第77回数学教育実践研究会　レポート発表

「『損』して『得』取れ！」

北海道室蘭東翔高等学校教諭　長尾良平

平成23年6月11日　北海道大学情報教育館

1　始めに

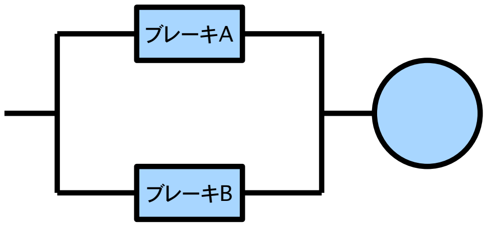
本稿では, 1年生と3年生に対して行った2つの実践を紹介してみたい. それらの実践に共通なキーワードとして, **「冗長性」**が挙げられる. それは, **余分なものを付け加えることにより, 信頼度を向上**させようという発想である. 実生活への応用例であり, 生徒の知的関心を少しつつくことのできる題材だと思う.

最後に, 発展事項等についても考えてみたい.

2　稼働率

確率の単元では, くじやさいころなど**身近な題材を用いた出題**も多いため, 生徒も興味をもって授業に臨んでくれることが多い. そこからもう一歩興味を深めて欲しいと思い, 独立試行のところで以下に述べる実践を行った.

例1　ある車には2系統のブレーキが整備されている. どちらのブレーキも, 確率0.9で正常に動作するように設計されている. 少なくとも1台のブレーキが作動して, この車が停止できる確率を求めよ.



1台のブレーキが故障する確率は0.1だから, 2台とも故障する確率は $0.1^2 = 0.01$ である.

したがって, 少なくとも1台のブレーキが正常に作動して車が停止できる確率は,

$$1 - 0.01 = 0.99$$

である.

類題は, 情報処理技術者試験の「ITパスポート試験」・「基本情報技術者試験」等で頻出である.

この問題が面白いのは, **並列接続することにより, 稼働率を上げることができる**点にある.

同様の計算を正常動作する確率を0.7で行うと, 少なくとも1台が動作する確率は0.91に上昇する. この結果を板書したとき, 生徒から**「すげー20％もアップする！」**という声が上がった.

教訓

精度が低い部品でも, 組み合せることで精度を上げることができる（**冗長化**という）.

サーバ等で用いられるRAIDも

Redundant Arrays of **Inexpensive** Disks

の略であり, 元来はあまり費用のかからない製品を組み合わせて効果を生むことを狙っている.

これらの題材を導入にして, **安全工学・信頼性工学**について取り扱うのも面白いと思う. その例を1つ挙げる.

例2　**故障時や緊急時に, 常に安全側に動作**する設計手法のことを**フェイルセーフ**という.

具体例としては, 鉄道車両における「直通空気ブレーキ」から「自動空気ブレーキ」への変更などが挙げられる.

3　ハミング符号

昨年度も「看護・医療系」対象の演習中心の授業を担当しており, 第一陣の受験が終了した後は, 初等整数論の話を扱った.

拙稿 [4] で取り上げた **ISBN** は今年度も扱い, 今年度新たに**ハミング符号**を取り扱ったので, 後者について紹介したい.

まず, 両者の性質を挙げると次のようになる.

ISBN

- 任意の 1 箇所のミスを**検出可能**
- 任意の 2 箇所の入れ替わりを**検出可能**
- 任意の 1 箇所について**消失訂正可能**

ハミング符号

- 2 ビットまでの誤りを**検出可能**
- 1 ビット誤りを**訂正可能**

ともに**誤り検出**が可能で, ハミング符号は**誤り訂正**も可能である. ハミング符号は 1950 年に発見された誤り訂正符号であり, 応用として ECC メモリにおいて, 誤り検出・訂正に活用されている.

授業には 2 時間を当て,

(1) 行列の説明, 行列の積の演習

(2) 有限体 $\mathrm{F}_2 = \{0, 1\}$ について説明・演習

(3) ハミング符号の説明・演習

(4) まとめのテスト

という流れで行った.

数学 C を履修している生徒が一人のみであったので, まず始めに行列の説明を行い, 続けて「行ベクトルと行列の積」の演習を行った.

ハミング符号では, **各ビットの値を $\mathbf{F_2}$ の値として扱う**ため, F_2 での演算法則を紹介した.

$+$	0	1
0	0	1
1	1	*0*

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

積は問題ないが, 和については $1 + 1 = \mathit{0}$ となるため,「0 を偶数の代表, 1 を奇数の代表として考えたらどうかな」と説明を加えた.

