■1 群（信号・システム）- 2 編（符号理論）

1 章 符号理論の基礎

（執筆者：鎌部　浩）［2013 年 10 月 受領］

■概要■

本章では，符号理論の基礎を述べる．有限体，通信路，誤り訂正の原理などを簡潔に説明する．

Shannon は「A mathematical theory of communication」において，情報源符号化定理と通信路符号化定理の二つの大きな結果を与えた[4]．これらの発見を契機として，情報・通信を数理的に扱う情報理論が誕生し，また，通信路符号化定理がその存在を保証する符号を構成するための理論である符号理論（coding theory）も，一つの学問分野として確立されていった．符号理論はその誕生の経緯から情報理論や確率論，代数学などと強い関係をもっているが，代数幾何学や離散数学，計算量の理論などとも密接な関係をもっていることが明らかになってきている．

本章ではまず，Shannon が与えた情報伝送の数理モデルを示し，符号器と復号器の組の評価尺度について述べる．符号理論では電子回路などによる実装を意識する必要があるため，符号器と復号器の計算量についても述べる．Shannon による伝送路のモデルは非常に一般的なモデルであり，実際には現実の伝送路に応じて様々なモデルがある．それらのいくつかについて述べたあと，通信路符号化定理について説明する．

本編で扱っている符号のほとんど，そして実際に使用されている符号のほとんどは線形符号である．そこで本章の後半では線形符号の基礎について述べる．1-3 節では符号理論の基礎として有限体を説明し，1-4 節で線形符号について概説する．距離の概念を導入することによって，符号の構造を調べたり，その性能を評価できるようになる．1-5 節では符号語間の距離を導入し，最ゆう復号法と限界距離復号などの基本的な復号の説明を与える．1-7 節では線形符号の例としてリード-マラー符号について述べる．これは，初期の頃に発見された符号で簡単な構造をもつ．1-8 節では，符号のトレリスについて概説する．線形符号のトレリス表現を用いると，その符号の構造や様々な復号法との関係が明かになることがある．

【本章の構成】

本章では，誤り訂正の原理（1-1 節），通信路（1-2 節），ガロア体（1-3 節），線形符号（1-4 節），距離・最ゆう復号・限界距離復号（1-5 節），ハミング符号（1-6 節），リード-マラー符号（1-7 節），線形ブロック符号のトレリス（1-8 節）からなる．

■1 群 - 2 編 - 1 章

1-1 誤り訂正の原理

（執筆者：松嶋敏泰）[2013 年 10 月 受領]

1-1-1 符号化・復号システムの概要[1, 2, 3)]

誤り訂正（検出）符号はブロック符号と木符号に大別される．ここではまずブロック符号の符号化と復号のシステムを図を用いて説明する．このシステムの基本的目的は情報源から発生したメッセージを誤りなく受信者に送信することである．情報源から発生するメッセージを集合 $\mathcal{M} = \{1, \ldots, M\}$ の元ととらえ，それぞれのメッセージは情報源アルファベットと呼ばれる有限集合 $\mathcal{U}$ 上の k 次元ベクトルである情報系列 $\boldsymbol{u} = (u_1, \ldots, u_k)$ で表現されるとする．メッセージは符号器により，符号アルファベット C 上の n 次元ベクトルである符号語（符号系列）$\boldsymbol{c} = (c_1, c_2, \ldots, c_n)$ に変換される．この符号語は，通信路を通して受信側へ送られる．受信側では，符号語が通信路において雑音などの影響で変化した受信語（受信系列）を受け取る．受信系列は受信アルファベット $\mathcal{R}$ の n 次元ベクトル $\boldsymbol{r} = (r_1, r_2, \ldots, r_n)$ で表現される．復号器により，受信語 $\boldsymbol{r}$ から元の情報系列 $\boldsymbol{u}$（または符号語 $\boldsymbol{c}$）が推定され受信者に渡される．

通信路については，第 1-2 節で詳しく説明されるが，通信路における符号語の変化は確率的に起こるとして，条件付確率 $P(\boldsymbol{r}|\boldsymbol{c})$ によって通信路のモデルが表現される．符号器による変換は，$\mathcal{U}^k$ から C^n への関数 $\phi(\boldsymbol{u}) = \boldsymbol{c}$ として表され，符号化と呼ばれる．この関数の値域である符号語の集合を符号と呼ぶ．復号器による変換は，$\mathcal{R}^n$ から $\mathcal{U}^k$（または C^n）への関数 $\psi(\boldsymbol{r}) = \hat{\boldsymbol{u}}$（または $\hat{\boldsymbol{c}}$）として表され，復号と呼ばれる．復号は，受信空間 $\mathcal{R}^n$ を各メッセージ $\boldsymbol{u}$ に対応する背反な領域に分割しておき，受信語 $\boldsymbol{r}$ がどの領域に入っているかで，それに対応するメッセージが送られたと判定している過程とみなすこともできる．この各メッセージに対応する領域は復号領域と呼ばれる．

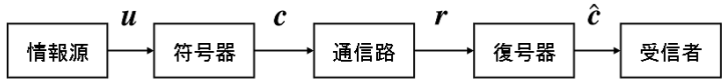

図 1·1　符号化・復号システム

1-1-2 符号化・復号システムの評価

符号化・復号システムの評価は，一般的に次の三つの評価基準で行われる．

1）信頼性（復号誤り率）：

一般的にブロック符号では，復号誤りとして次のブロック誤りとシンボル誤りの 2 種類の誤りを考えることができる．復号によって推定されたメッセージ $\hat{\boldsymbol{u}}$ が送信された真のメッセージ $\boldsymbol{u}$ と一致していない誤りをブロック誤り，復号されたメッセージ（または符号語）の各シンボル $\hat{u}_i$（または $\hat{c}_i$）が送信された対応するシンボル u_i（または c_i）と一致していない誤りをシンボル誤りと呼ぶ．一般的評価基準としては，これらの誤りについて，情報源からメッセージが発生する確率分布 $P(\boldsymbol{u})$ と，通信路の確率分布によって期待値をとった，平均ブ

ロック誤り率と平均シンボル誤り率が用いられる．

例えば，平均ブロック誤り率は以下で表される．

$$\sum_{\mathcal{R}^n}\sum_{\mathcal{U}^k} P(\boldsymbol{r}|\phi(\boldsymbol{u}))P(\boldsymbol{u})L(\psi(\boldsymbol{r}),\boldsymbol{u}),$$

ここで，$L(x,y)$ は $x=y$ のときに 0，それ以外では 1 をとる関数とする．

2）効率性（伝送レート，符号化レート）：

信頼性と共にメッセージを効率よく送ることが通信の目的である．効率の基準として，符号系列の 1 シンボルによって伝送されるメッセージの量を表す伝送レートがある．伝送レートはメッセージの集合の大きさを $M=|\mathcal{U}|^k$ とすると，$R=\log M/n$ で定義される．また，同様に効率を表す量として，符号アルファベットの数で正規化して送られるメッセージの量を表したのが符号化レートで，$R_C=\log_{|C|} M/n$ で定義される．情報源アルファベットと符号アルファベットの大きさが等しい場合，符号化レートは $R_C=k/n$ と簡素に表される．

3）計算量（時間計算量，空間計算量）：

符号化・復号システムの正確性と効率性のほかの評価基準として，その符号器，復号器の計算量は実用化にとって重要な評価基準である．次の小節でこの計算量について説明を行う．

1-1-3 符号化と復号の計算量

復号誤り率を限りなく 0 に近づけるもとで，符号化レートを理論的に最大化するような符号のクラスとして次節で説明するランダム符号がある．この符号の符号化はメッセージに対して対応する符号語の表を用意しなければならず，空間計算量が符号長 n または k の指数オーダとなる．

ブロック誤り率を最小化する復号は，受信語 $\boldsymbol{r}$ を受け取った元でのメッセージ $\boldsymbol{u}$ の事後確率 $P(\boldsymbol{u}\mid\boldsymbol{r})$ を最大にするメッセージを選択することになる．これはメッセージ $\boldsymbol{U}$ の発生確率が一様な場合は，ゆう度 $P(\boldsymbol{r}\mid\boldsymbol{u})$ を最大化するメッセージと一致し，通常これを最ゆう復号と呼んでいる．このようなゆう度最大のメッセージ $\boldsymbol{u}$ を候補のなかから探索する問題は符号長 n または k の指数オーダの計算量が必要とされる．

