3 で示したことから、C_q の生成多項式は

$$g_q(X) = (X - \alpha)(X - \alpha^2) \cdots (X - \alpha^{n-k}) \qquad (42.3)$$

で与えられる。33.2 より巡回符号 C_p の生成多項式 $g_p(X) \in \mathbb{F}_p[X]$ は、C_p の非零符号多項式 $c_p(X)$ のうち次数が最小のモニック多項式である。$c_p(X) \in C_p$ は C_q の符号語でもある。したがって、33.4 の 5 から $c_p(X)$ は $g_q(X)$ の倍多項式となっているので、(42.3) より $c_p(X)$ は、$\alpha^1, \alpha^2, \ldots, \alpha^{n-k}$ を根にもつ。このような $c_p(X)$ のうち次数最小のモニック多項式が C_p の生成多項式 $g_p(X)$ となる。

定義 41.3 を思い出そう。$\alpha^1, \alpha^2, \ldots, \alpha^{n-k}$ を根にもつ次数最小のモニック多項式によって定義される巡回符号を設計距離 $\hat{d} := n-k+1$ の $\mathbb{F}_p$ 上の BCH 符号と言った。これは C_p が設計距離 $\hat{d} := n-k+1$ の $\mathbb{F}_p$ 上の BCH 符号となることを意味する。 □

議論 42.4. 42.2 より、次の 2 つが言える。

- 42.2 の方法で $[n,k]$ 巡回 RS 符号 C_q から作られた C_p は、符号長 n で設計距離 $\hat{d}$ の BCH 符号であることがわかる。
- 逆に、符号長 n で設計距離 $\hat{d}$ の BCH 符号は、$[n =: p^m - 1 =: q-1, k = n-\hat{d}+1]$ 巡回 RS 符号を C_q として選んで、42.2 の方法で作られる C_p と一致する。

このことから次の 2 つが分かる。

1. BCH 符号 C_p の最小距離は巡回 RS 符号 C_q の最小距離を下回らない。

   $$d(C_p) \geq d(C_q) \overset{28.8}{=} n-k+1 = \hat{d}$$

   これは、BCH 符号の最小距離が $\hat{d}$ 以上となることの別証明を与えている。

2. BCH 符号を RS 符号とみなして、RS 符号の半径 t の限界距離復号を BCH 符号に適用する。これは、BCH 符号に対する半径 t の限界距離復号となっている。

-代数系と符号理論の講義に関する内容はここまで-

参考文献