ハミング [7,4] 符号は, 4 ビットのデータに 3 ビットのデータを付け加え, 7 ビットのデータに符号化する.

$$\text{元データ}\ \boldsymbol{u} \xrightarrow{\text{生成行列}\ G\ \text{による符号化}} \text{符号}\ \boldsymbol{v} = \boldsymbol{u}G$$

符号化の際に 4 行 7 列の行列を扱うが, 行列演算に不慣れな生徒が対象であったので, 近畿大学の知念先生の Web ページ[1]を参考にし,（小振りな）ハミング符号から導入を行った.

例 3　生成行列 G

$$G = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \end{bmatrix}$$

を用いて, データ [1 0] を符号化せよ.

$$[\mathbf{1}\ \mathbf{0}] \begin{bmatrix} 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \end{bmatrix} = [\mathbf{1}\ \mathbf{0}\ 1\ 1\ 1]$$

生成行列 G の成分からも分かるように, 符号化されたベクトルの左側 2 列は元データそのものであり, 残り 3 列が新たに付け加えられた部分である.

このことから, 符号化されたデータが誤りを含んでいないことが分かれば, **元データに戻す復号は左側 2 列を取り出すだけ**で良い.

次に, その復号を見てみよう.

例 4　パリティ検査行列 H

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

を用いて, 符号 [1 1 1 1 1] が誤りを含むかチェックせよ. 誤りを含む場合はそれを訂正し, さらに元のデータに復号せよ.

[1] `http://www.math.kindai.ac.jp/~chinen/index.html`

符号とパリティ検査行列 H との積（**シンドローム**と呼ぶ）を計算することにより, 誤りを検出することができる.

$$[1\ 1\ 1\ 1\ 1]\begin{bmatrix}1&1&1\\1&0&1\\1&0&0\\0&1&0\\0&0&1\end{bmatrix}=[1\ 0\ 1]$$

計算結果 $[\mathbf{1}\ \mathbf{0}\ \mathbf{1}]$ と

$$H=\begin{bmatrix}1&1&1\\\mathbf{1}&\mathbf{0}&\mathbf{1}\\1&0&0\\0&1&0\\0&0&1\end{bmatrix}$$

とを見比べると, **2 行目が一致**していることが分かる．これは, **符号の 2 列目が誤りを含む**ことを示している.

よって,

$$[1\ \mathbf{1}\ 1\ 1\ 1]\xrightarrow{\text{訂正}}[1\ \mathbf{0}\ 1\ 1\ 1]\xrightarrow{\text{復号}}[1\ 0]$$

となる.

符号 $[1\ 1\ 1\ 1\ 1]$ は例 2 の符号化

$$[1\ 0]\to[1\ 0\ 1\ 1\ 1]$$

において 2 ビット目を反転させたものであり, パリティ検査行列 H を用いて, 確かに誤り検出ができている．なお, **符号が誤りを含まない時は, シンドロームは零ベクトルになる**.

また, 2 ビットの誤りに関しては, シンドロームが零ベクトルとならないので検出はできるが, **それが 1 ビットの誤りによるものなのかどうかと判別ができない**.

生徒達にとって, 行列演算と F_2 の扱いが初めてだったため授業がうまくいくか不安ではあったが, **0 と 1 だけの世界の演算に生徒達は順応**したようである．練習問題も後半はスイスイと解いていた.

まとめのテストでは, ハミング [7,4] 符号で用いられる

$$G=\begin{bmatrix}1&0&0&0&0&1&1\\0&1&0&0&1&0&1\\0&0&1&0&1&1&0\\0&0&0&1&1&1&1\end{bmatrix}$$

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

を用いた問題をチャレンジ問題として出題したが, 生徒達はコツを掴んだようで, 正答率はこちらの予想以上に高かった．（小振りな）ハミング符号から導入したのが良かったのかなと考える一方で, 最初からハミング [7,4] 符号でも良かったのかなとも考えている.

4　授業を終えて

今回は, 一話読切形式の授業であり, 理論的な取扱いは行わなかった．数学 C で行列を既習の生徒に対しては, 理論的な扱いも可能だと思う.