また，シンボル誤り率を最小化する復号は，周辺事後確率 $P(u_i|\boldsymbol{r})$ を最大化するシンボル u_i を選択することになる．この復号は MPM（Maximum posterior marginal）復号または，MAP（Maximum a posteriori probability）復号* と呼ばれる．周辺事後確率の計算には結合事後確率 $P(\boldsymbol{u}|\boldsymbol{r})$ から周辺確率 $P(u_i|\boldsymbol{r})$ を計算することが必要で，こちらも一般には符号長 n の指数オーダの計算量が必要とされる．

実用的には，多項式オーダ，できれば線形オーダの符号化と復号アルゴリズムが望まれる．符号理論研究の多くは，この計算量制約のもとで，次節で述べる符号化レートの限界を達成する符号と復号法の構成を目指しているといえる．

* 正確にはシンボルに対する最大事後確率復号と呼び，メッセージ（ブロック）に対する最大事後確率復号と区別すべきであろうがここでは慣例に従う．

■1 群 - 2 編 - 1 章

1-2 通信路

（執筆者：松嶋 敏泰）[2013 年 10 月 受領]

1-2-1 入力，出力，通信路モデル

前節の 1-1 節の符号化・復号システムをもう少し細かく見た典型的な通信のシステムを図に示した．前節の図では，通信路への入力は符号系列 $\boldsymbol{c}$ で出力は受信系列 $\boldsymbol{r}$ で，それらのアルファベットは離散集合と仮定していた．この通信路のなかの情報の変換の流れを更に詳しく述べると，まず，符号系列 $\boldsymbol{c}$ は変調によって何らかのアナログ信号系列 $\boldsymbol{x}$ に変換され，アナログ通信路（これも通信路と呼ばれるが，前述の通信路と区別するため，ここではこのように呼ぶ）を経由して，出力系列 $\boldsymbol{y}$ が伝送され，復調器によって受信系列 $\boldsymbol{r}$ に変換される．このアナログ通信路では，入力アルファベット $\mathcal{X}$ と出力アルファベット $\mathcal{Y}$ として連続体の集合が用いられるのが一般的である．どちらの通信路においても，入力と出力の関係は入力系列を条件とした条件付確率 $P(\boldsymbol{r}|\boldsymbol{c})$ や条件付確率密度関数 $p(\boldsymbol{y}|\boldsymbol{x})$ で表される．

また，ここまでは各時点 i ごとにシンボル c_i や信号 x_i が通信路を用いて送信される離散時間通信路を考えていたが，アナログ通信路では連続的に信号波形 $x(t)$ が送信される連続時間通信路の通信路モデルも用いられる．

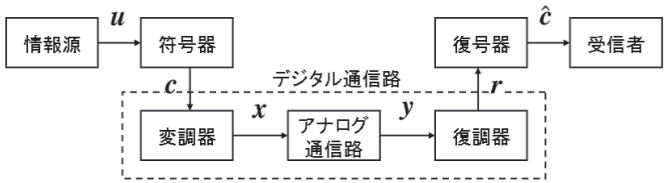

図 1･2　通信路モデル

1-2-2 様々な通信路モデル[4, 7)]

上記のように，符号理論で主に扱う通信路は二つのレベルがあり，それらの通信路モデルは，概ね，入力と出力のアルファベットが離散値の集合のモデルと連続値の集合のモデルとして区別できる．また，時間が離散か連続かによる区別もできるが，ここではまず離散時間通信路モデルで説明をする．

通信路モデルの条件付確率が独立 $P(\boldsymbol{r}|\boldsymbol{c}) = \prod_{i=1}^{n} P_i(r_i|c_i)$ のとき，記憶のない（無記憶）通信路と呼ばれ，独立でない場合は記憶のある通信路と呼ばれる．更に，無記憶で，時点 i により，確率が変わらない場合は定常無記憶通信路と呼ばれる．また，離散確率変数の通信路遷移確率行列 $[P(r|c)]$ の各行がある一つの行の要素の置換で得られ，更に各列もある一つの列の要素の置換で得られるとき，その通信路は対称であるという．

最も簡単で符号理論の様々な評価に用いられる基本的な通信路モデルは，入出力アルファベットが離散値，特に 2 元 $\{0, 1\}$ で，定常無記憶，更に対称性が成り立つ通信路モデルであり，2 元対称通信路（binary symmetric channel）と呼ばれる．つまり，この通信路モデルの

遷移確率は $P_{R|C}(0|0) = 1-p, P_{R|C}(1|0) = p, P_{R|C}(0|1) = p, P_{R|C}(1|1) = 1-p$ で表現され，通信路遷移確率行列の行と列について上記で述べた対称性が成り立っている．

入力アルファベットが出力アルファベットの部分集合になっており，加法 + に対して群をなす場合，符号系列 $\boldsymbol{c}$ に誤り系列 $\boldsymbol{e}$ が加算され受信系列 $\boldsymbol{r} = \boldsymbol{c} + \boldsymbol{e}$ が出力されるような通信路モデルを考えることができる．符号系列と統計的独立な確率分布から誤り系列が発生している場合，このモデルを加法的通信路と呼ぶ．この通信路は対称な通信路であり，先に述べた 2 元対称通信路は，誤り e が $P_E(0) = 1-p, P_E(1) = p$ で発生する加法的離散通信路とみなすこともできる．

記憶のある通信路の基本的な例としては，ギルバート（Gilbert）モデルがある．この通信路モデルは，通信路の誤り率 p が 0 か極めて低い 2 元対称通信路（良い状態）と p が比較的高い 2 元対称通信路（悪い状態）の二つの状態をマルコフ過程で遷移するモデルとなっている．これは，誤り系列を隠れマルコフモデルで表現した通信路モデルということもできる．このモデルは，一度誤りが起こると連続して誤りが発生しやすい（バースト誤り）通信路を表した簡単なモデルとなっている．

次に，入出力アルファベットが実数などの連続値の集合となるアナログ通信路モデルの例を示す．入力系列 $\boldsymbol{x}$ に誤り系列 $\boldsymbol{z}$ が加算され出力系列 $\boldsymbol{y} = \boldsymbol{x} + \boldsymbol{z}$ が得られるような通信路モデルを考えることができ，加法的アナログ通信路と呼ばれる．この誤り系列は雑音系列と呼ばれ，各時点の雑音 z_i が独立で平均が 0 の正規分布に従う場合，加法的白色ガウス雑音通信路（AWGN 通信路）（AWGN channel）と呼ばれ，アナログ通信路の基本的で重要な通信路モデルとなっている．

ここまでは離散時間通信路のモデルの例を挙げたが，信号波形 $x(t)$ を送る連続時間アナログ通信路の例も示しておく．連続時間通信路においても，$y(t) = x(t) + z(t)$ で表現される 加法的通信路モデルが基本モデルとしてよく用いられる．ここでも雑音波形 $z(t)$ に白色ガウス雑音を仮定する場合が重要な通信路モデルとなっている．

1-2-3 通信路符号化定理[4, 5, 6, 7)]

第 1-1 節で，符号化復号システムに対する評価基準を三つ挙げたが，復号誤り率と伝送レートはトレードオフの関係にあることは容易に想像される．復号誤り率を 0 に近づけたもとで，伝送レートをどこまで高められるかの限界を示したものが，以下のシャノン（Shannon）の通信路符号化定理（channel coding theorem）である．

通信路容量（channel capacity）CA をもつ離散無記憶通信路において，伝送レート R が $R < CA$ を満たせば，任意の $\varepsilon > 0$ に対して N_ε が存在して，符号長 $n \geq N_\varepsilon$ のもとで，平均ブロック復号誤り率を ε 以下にする符号が存在する．この通信路容量 CA は遷移確率 $P(r|c)$ の離散無記憶通信路において，以下のように定義される．

$$CA = \max_{P_C(\cdot)} \sum_{c \in C} \sum_{r \in \mathcal{R}} P_{R|C}(r|c) P_C(c) \log \frac{P_{R|C}(r|c)}{P_R(r)}$$

この定理のより精密な表現として，復号誤り率を直接的に伝送レート R と符号長 n の関数で表現した信頼性関数（その上界や下界）がある．上記の定理の証明には，ランダム符号化（random coding）と呼ばれるテクニックが用いられており，ランダムに構成した符号のクラ

