

コラム：線形符号

実数体 $\mathbb{R}$ や複素数体 $\mathbb{C}$ 等の様なよく知られた体以外にも体は色々あって、身近なところで役に立っている．例えば p を素数として、 $0, 1, \dots, p-1$ という p 個の整数を $\text{mod } p$ で考えると、これらは体をなす．元の個数が p 個であるから、これは p 元体と呼ばれ、 $\mathbb{F}_p$ なる記号で表す（一般に、元の個数が有限個である体を有限体と呼ぶ）．有限体は例えば情報理論で活躍する．ここでは一例として線形符号の理論の一端を紹介しよう．

デジタル通信では多くの場合情報を 2 進数の列で表す．それは 2 元体 $\mathbb{F}_2$ 上のベクトル空間の元の列とも思える．そこで以下では $V = (\mathbb{F}_2)^n$ を $\mathbb{F}_2$ 上の n 次元数ベクトル空間とし、その元を「情報」と思って、これを送信する、という状況を想定しよう．情報を電気信号として送信する場合、誤りが生じる可能性がある．例えば 010 と送ったつもりが 011 と受信されてしまった、等．物理的に誤りが生じてしまうことは完全には防げないので、その様な場合でも、ある程度までの誤りであれば、それを訂正して、正しい情報を復元出来るようにしたい．単純なアイディアとしては、情報を構成する各数を複数回繰り返す、という手がある（その様な方式で送信する事はもちろん受信者にも周知しておく）．例えば、「010」というメッセージを送りたいとき、各数を二度繰り返して「001100」と送る．すると、もしこれが誤って「001000」と送られてしまったとすると、中央の「10」の部分は誤りであると分かる．しかし元々「00」だったのか「11」だったのかは分からない．そこで今度は各数を三度繰り返して「000111000」と送る．すると、どこか一ヶ所で誤りが生じても（誤りが多過ぎなければ）訂正できる．例えばこれが「000101000」と受信されてしまったとしたら、恐らく中央の「0」は誤りで、正しくは「000111000」であろうと見当がつく．しかしもし二ヶ所誤りが生じて「000100000」と受信されてしまったとすると、恐らく 4 番目の「1」が誤りで、正しくは「000000000」であろうと推測されてしまい、メッセージが誤って伝わってしまう．この様な可能性も無くはないが、もともと一ヶ所の誤りが生じる可能性も低いと仮定するならば、この様な可能性はさらに低い．もし二ヶ所の誤りも訂正したければ、各数を 5 回繰り返して送信すればよい．この様にして、繰り返しを増やせば訂正能力は上がって行くが、 n 回繰り返すことにすると、折角 $3n$ 桁

のスペースを用意しておきながら実際に送れるのは3桁分のメッセージに留まるので、通信リソースの「無駄」が大きくなる。実用的には、無駄を最小限に抑えながら誤り訂正能力を上げたい。これが符号理論の目標の一つである。

線形代数学の立場から上の議論を見直してみよう。上の例で、送りたい元のメッセージ「010」は3次元 $\mathbb{F}_2$ ベクトル空間 $\mathbb{F}_2^3$ の元（3次元列ベクトル）と見なせるが、これを、例えば「000111000」と送るのであれば、この信号は9次元 $\mathbb{F}_2$ ベクトル空間 $V = \mathbb{F}_2^9$ の元と見なせる。正しく送られた信号は「 $xxxyyyzzz$ 」（ $x, y, z \in \mathbb{F}_2$ ）の形をしているのだから、それらは V の3次元部分空間

$$W = \{[x \ x \ x \ y \ y \ y \ z \ z \ z] \mid x, y, z \in \mathbb{F}_2\}$$

に属する（この W のことを、符号理論では「線形符号」と呼ぶ）。逆に、受け取った信号がこの部分空間に入っていなければ、どこかで誤りが生じたと判明する。本来の信号 v ($\in W$) が誤って v' ($\notin W$) と配信されてしまったとき、 v' に「一番近い」 $v \in W$ がただ一つ存在すれば、訂正が可能である。上で述べた「誤り訂正能力が高い」とは、 v' が W から比較的遠く離れていてもそれに「一番近い」 $v \in W$ がただ一つ存在する、という事を意味している。また、「無駄が小さい」とは、信号全体のなすベクトル空間 V の次元に対して、正しい信号全体のなす部分空間 W の次元が比較的大きい事を指している。

上で説明したものは線形符号の非常に簡単な場合である。この様に、線形符号の理論は有限体上のベクトル空間の理論を基礎としている。現実に使われている符号には様々なものがあり、電子機器などに広く応用されている。