例 5　生成行列 G からパリティ検査行列 H を作成する.

$$G=\begin{bmatrix}1&0&0&0&0&1&1\\0&1&0&0&1&0&1\\0&0&1&0&1&1&0\\0&0&0&1&1&1&1\end{bmatrix}$$

を用いて,

$$\boldsymbol{u}=[u_1\ u_2\ u_3\ u_4]\xrightarrow{\text{符号化}}\boldsymbol{v}=[v_1\ v_2\ v_3\ v_4\ v_5\ v_6\ v_7]$$

を行うと, $\boldsymbol{u}$ と $\boldsymbol{v}$ の成分の間に

$$\begin{cases}u_i=v_i\quad(1\leqq i\leqq 4)\\u_2+u_3+u_4=v_5\\u_1+u_3+u_4=v_6\\u_1+u_2+u_4=v_7\end{cases}$$

を得る．F_2 においては, 加法と減法が等しくなることに注意し, $\boldsymbol{v}$ の成分間の関係式を求めると,

$$\begin{cases}v_2+v_3+v_4+v_5=0\\v_1+v_3+v_4+v_6=0\\v_1+v_2+v_4+v_7=0\end{cases}$$

を得る．この関係式を行列を用いて表現すると，

$$[v_1\ v_2\ v_3\ v_4\ v_5\ v_6\ v_7]\begin{bmatrix}0&1&1\\1&0&1\\1&1&0\\1&1&1\\1&0&0\\0&1&0\\0&0&1\end{bmatrix}=\boldsymbol{O}$$

となり，パリティ検査行列 H が得られる．

例 6　シンドロームについて調べてみる．符号 $\boldsymbol{v}=\boldsymbol{u}G$ が「誤り $\boldsymbol{e}_i$：第 i 成分のみ 1」を含み，$\boldsymbol{v}'=\boldsymbol{v}+\boldsymbol{e}_i$ になったとすると，線形性から

$$\boldsymbol{v}'H=(\boldsymbol{v}+\boldsymbol{e}_i)H=\boldsymbol{v}H+\boldsymbol{e}_iH=\boldsymbol{e}_iH$$

となり，パリティ検査行列の第 i 行が生じることが確かめられる．

前半に扱った独立試行との関連として，次の問題を扱うことも考えられる．

例 7　データ通信を行う際に，正しく伝送される確率 p を，1 ビットあたり $p=0.99$ とする．

1 ビットの誤りが発生する確率 p_1，2 ビットの誤りが発生する確率 p_2 を求めよ．

$$\begin{aligned}p_1 &= {}_7\mathrm{C}_1\cdot 0.99^6\cdot(1-0.99)\\ &= 0.06590361045807\end{aligned}$$

$$\begin{aligned}p_2 &= {}_7\mathrm{C}_2\cdot 0.99^5\cdot(1-0.99)^2\\ &= 0.00199707910479\end{aligned}$$

となる．なお，数学IIIで近似式

$$(1+x)^n \fallingdotseq 1+nx \quad (|x|\ll 1)$$

を学んでいれば，0.99^n の計算時に利用してみるのも面白いだろう．近似式を利用すると，

$$p_1 \fallingdotseq 0.0658,\ p_2 \fallingdotseq 0.001995$$

となり，良い近似を与えている．

5　終わりに

1 年生には最後の授業でアンケートをとったが，**印象に残っていることに「稼働率」のことを書いた生徒**がいた（**「20 %もアップする！」**という声を挙げた生徒である）．授業から 3 ヶ月以上が過ぎた年度末に実施したアンケートで記述があったということは，彼にとっては強く印象に残ったのだと思う．**授業者としては，嬉しい限り**である．

ハミング符号はやや敷居が高いかなと考えていたが，杞憂に終わった．誤り検出や消失訂正ができる ISBN を事前に扱っていたのも有効であったと思う．

放課後の講習の際に，生徒から**「先生は普段どんな本読んでるんですか？」**との質問を受けた．筆者が，授業で扱った内容を知っていることが不思議だったようだ．その生徒は，**「ISBN もハミング符号も誤りが発見できるのが，何だかとっても不思議で面白いです」**と笑顔で話してくれた．

京都大学の深谷先生は著書 [3] の中で，

> なによりまず数学をすることが好きで，数学にその人の思い入れがいっぱい詰まっていなければならない．**先生が嫌いなことを学生が好きになるはずがないのだ**

と書かれている．

これからも生徒の好奇心を刺激できるよう，教材研究を進めていきたい．

参考文献

[1] G.A. ジョーンズ, J.M. ジョーンズ
「情報理論と符号理論」シュプリンガー・ジャパン

[2] 「数学セミナー 2004 年 6 月号」日本評論社

[3] 深谷賢治「数学者の視点」岩波書店

[4] 長尾良平「余りものには『福』がある」
第 73 回数学教育実践研究会　発表レポート