ス全体での平均的性質から，上記の性質を満たす符号と復号の存在を証明しているだけで，上記の性能を満たすある一つの符号を構成して証明を行っているわけではない．

また，この通信路符号化定理の逆定理として，同様の通信路において，$R > CA$ の場合，任意の $0 < \varepsilon < 1$ が与えられたもとで，どのような符号を選んでも符号長 n を大きくしていくと復号誤り率は ε 以上となる．更に強い逆符号化定理として，この復号誤り率は n に関して指数関数的に 1 に近づくことが知られている．

これらの定理により伝送レートの限界とその限界を達成する符号の存在は示されたが，その具体的符号の構成法や実用的復号法については，前節の計算量のところで述べられているように，次の課題として残されてしまった．

入力と出力アルファベットが連続値のアナログ通信路の場合も，伝送レートの限界である通信路容量を上記の拡張で考えることができる．この場合も，離散時間通信路と連続時間のモデルを考えることができるが，まず，各時点で信号 x_i を送信する離散時間アナログ通信路から考えていく．

離散アルファベットの場合と違い，信号電力を無尽蔵に使えるのであればいくらでも情報を送ることが可能となってしまうため，平均信号電力の制約 $\sum_{i=1}^{n} x_i \leq P_S$ のもとで通信路容量を考える必要がある．ここでは，重要な通信路である加法的白色ガウス雑音通信路の通信路容量を示す．雑音電力（分散）が P_N の加法的白色ガウス雑音通信路において，平均信号電力を P_S と制限したもとで，通信路容量 $CA = 1/2 \log(1 + P_S/P_N)$ となることが知られている．

次に，信号波形 $x(t)$ を送る連続時間アナログ通信路の通信路容量についても示しておく．この通信路においては，信号電力制限の上に更に帯域制限も考えることになる．具体的には，周波数 W より大きい周波数をカットする理想帯域通過フィルタのインパルス応答 $h(t)$ を用い，受信波形が $y(t) = (x(t) + z(t)) * h(t)$ で表されるような通信路モデルを考える．この帯域制限と単位時間当たりの信号電力を P_S と制限したもとで，雑音波形 $z(t)$ の単位時間当たりの電力が P_N である加法的白色ガウス通信路において，通信容量 $CA = W \log(1 + P_S/P_N)$ となる．この信号電力と雑音電力の比 P_S/P_N は信号対雑音比（S/N 比）と呼ばれ，通信路の特性を表す代表的な指標となっている．伝送ビットと帯域幅で正規化するという意味から，S/N 比をビット当たりの信号電力 E_b と雑音の電力スペクトル密度 N_0 の比 E_b/N_0 で表す場合も多い．$-W$ から W までに帯域制限された白色ガウス雑音の場合，電力スペクトル密度は平坦であり，その密度を $N_0/2$ とすると $P_N = N_0 W$ となる．

■1 群 - 2 編 - 1 章

1-3 ガロア体

（執筆者：松嶋敏泰）[2013 年 10 月 受領]

1-3-1 有限体[8)]

集合 A 上に定義された 2 項演算 $\circ$ が次の (1) を満たすとき半群，(1)(2)(3) を満たすとき群（group）更に (4) も満たすとき可換群またはアーベル群と呼ぶ．

(1) 結合律： $\forall x, y, z \in A\ (x \circ y) \circ z = x \circ (y \circ z)$.

(2) $\exists e \in A \forall x \in A\ x \circ e = e \circ x = x$，この元を単位元と呼ぶ．

(3) $\forall x \in A \exists x' \in A\ x' \circ x = x \circ x' = e$，この元を x の逆元と呼ぶ．

(4) 可換律： $\forall x, y \in A\ x \circ y = y \circ x$.

集合 A 上の 2 種類の 2 項演算，加法 $+$ と乗法 $\cdot$ で定義された代数系で，以下の (5)(6)(7) の三つの条件を満たすものを環（ring）と呼ぶ．更に，(8) のすべての条件をみたすものを体（field）と呼ぶ．

(5) 加法に関してアーベル群となる．

(6) 乗法に関して半群となる．

(7) 分配律： $\forall x, y, z \in A\ x(y + z) = xy + xz,\ (x + y)z = xz + yz$.

(8) 乗法に関して可換で，単位元 1 があり，零元（加法に関する単位元）0 以外のすべて元に関する逆元が存在する．

整数全体の集合に通常の加法と乗算を定義した代数系は環であり，整数環と呼ばれる．有理数全体，実数全体，複素数全体の集合上に，通常の加法，乗法を定義した代数系は体となることが分かる．これらの環や体は無限集合上に定義され，無限環や無限体となるが，有限集合上に定義される有限環と有限体が符号理論では重要な役割を担う．

可換環 R の部分集合 I が次の (9)(10) の条件を満たすとき，I は R のイデアル（ideal）であるという．

(9) I は加法に関し，R の部分群となる．

(10) $\forall x \in I\ \forall y \in R\ xy \in I$.

可換環 R の元 x, y に対し，$x + i = y$ となる元 i が R のイデアル I に含まれるとき，x と y はイデアル I を法として合同であるという．この同値関係により，加法及び乗法が $[x] + [y] = [x + y]$，$[x][y] = [xy]$ で定義される代数系（商代数系と呼ばれる）が導かれる．ここで $[x]$ は R の元 x を含む剰余類（同値類）で，$[x] = \{x + i | i \in I\}$ で表現される集合である．さて，このような商代数系は環となることが簡単に証明でき，この環を I を法とする R

の商環または剰余環と呼び，R/I で表す．例えば，整数環 $\mathbf{Z}$ の p を生成元とするイデアル $I_p = \{pi | i \in \mathbf{Z}\}$ を考える．I_p を法とする商環 $\mathbf{Z}/I_p$ の元は $[0], [1], \cdots, [p-1]$ で表され，加算と乗算は以下のようには行えばよい．$[x] + [y] = [(x+y) \bmod p]$，$[x][y] = [xy \bmod p]$，ここに，$x \bmod p$ は x を p で割った余りを表すものとする．

上記の剰余環は有限環となるが，p が素数の場合は有限体（finite field）となる．有限代数系を定義する集合 A の元の数を位数と呼び，位数が p の有限体を F_p で表す．特に，位数 p が素数の有限体は素体（prime field）と呼ばれる．

1-3-2 多項式環と拡大体

$f_0, f_1, \cdots, f_n$ を体 F の元とするとき，$f(X) = f_0 + f_1 X + \cdots + f_n X^n$ を体 F 上の多項式と呼ぶ．f_i $(i = 0, 1, \cdots, n)$ は i 次の係数と呼ばれる．また，非零の最高次の係数が f_j であれば，j を $f(X)$ の次数といい，$\deg f(X)$ で表す．この定義によれば，体 F の非零の元は 0 次の多項式となり，零元 0 を含め定数と呼ぶ．また，最高次の係数が 1 である多項式をモニック多項式という．

体 F 上の多項式は，体 F の加法と乗法を用い，多項式どうしの加法，乗法が定義でき，その代数系は環となる．この環を多項式環と呼び，$F[X]$ で表す．体 F 上の任意の多項式 $f(X)$ を非零の多項式 $g(X)$ で割ったとき，$f(X) = g(X)q(X) + r(X)$, $\deg r(X) < \deg g(X)$ を満たす商多項式 $q(X)$ と剰余多項式 $r(X)$ が一意に定まる．多項式 $f(X)$ と $g(X)$ の最大公約数が 1 のとき，$f(X)$ と $g(X)$ は互いに素であるという．また体 F 上の多項式 $f(X)$ が，次数 1 以上 $n-1$ 以下のいかなる F 上の多項式によっても割り切れないとき，$f(X)$ を既約多項式と呼ぶ．多項式環の既約多項式は，整数環の素数と同じ役割を演じる．例えば，整数の素因数分解と同様，F 上の任意の多項式は F 上の有限個の既約多項式の積として一意に表せる．

さて，整数の商環 Z/I_p は p が素数のとき有限体となった．これと同様に，生成多項式 $p(X)$ で生成されるイデアル $I_{p(X)}$ を法とする商環 $F[X]/I_{p(X)}$ は $p(X)$ が既約多項式のとき，F が有限体であれば有限体となる．多項式を定義した体が有限体 F_p で，既約多項式 $p(X)$ の次数が n のとき，この有限体 $F[X]/I_{p(X)}$ の位数は p^n となり，F_{p^n} と表される．このような体を F_p の n 次拡大体（extension field）と呼ぶ．このようにしてつくられた有限体 F_{p^n} はガロア（Galois）体と呼ばれ GF(p^n) と書かれることもある．すべての有限体は，ガロア体と同型であることが知られている．

1-3-3 多項式の根と原始元

体 F 上の多項式 $f(X) = f_0 + f_1 X + \cdots + f_n X^n$ が，元 α に対し $f(\alpha) = f_0 + f_1 \alpha + \cdots + f_n \alpha^n = 0$ を満たすなら，α を $f(X)$ の根という．ある正整数 n に対し $\alpha^n = 1$ となるが，$l < n$ となる正整数 l に対し，$\alpha^l \neq 1$ であるとき，元 α を 1 の原始 n 乗根といい，n を元 α の位数という．GF(p^n) の元で位数が $p^n - 1$ の元を原始元といい，原始元を根としてもつ n 次の GF(p) 上の既約多項式を原始多項式（primitive polynomial）と呼ぶ．

また，GF(p) の拡大体 GF(p^n) の非零の元 α が GF(p) 上の多項式 $f(X)$ の根となるとき，$\alpha^p, \alpha^{p^2}, \cdots, \alpha^{p^{d-1}}$ も $f(X)$ の根となる．ただし，d は $\alpha^{p^d} = \alpha$ となる最小の整数とする．このような根 $\alpha^p, \alpha^{p^2}, \cdots, \alpha^{p^{d-1}}$ を元 α の共役元（conjugate）と呼ぶ．

■1 群 - 2 編 - 1 章

1-4 線形符号

（執筆者：鴻巣敏之）[2013 年 10 月 受領]

GF(q) 上の n 次元ベクトル空間 $\{0,1,\ldots,q-1\}^n$ の部分空間を GF(q) 上の線形符号（linear code）という．線形符号 C では，任意の符号語 $\boldsymbol{c}_i$ と $\boldsymbol{c}_j$ に対し，

$$u_i\boldsymbol{c}_i + u_j\boldsymbol{c}_j,\ u_i, u_j \in \mathrm{GF}(q) \tag{1·1}$$

も C の符号語となる．また線形符号は，全零符号語 $\mathbf{0}$ を必ず含み，最小（ハミング）距離（minimum Hamming distance）$d_{\min}$ と非零の符号語の最小（ハミング）重みが等しい．

GF(q) 上の線形符号 C の符号語 $\boldsymbol{c}$ は，一次独立な k 個の符号語 $\boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_k$ の一次結合

$$\boldsymbol{c} \quad = \quad u_1\boldsymbol{c}_1 + u_2\boldsymbol{c}_2 + \cdots + u_k\boldsymbol{c}_k,\ u_i \in \mathrm{GF}(q),\ i = 1,2,\ldots,k \tag{1·2}$$

で表すことができる．$\{\boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_k\}$ を線形符号 C の基底（basis）という．また k は線形符号 C の次元（dimension）といい，これを $\dim(C)$ で表す．

符号長 n，次元 k，最小（ハミング）距離 $d_{\min}$ の符号を $(n,k,d_{\min})$ 符号と表記する．最小（ハミング）距離 $d_{\min}$ を特定しないときは，その項は省かれる．

線形符号の生成行列（generator matrix）G は，基底を用い，

$$G \quad = \quad \begin{bmatrix} \boldsymbol{c}_1 \\ \boldsymbol{c}_2 \\ \vdots \\ \boldsymbol{c}_k \end{bmatrix} \tag{1·3}$$

で定義される．G は，$k \times n$ 行列であり，その階数は k である．メッセージを $\boldsymbol{u}$ とするとき，その長さは k であり，この k を情報記号数ともいう．メッセージ $\boldsymbol{u}$ に対する線形符号の符号語 $\boldsymbol{c}$ は，生成行列から

$$\boldsymbol{c} \quad = \quad \boldsymbol{u}G \tag{1·4}$$

により符号化される．

GF(q) 上の C の任意の符号語 $\boldsymbol{c}$ に対して，

$$\boldsymbol{c}H^T \quad = \quad \mathbf{0} \tag{1·5}$$

を満足する GF(q) 上の階数 $n-k$ の $(n-k)\times n$ 行列をパリティ検査行列（parity check matrix），もしくは単に検査行列という．T は，転置を表す．広義には，式 (1·5) を満たす 階数 $n-k$ の $n-k$ 以上の行をもつ行列をパリティ検査行列という．

式 (1·4) と式 (1·5) から

$$\boldsymbol{u}GH^T \quad = \quad \mathbf{0} \tag{1·6}$$

が，任意のメッセージ $\boldsymbol{u}$ で成立することから，生成行列 G とパリティ検査行列 H には

$$GH^T \quad = \quad \mathbf{0} \tag{1・7}$$

が成り立つ．したがって，線形符号を具体的に定義することは，生成行列 G を定義するか，もしくはパリティ検査行列 H を定義することといえる．例えばハミング符号は，パリティ検査行列 H を定義している．

GF(q) 上の (n,k) 線形符号 C の $(n-k)\times n$ 行列であるパリティ検査行列 H を生成行列とする $(n,n-k)$ 線形符号 $C^\perp$ を C の双対符号（dual code）という．このとき，$C^\perp$ の $k\times n$ 行列であるパリティ検査行列 $H^\perp$ は，C の生成行列である．$C^\perp$ は C の直交補空間であり，

$$\dim(C) + \dim(C^\perp) \quad = \quad n \tag{1・8}$$

が成り立つ．$C^\perp$ の任意の符号語 $\boldsymbol{c}^\perp$ と C の任意の符号語 $\boldsymbol{c}$ は直交する．

GF(q) 上の線形符号 C_0 の生成行列 G_0 が $k\times k$ 単位行列 I_k をもつとき，符号語では k 個の情報記号と 符号化により付加された $n-k$ 個の検査記号が，明確に区別できる．このような符号を組織符号（systematic code）といい，組織符号でない符号を非組織符号（nonsystematic code）という．組織符号は，情報記号と検査記号が区別できるので分かりやすいが，実用で用いられる符号は非組織符号である方が復号が容易であることが多い．組織符号 C_0 の生成行列 G_0 が，

$$G_0 \quad = \quad [I_k \; P] \tag{1・9}$$

であるとき，そのパリティ検査行列 H_0 は，

$$H_0 \quad = \quad [-P^T \; I_{n-k}] \tag{1・10}$$

となる．ここで P は，$k\times(n-k)$ 行列である．

任意の線形符号 C の生成行列 G は，基本行操作と列置換を用いることにより，組織符号 C_0 の生成行列 G_0 に変換できる．基本行操作のみで組織符号の生成行列となる場合は，情報記号と符号語の対応が異なるが同じ符号となる．すなわち，符号語の集合が全く等しい．列置換までを行って組織符号の生成行列となる場合は，もとの符号の符号語の記号位置が置換されたものが，得られた組織符号の符号語となっている．このような関係の符号を等価（equivalent）な符号という．すなわち，生成行列が基本行操作と列置換のもとで同一であるとき，それらの符号を等価という．等価な符号において，最小距離，重み分布（weight distribution）などの特性は等しい．

受信語 $\boldsymbol{r}$ に対して

$$\boldsymbol{s} \quad = \quad \boldsymbol{r}H^T \tag{1・11}$$

をシンドローム（syndrome）という．誤りベクトル $\boldsymbol{e}$ を用いて，受信語は $\boldsymbol{r} = \boldsymbol{c} + \boldsymbol{e}$ とかけるので，

$$\begin{aligned} \boldsymbol{s} \quad &= \quad \boldsymbol{c}H^T + \boldsymbol{e}H^T \\ &= \quad \boldsymbol{e}H^T \end{aligned} \tag{1・12}$$

である．したがってシンドロームは，送信符号語によらず，誤りベクトル $\boldsymbol{e}$ の誤り位置に対応するパリティ検査行列 H の列位置の一次結合になっている．シンドロームは，代数的復号法における誤り訂正アルゴリズムで重要な役割をはたす．

線形符号の非零符号語に対して，パリティ検査行列の d 列の一次結合が $\mathbf{0}^T$ となるものが存在し，d 以下の列のすべての一次結合が $\mathbf{0}^T$ にならなければ，重み d の符号語が最小重みの非零符号語となる．また，線形符号の最小距離と非零符号語の最小重みが等しいことから，線形符号の最小距離 $d_{\min}$ に関して次の重要な性質が成り立つ．すなわち GF(q) 上の線形符号 C において，パリティ検査行列 H のすべての組合せの $d_{\min}-1$ 列が GF(q) で一次独立であり，$d_{\min}$ 列で一次従属な組合せがあるとき，C の最小距離は $d_{\min}$ である．

更に，GF(q) 上の (n,k) 線形符号 C のパリティ検査行列 H の階数は $n-k$ であるから，GF(q) 上で H の $n-k+1$ 列は常に一次従属となる．したがって，(n,k) 線形符号 C の最小距離 $d_{\min}$ に対して，

$$d_{\min} \quad \leq \quad n-k+1 \tag{1・13}$$

が成り立つ．これをシングルトン限界（Singleton bound）という．シングルトン限界は，組織符号において k 個の情報シンボルのなかで 1 個が非零の情報シンボルとき，符号語の重みを最大にする条件が $n-k$ 個の検査シンボルを非零とすることからも導くことができる．シングルトン限界を等号で満足する線形符号を最大距離分離符号（maximun distance separable code: MDS code）という．2 元の最大距離分離符号は，$(n,1,n)$ 反復符号と $(n,n-1,2)$ パリティ検査符号しか存在しないが，$q(q\neq 2)$ 元符号ではリード-ソロモン（Reed-Solomon: RS）符号を代表とした最大距離分離符号が存在する．

■1 群 - 2 編 - 1 章

1-5 距離・最ゆう復号・限界距離復号

（執筆者：鴻巣敏之）[2013 年 10 月 受領]

符号を幾何学的に扱い，距離を導入することにより，符号の構造を調べたり，誤り訂正能力を評価することができる．

距離の定義はいくつかあるが，符号理論でよく用いられる距離はハミング距離（Hamming distance）である．二つの n 次元ベクトル $\boldsymbol{u}, \boldsymbol{v}$ のハミング距離 $d_{\mathrm{H}}(\boldsymbol{u}, \boldsymbol{v})$ は，

$$d_{\mathrm{H}}(\boldsymbol{u}, \boldsymbol{v}) \quad = \quad \sum_{i=1}^{n} d_{\mathrm{H}}(u_i, v_i) \tag{1・14}$$

で定義される．ただし，

$$d_{\mathrm{H}}(u, v) \quad = \quad \begin{cases} 0, & u = v \\ 1, & u \neq v \end{cases} \tag{1・15}$$

である．ハミング距離は，二つのベクトルの対応する位置の成分対を比較したとき，異なる成分対の数となる．また，長さ n のベクトル $\boldsymbol{u}$ のハミング重み $w_{\mathrm{H}}(\boldsymbol{u})$ は，$\boldsymbol{u}$ の非零の成分の数で定義される．したがって，

$$w_{\mathrm{H}}(\boldsymbol{u}) \quad = \quad d_{\mathrm{H}}(\boldsymbol{u}, \boldsymbol{0}) \tag{1・16}$$

が成り立つ．ハミング距離は，離散通信路における誤りの数に対応させることができるため有用であり，符号理論において広く用いられている．

成分が実数，もしくは複素数の長さ n の二つのベクトル $\boldsymbol{u}, \boldsymbol{v}$ のユークリッド距離（Euclidean distance）$d_{\mathrm{E}}(\boldsymbol{u}, \boldsymbol{v})$ は，

$$d_{\mathrm{E}}(\boldsymbol{u}, \boldsymbol{v}) \quad = \quad \Big(\sum_{i=1}^{n} |u_i - v_i|^2\Big)^{1/2} \tag{1・17}$$

で定義される．ユークリッド距離は，加法的白色ガウス通信路などのアナログ通信路での符号の能力を評価するのに有用である．

次に符号の復号について考える．符号 C の M 個の符号語のうち $\boldsymbol{c}_m$ が送信され，受信語 $\boldsymbol{r}$ に対し復号器が符号語 $\boldsymbol{c}_{\hat{m}}$ を送信符号語と推定したとする．受信語 $\boldsymbol{r}$ に対して，すべての符号語 $\boldsymbol{c}_i$, $\imath = 1, 2, \ldots, M$ についての事後確率 $P(\boldsymbol{c}_i|\boldsymbol{r})$ を求め，それを最大とする符号語，すなわち

$$\hat{m} \quad = \quad \arg\max_{i} P(\boldsymbol{c}_i|\boldsymbol{r}) \tag{1・18}$$

とする符号語 $\boldsymbol{c}_{\hat{m}}$ を送信符号語と推定する復号法を最大事後確率復号法（maximum a posterior probability decoding: MAP decoding）という．最大事後確率復号法は，復号誤り確率を最小とする復号法である．

通常，符号語 $\boldsymbol{c}_i$ は等確率で生起すると仮定して問題ない．このとき，事後確率 $P(\boldsymbol{c}_i|\boldsymbol{r})$ を

最大にする符号語を求めることは，ベイズ規則よりゆう度 $P(\boldsymbol{r}|\boldsymbol{c}_i)$ を最大にする符号語，すなわち

$$\hat{m} \quad = \quad \arg\max_i P(\boldsymbol{r}|\boldsymbol{c}_i) \tag{1･19}$$

とする符号語 $\boldsymbol{c}_{\hat{m}}$ を送信符号語とすることと等価となる．これを最ゆう復号法（maximum likelihood decoding: MLD）という．最ゆう復号法は，符号語の生起確率が等確率のとき復号誤り確率を最小とする復号法であるといえる．

以上のような復号法に対し，符号の符号語と受信語の距離を利用する復号法を考えることができる．

受信語 $\boldsymbol{r}$ が受信されたとき，$\boldsymbol{r}$ から最小の距離に位置する符号語を送信符号語 $\hat{\boldsymbol{c}}_m$ と推定する復号法を最小距離復号法（mimimum distance decoding: MDD）という．2 元対称通信路を仮定すると，最ゆう復号法は最小距離復号法と等価である．

符号の最小（ハミング）距離 $d_{\min}$ に対して，

$$d_{\min} \quad \geq \quad 2t+1 \tag{1･20}$$

を満足する t を定め，受信語 $\boldsymbol{r}$ が受信されたとき，

$$d_{\mathrm{H}}(\boldsymbol{c}_i, \boldsymbol{r}) \quad \leq \quad t \tag{1･21}$$

なる符号語を送信符号語 $\hat{\boldsymbol{c}}_m$ と推定する復号法を限界距離復号法（bounded distance decoding）という．この復号法では，t 個以下の誤りをすべて訂正する．また，$t_{\max} = \lfloor (d_{\min}-1)/2 \rfloor$ 個までの誤りに対しては復号領域の重なりがないため，すべて正しく訂正することが可能となる．したがって，この $t_{\max}$ を符号の誤り訂正能力と呼ぶことがある．実際には限界距離復号法は，代数的符号の設計最小距離に基づき，符号の代数的構造を利用した代数的復号法により行われる．設計最小距離 d_δ は，$d_\delta \leq d_{\min}$ であり，設計最小距離を最小距離とみなし，復号の計算量が実用的な代数的復号法が行われる．

最ゆう復号法や最小距離復号法は，受信語とすべての符号語に対して，ゆう度やハミング距離の比較を行わなければならない．よって，符号長 n の指数オーダの演算回数，例えば 2 元符号については $O(2^{nR})$ を必要とし，n が大きいときにはこれらの復号法は実用的ではない．ここで，R は符号化比率である．しかしながら，代数的な演算を行う代数的復号法は，n の多項式オーダの演算回数，例えば 2 元 BCH 符号においては $O(n\log_2^2 n)$ で実行する復号アルゴリズムが存在する．バーレカンプ-マッシーアルゴリズム，ユークリッド復号アルゴリズムなどはその例であり，広く実用に供されている．ただし，畳込み符号のように最ゆう復号を少ない計算量で実行する復号アルゴリズムも存在する．

■1 群 - 2 編 - 1 章

1-6 ハミング符号

（執筆者：高田豊雄）[2013 年 10 月 受領]

ハミング符号（Hamming code）とは，線形ブロック符号における最も基本的かつ重要な符号のクラスの一つであり，1950 年に Richard W. Hamming によって発見された[9]．ここでは，はじめに 2 元ハミング符号について述べる．

1-6-1 ハミング符号の基本パラメータ

m を 3 以上の正整数とする．2 元ハミング符号の基本パラメータは以下のとおりである．

符号長　　$n = 2^m - 1$

情報ビット数　$k = 2^m - m - 1$

冗長ビット数　$r = m$

最小距離　　$d = 3$

ハミング符号の検査行列 H は長さ m のすべての非零の 2 元（列）ベクトルの集合から構成される．例えば $m = 3$ の場合は以下の式となる．

$$H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \tag{1･22}$$

検査行列 H の異なる任意の二つの列ベクトルが一致しないことから，ハミング符号の最小（ハミング）距離は $d \geq 3$ であること，また，H の任意の二つの列ベクトル $\boldsymbol{h}_1^T, \boldsymbol{h}_2^T$ について，和 $\boldsymbol{h}_1^T + \boldsymbol{h}_2^T$ と一致する別の列ベクトルが H に必ず存在することから，$d \leq 3$ であることがいえるため，最小距離 $d = 3$ であることが分かる．

符号ビット位置の適切な置換を考えれば，ハミング符号は一意であることが, 上の構成法から明らかである．すなわち，任意の 2 元 $(2^m - 1, 2^m - m - 1, 3)$ 線形ブロック符号は等価（1-4 節）である．（注: $m = 2$ のとき， 2 元 $(3, 1, 3)$ 線形ブロック符号が構成可能だが，この符号は通常，繰り返し符号（repetition code）と呼ばれる．）

1-6-2 誤り訂正能力，復号法

1-6-1 項の検査行列 H の構成法から，受信語中の任意の 1 ビットの誤りに対して，それぞれシンドロームが異なることとなる．そこで，シンドロームと一致する列ベクトルを H 中から見いだせば，そのときの列インデクスが，誤り位置となる．このようにして，ハミング符号は任意の 1 ビットの誤りを正しく訂正することが可能である．

1-6-3 ハミング符号と完全符号

さて，ハミング符号は単一の誤りを訂正可能であることが分かった．ここで，ある符号語を中心とする半径 1 の超球内のベクトルの個数は $1 + n = 2^m$ 個であり，符号語の総数は $2^k = 2^{2^m - m - 1}$ 個であることと，全符号語の半径 1 の超球はお互いに重ならないことから，ベクトルの総数は $2^m \cdot 2^{2^m - m - 1} = 2^n$ となり，長さ n の全ベクトルは，いずれかの超球に属して

いることが分かる．一般に長さ n の全ベクトルがある符号のいずれかの符号語を中心とする半径 $\lfloor \frac{d-1}{2} \rfloor$ の超球内に属するとき，その符号を完全符号（perfect code）という．実際，ハミング限界の式（3-1 節）に，1-6-1 項に述べた基本パラメータを代入すると，等号が成立する．すなわち，ハミング符号は完全符号である．

ハミング符号を除く唯一の非自明な 2 元完全符号として，あるいは，その様々な数学的な性質，また実用上の観点から重要な符号としてゴーレイ符号（Golay code）が知られている[10]．

1-6-4 シンプレックス符号

ハミング符号の双対符号（1-4 節）はシンプレックス符号（simplex code）と呼ばれる．シンプレックス符号のパラメータは $(2^m - 1, m, 2^{m-1})$ となる．実際，シンプレックス符号の符号語は重み 0 の符号語が 1 個，残り $2^m - 1$ 個の符号語の重みは 2^{m-1} となり，それらの符号語はシンプレックス（幾何図形（多様体）の一種）を構成する．

1-6-5 巡回ハミング符号

1-6-1 項で述べたとおり，パラメータが $(2^m - 1, 2^m - m - 1, 3)$ である 2 元線形ブロック符号はすべて等価な符号であるが，そのなかには巡回符号（巡回ハミング符号）が存在する（2-1 節）．例えば，$m = 3$ のとき，α をガロア体 GF(2^3) の原始元，ただし，$\alpha^3 + \alpha + 1 = 0$ とすると，

$$
\begin{aligned}
H &= (1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6) \\
H &= \begin{pmatrix} 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}
\end{aligned} \qquad (1\cdot23)
$$

となり，巡回ハミング符号の検査行列が得られる．詳細は巡回 BCH 符号の項（2-2 節）を参照のこと．

1-6-6 非 2 元のハミング符号

2 元の場合と全く同様の構成法でガロア体 GF(q) 上の q 元ハミング符号が構成可能である．例えば，$q = 3, m = 3$ の 3 元ハミング符号の検査行列は以下のようになる．

$$
H = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 1 & 2 & 1 & 2 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 2 & 2 \\ 1 & 0 & 0 & 1 & 2 & 1 & 1 & 0 & 0 & 1 & 2 & 1 & 2 \end{pmatrix} \qquad (1\cdot24)
$$

GF(q) 上の q 元ハミング符号は，符号長 $n = (q^r - 1)/(q - 1)$，情報記号号数 $n - r$，最小距離 3 の単一誤り訂正可能完全符号である．

■1 群 - 2 編 - 1 章

1-7 リード-マラー符号

（執筆者：高田豊雄）[2013 年 10 月 受領]

リード-マラー符号（Reed-Muller code）符号の性能（3-1 節）としては必ずしも最適ではないが，構造的な性質の面から，あるいは，比較的効率のよい硬判定復号法，軟判定復号法（2-6 節）をもつことによる実用的な面から重要な符号のクラスである．1954 年に Muller によって発見され[11]，同年 Reed によって最初の復号アルゴリズム（多数決論理復号法）[12]が提案された．

1-7-1 基本パラメータ

m を任意の非負整数とし，r を m 以下の非負整数とする．そのとき，r 次の 2 元リード-マラー符号 RM(r, m) の基本パラメータは以下のとおりである．

符号長　　$n = 2^m$

情報ビット数　　$k = 1 + \begin{pmatrix} m \\ 1 \end{pmatrix} + \begin{pmatrix} m \\ 2 \end{pmatrix} + \cdots + \begin{pmatrix} m \\ r \end{pmatrix}$

最小距離　　$d = 2^{m-r}$

リード-マラー符号 RM(r, m) の生成行列の構成法は次のとおりである．j を $0 \le j \le 2^m - 1$ の非負整数とし，j の 2 進展開を $(v_{1,j},\ v_{2,j},\ \ldots,\ v_{m,j})$（ただし，$v_{1,j}$ を最下位ビット）とする．長さ 2^m の 2 元ベクトル $\boldsymbol{v}_i$,（ただし，$1 \le i \le m$）を，以下のとおり定義する．

$$\boldsymbol{v}_i \triangleq (v_{i,0},\ v_{i,1},\ \ldots,\ v_{i,2^m-1})$$

また，2 元ベクトル $\boldsymbol{u} = (u_0, u_1, \ldots, u_{2^m-1})$, $\boldsymbol{v} = (v_0, v_1, \ldots, v_{2^m-1})$ の（成分ごとの）論理積 $\boldsymbol{u} \cdot \boldsymbol{v}$ を以下のとおり定義する．

$$\boldsymbol{u} \cdot \boldsymbol{v} \triangleq (u_0 \cdot v_0,\ u_1 \cdot v_1,\ \ldots,\ u_{2^m-1} \cdot v_{2^m-1})$$

ただし 右辺の $\cdot$ は論理積を表す．また，$\mathbf{1}$ を成分がすべて 1 の長さ 2^m の 2 元ベクトルとする．

異なる r 個の $\boldsymbol{v}_i$ の論理積のベクトルを r 次のベクトルという（$\mathbf{1}$ を 0 次のベクトルという）．このとき，r 次のリード-マラー符号 RM(r, m) は r 次以下のベクトルで生成される符号である．すなわち，RM(r, m) の生成行列 $G_{\mathrm{RM}(r,m)}$ は

$$G_{\mathrm{RM}(r,m)} = (\mathbf{1}, \boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_m, \boldsymbol{v}_1 \cdot \boldsymbol{v}_2, \boldsymbol{v}_1 \cdot \boldsymbol{v}_3, \ldots, \boldsymbol{v}_{m-1} \cdot \boldsymbol{v}_m, \ldots,)^T \tag{1·25}$$

である．

1-7-2 クロネッカー積によるリード-マラー符号の構成法

$m \times m$ の 2 元行列　$A = [a_{ij}]$ と $n \times n$ の 2 元行列 B について A と B のクロネッカー積 $A \otimes B$ は 行列 A の各成分 a_{ij} を $n \times n$ 行列 $a_{ij}B$ に置き換えることによって得られる $mn \times mn$ 行列である．行列 $G_{(2,2)}$ を $G_{(2,2)} \triangleq \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ と定義する．$i\ (\ge 2)$ に対して $G_{(2^i,\ 2^i)}$ を以下の

ように定義する．

$$G_{(2^i,\ 2^i)} \triangleq (G_{(2,2)} \otimes (G_{(2,2)} \otimes (\cdots (G_{(2,2)} \otimes \underbrace{G_{(2,2)}))\cdots)}_{i-1\ 重}$$

そのとき，リード-マラー符号 RM(r,m) の生成行列 $G_{\mathrm{RM}(r,m)}$ は $G_{(2,2)}$ の m 重クロネッカー積 $G_{(2^m,2^m)}$ の重み 2^{m-r} 以上のすべての行ベクトルから構成された行列である．

1-7-3 $|\boldsymbol{u}|\boldsymbol{u}+\boldsymbol{v}|$ 構成法によるリード-マラー符号の構成法

長さ n の 2 元ベクトル $\boldsymbol{u}=(u_0,u_1,\ldots,u_{n-1})$, $\boldsymbol{v}=(v_0,v_1,\ldots,v_{n-1})$ が与えられたとき，長さ $2n$ の 2 元ベクトル $|\boldsymbol{u}|\boldsymbol{u}+\boldsymbol{v}|$ を以下のとおり定義する．

$$|\boldsymbol{u}|\boldsymbol{u}+\boldsymbol{v}| \triangleq (u_0,u_1,\ldots u_{n-1},\ u_0+v_0,\ u_1+v_1,\ \ldots,\ u_{n-1}+v_{n-1})$$

C_1，C_2 をそれぞれ 2 元 (n,k_1)，(n,k_2) 線形符号とするとき，

$$\{|\boldsymbol{u}|\boldsymbol{u}+\boldsymbol{v}| : \boldsymbol{u}\in C_1,\ \text{かつ}\ \boldsymbol{v}\in C_2\}$$

により，2 元 $(2n,k_1+k_2)$ 線形符号を構成することができる．この符号構成法は $|\boldsymbol{u}|\boldsymbol{u}+\boldsymbol{v}|$ 構成法と呼ばれる．

符号長 2^m の r 次のリード-マラー符号 RM(r,m) は，符号長 2^{m-1} のリード-マラー符号から $|\boldsymbol{u}|\boldsymbol{u}+\boldsymbol{v}|$ 構成法により次のように構成される．

$$\mathrm{RM}(r,m)=\{|\boldsymbol{u}|\boldsymbol{u}+\boldsymbol{v}| : \boldsymbol{u}\in \mathrm{RM}(r,m-1),\ \text{かつ}\ \boldsymbol{v}\in \mathrm{RM}(r-1,m-1)\} \tag{1・26}$$

RM(r,m) の生成行列 $G_{\mathrm{RM}(r,m)}$ は以下のとおりとなる．

$$G_{\mathrm{RM}}(r,m)=\begin{pmatrix} G_{\mathrm{RM}(r,m-1)} & G_{\mathrm{RM}(r,m-1)} \\ \mathbf{0} & G_{\mathrm{RM}(r-1,m-1)} \end{pmatrix} \tag{1・27}$$

1-7-4 リード-マラー符号のその他の性質

- リード-マラー符号は，符号長が同じで，より次数の高いリード-マラー符号の部分符号の関係にある．すなわち，

$$\mathrm{RM}(0,m)\subseteq \mathrm{RM}(1,m)\subseteq\cdots\subseteq \mathrm{RM}(m,m)$$

- リード-マラー符号 RM(r,m) の双対符号（1-4 節）はリード-マラー符号 RM$(m-r-1,m)$ である．

- リード-マラー符号 RM(r,m) は，設計距離 $2^{m-r}-1$ の拡大 BCH 符号（2-2 節）の部分符号である．特に リード-マラー符号 RM$(m-2,m)$ は $(2^m,2^m-m-1,4)$ 拡大ハミング符号（節）と同じ符号である．

■1 群 - 2 編 - 1 章

1-8 線形ブロック符号のトレリス

（執筆者：高田豊雄）[2013 年 10 月 受領]

トレリスダイアグラム（trellis diagram）は畳込み符号のそれと同様（5-1 節），ブロック符号の図的な表現法の一種であり，符号の構造的な性質のみならず，様々な復号法（特に軟判定復号法）と密接な関連をもつ．詳細については例えば，文献 13) が詳しい．

1-8-1 定義

あるガロア体 GF(q) の上の線形ブロック符号 C のトレリスダイアグラムは以下の条件を満たす有向非循環グラフである．

1. 枝ラベルは，GF(q) の元あるいはその元の有限長の系列である．
2. 初期状態 σ_0，最終状態 σ_F と呼ばれる特別な状態（トレリスダイアグラムではグラフのノードは（畳込み符号のときと同様），状態（state）と呼ばれる）をもつ．
3. σ_0 と σ_F の間のパス上のラベル系列が C の符号語と，1 対 1 に対応する．

通常，枝のラベルの長さは，符号長 n の約数かつ一定長 ℓ とすることが多く，n/ℓ，すなわち，各符号語に対応する σ_0 と σ_F の間のパスの枝数のことをセクション数と呼ぶ．例として，GF(2) 上の $(8, 4, 4)$ 1 次のリード-マラー符号（拡大ハミング符号）（節）の 8 セクショントレリスダイアグラムを図 1･3 に示す．

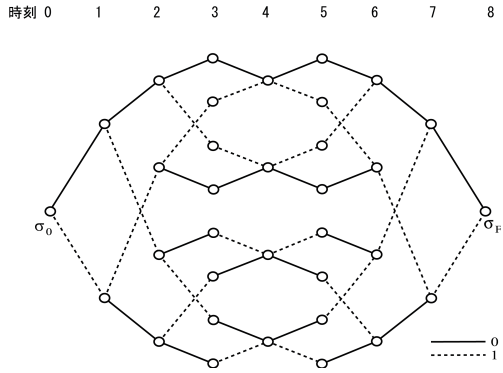

図 1･3　(8,4,4) リード-マラー符号の 8 セクショントレリスダイアグラム

後節のトレリスダイアグラムの構成法の説明の都合上，時刻の概念を導入する．すなわち，符号語の生成を有限状態機械で行うとみなし，初期時刻 0 から各時刻ごとに 1 セクションの長さ ℓ 分の符号語の部分系列が出力されると考える．このとき，トレリスダイアグラムの状態の縦方向の各列が左から順に時刻 $0, 1, \ldots, n/\ell$ に対応する．

以下では，最も基本的な n セクショントレリスダイアグラムの生成法について考える．

1-8-2 トレリス指向生成行列

まず，線形ブロック符号の最簡トレリスの構成法を説明するための準備として，トレリス指向行列（trellis oriented generator matrix）について述べる．

ある GF(q) の上の長さ n の非零ベクトル $\boldsymbol{v} = (v_1, v_2, \ldots, v_n)$ について，先頭非零成分，最終非零成分を，それぞれ，

先頭非零成分 v_i: $v_i \neq 0$ かつ各 $1 \leq j \leq i-1$ に対して $v_j = 0$

最終非零成分 v_i: $v_i \neq 0$ かつ各 $i+1 \leq j \leq$ に対して $v_j = 0$

とする．このとき，トレリス指向生成行列 $G_{TOGM} = (\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_k)^T$ の定義は次のとおり．

1. 各 $1 \leq i \leq k$ について，$\boldsymbol{v}_i$ の先頭非零成分のある列を j とすると，i 行目より下のすべての行ベクトル $\boldsymbol{v}'_i$（すなわち $i+1 \leq i' \leq k$）について，先頭非零成分の出現位置は j より後である．

2. 各行ベクトルの，$\boldsymbol{v}_i$ の最終非零成分の出現位置はすべて相異なる．

例えば，2 元 $(8,4,4)$ 線形符号である，節の 1 次のリード-マラー符号 RM$(1,3)$ のトレリス指向生成行列は以下のとおりとなる．

$$G_{\mathrm{RM}(1,3)\text{-}TOGM} = [\boldsymbol{v}_1, \boldsymbol{v}_2, \boldsymbol{v}_3, \boldsymbol{v}_4]^T = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} \tag{1·28}$$

1-8-3 トレリス指向生成行列と最簡トレリス

節で述べたトレリスダイアグラムの定義から，ガロア体 GF(q) 上の (n,k) 線形符号のトレリスダイアグラム上の σ_0 と σ_F の間の各パスは C の符号語 $\boldsymbol{c}$:

$$\boldsymbol{c} = i_1\boldsymbol{v}_1 + i_2\boldsymbol{v}_2 + \cdots + i_k\boldsymbol{v}_k, \qquad (i_1, i_2, \ldots, i_k) \in \mathrm{GF}(q)^n$$

と 1 対 1 に対応する．ここで，$\boldsymbol{v}_j$ は C の生成行列の j 番目の行ベクトルである．このことから，トレリスダイアグラムにおける状態とは，$(i_1, i_2, \ldots, i_k)$ の値に対応していることが分かる．

更に，状態数が最小という意味で最簡トレリスダイアグラム（minimal trellis diagram）について考える．例えば，$(n,1)$ 2 元線形符号 C，その生成行列の唯一の行ベクトルを $\boldsymbol{v} = (v_1, v_2, \ldots, v_n)$，$\boldsymbol{v}$ の先頭非零成分，最終非零成分の列位置をそれぞれ，i, j とすると，C の最簡トレリスダイアグラムは次の，図 1·4 のようになる．

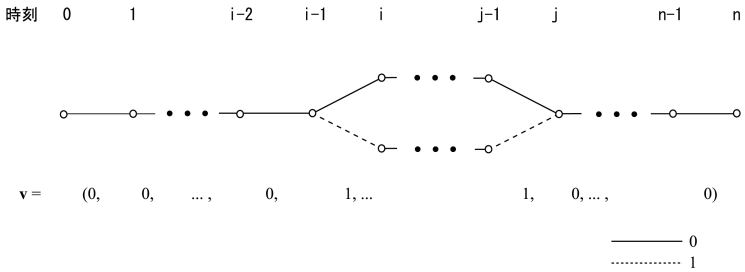

図 1･4 (n,1) 2 **元符号の 最簡トレリスダイアグラム**

このように時刻 $0, 1, \ldots, i-1$ 及び，$j,\ j+1, \ldots, n$ の各時刻ではトレリスダイアグラムに複数の状態を設けて符号語 $0 \cdot \boldsymbol{v}$ と $1 \cdot \boldsymbol{v}$ を区別する必要がないことが分かる．

一般の場合を考える．最簡トレリスダイアグラムの行ベクトルを $\boldsymbol{v}$，その先頭非零成分，最終非零成分の列位置をそれぞれ，$i,\ j$ とする．このとき，$\boldsymbol{v}$ の活性化（active）時間 $\tau_a(\boldsymbol{v})$ を区間 $[i, j-1]$ と定義する（ただし $i = j$ のときは $\tau_a(\boldsymbol{v}) = \phi$）とする．

例: リード-マラー符号 RM(1, 3) のトレリス指向生成行列（式 (1･28）の各行ベクトルの活性化時間はそれぞれ次のとおり．

$$\tau_a(\boldsymbol{v}_1) = [1, 3],\ \tau_a(\boldsymbol{v}_2) = [2, 6],\ \tau_a(\boldsymbol{v}_3) = [3, 5],\ \tau_a(\boldsymbol{v}_4) = [5, 7]$$

各時刻 t ごとの活性化しているベクトルは次のとおり．

時刻	1	2	3	4	5	6	7
活性化しているベクトル	$\boldsymbol{v}_1$	$\boldsymbol{v}_1, \boldsymbol{v}_2$	$\boldsymbol{v}_1, \boldsymbol{v}_2, \boldsymbol{v}_3$	$\boldsymbol{v}_2, \boldsymbol{v}_3$	$\boldsymbol{v}_2, \boldsymbol{v}_3, \boldsymbol{v}_4$	$\boldsymbol{v}_2, \boldsymbol{v}_4$	$\boldsymbol{v}_4$

この符号の符号語 $\boldsymbol{v}$ を $\boldsymbol{v} = i_1\boldsymbol{v}_1 + i_2\boldsymbol{v}_2 + i_3\boldsymbol{v}_3 + i_4\boldsymbol{v}_4$ とすると，$\boldsymbol{v}_j$ が活性化している時間だけ，最簡トレリスダイアグラムにおいて異なる状態を設け，i_j が 0 であるか 1 であるかを区別すればよいわけであるから，この符号の最簡トレリスダイアグラムは図 1･3 となる．

ここで，例えば時刻 4 におけるトレリスダイアグラムの四つの状態は上から順に，$0 \cdot \boldsymbol{v}_2 + 0\boldsymbol{v}_3$，$0 \cdot \boldsymbol{v}_2 + 1\boldsymbol{v}_3$，$1 \cdot \boldsymbol{v}_2 + 0\boldsymbol{v}_3$，$1 \cdot \boldsymbol{v}_2 + 1\boldsymbol{v}_3$ に対応している．同じく時刻 5 におけるトレリスダイアグラムの八つの状態は上から順に，$0 \cdot \boldsymbol{v}_2 + 0\boldsymbol{v}_3 + 0\boldsymbol{v}_4$，$0 \cdot \boldsymbol{v}_2 + 0\boldsymbol{v}_3 + 1\boldsymbol{v}_4$，$0 \cdot \boldsymbol{v}_2 + 1\boldsymbol{v}_3 + 0\boldsymbol{v}_4$，$0 \cdot \boldsymbol{v}_2 + 1\boldsymbol{v}_3 + 1\boldsymbol{v}_4$，$1 \cdot \boldsymbol{v}_2 + 0\boldsymbol{v}_3 + 0\boldsymbol{v}_4$，$1 \cdot \boldsymbol{v}_2 + 0\boldsymbol{v}_3 + 1\boldsymbol{v}_4$，$1 \cdot \boldsymbol{v}_2 + 1\boldsymbol{v}_3 + 0\boldsymbol{v}_4$，$1 \cdot \boldsymbol{v}_2 + 1\boldsymbol{v}_3 + 1\boldsymbol{v}_4$ に対応している．

以上の議論より分かるとおり，各時刻の活性化行ベクトルの本数は最簡トレリスダイアグラムの当該時刻の状態数を定める．そのため，時刻 0 から n までの活性化行ベクトルの本数を成分にもつベクトルのことを状態空間次元プロファイル（state space dimension profile）と呼ぶ．例えば，リード-マラー符号 RM(1, 3) の状態空間次元プロファイルは，

$$(0, 1, 2, 3, 2, 3, 2, 1, 0)$$

である．

また，単に，（ガロア体 GF(q) の上の）線形ブロック符号のトレリスダイアグラムの状態数という場合，q^{ν} のことを指す．ここで，ν は，その符号の状態空間次元プロファイル中の最大値である．例えば，リード-マラー符号 RM(1, 3) の 8 セクショントレリスダイアグラムの状態数は $2^3 = 8$ である，という．

■参考文献

1) S. Lin and D.J. Costello, Jr., “Error Control Coding, Second Edition,”Pearson Prentice Hall, 2004.
2) 平澤茂一, “情報理論入門,” 培風館, 2000.
3) 今井秀樹, “符号理論,” 電子情報通信学会, 1990.
4) C.E. Shannon, “The mathematical theory of communication,” Bell Sys. Tech. Journal, vol.27, pp.379-423, 623-656, 1948.
5) R.G. Gallager, “Information theory and reliable communication,” Wiley, New York, 1968.
6) R. Blahut, “Principles and Practice of Information Theory,” Addison-Wesley, 1987.
7) T.M. Cover and J.A. Thomas, “Elements of Information Theory, 2nd edition,” John Wiley & Sons, 2006.
8) B.L. van der Waerden, “Algebra,” Springer-Verlag, Berlin, 1966.
9) R.W. Hamming, “Error Detecting and Error Correcting Codes,” *Bell Syst. Tech. J.*, vol.29, pp.147–160, April 1950.
10) M.J.E. Golay, “Notes on Digital Coding,” *Proc. IEEE*, vol.37, p.657, June 1949.
11) D.E. Muller, “Applications of Boolean Algebra to Switching Circuits Design and Error Detection,” *IRE Trans.*, vol.EC-3, pp.6–12, Sept. 1954.
12) I.S. Reed, “A Class of Multiple-Error-Correcting Codes and the Decoding Scheme,” *IRE Trans.*, vol.IT-4, pp.38-49, Sept. 1954.
13) S. Lin, T. Kasami, T. Fujiwara, M. Fossorier, “*Trellis and Trellis-Based Decoding Algorithms for Linear Block Codes*,” Kluwer Academic Press, MA, 1998.