数学パズルにおける数学的性質

2015SS014 日比野 郁
指導教員: 佐々木 克巳

1 はじめに

本研究の目的は, [1]の数学パズルのもとになっている数学的性質を詳しく調べることで, その数学パズルの本質を理解することである.

卒業論文では, [1]の問題のうちの3つを詳しく考察した. 本稿では, そのうちの巡回置換を用いる問題と誤り訂正符号を用いる問題を考察する.

2 第2話 死刑囚の生き残り戦略

この節では[1]の第2話の「死刑囚の生き残り戦略」という問題を詳しく考察する. まず, その問題を要約して以下に示す.

問題:刑場に4人の囚人が引き出され, ゲームを始める. 隣の部屋に箱が4つ並べてあり, それぞれに囚人の番号が書いてある免罪符が入っているが, どの箱に誰の免罪符が入っているかわからない. 3回以内に自分の免罪符を引き当てたら放免する. 他の囚人に箱の内容を仲間に伝えられない. 全員助かる確率を上げるのにはどんな戦略があるだろうか.

この問題に対する[1]の戦略は次のとおりである.
戦略1:左から数えて自分の番号になる箱を最初に開ける. その箱に自分の番号の免罪符が入っていなければ入っていた免罪符の番号の箱を開ける. 以下同様に続ける.

本研究では, [1]の解答の中の「最初の1人がどこかで免罪符を引ければ, 必ず全員が免罪符を引ける. その確率は$1-\frac{1}{n}$」を, 数学的に考察した. すなわち, 次の定理を証明した.

定理 2.1. 戦略1を使った場合, 次が成り立つ.
(1) 1人の囚人が免罪符を引く⇔全員が免罪符を引く
(2) 全員が免罪符を引く確率は$1-\frac{1}{n}$である.

定理 2.1.を証明するためにいくつかの準備をする. 本研究では, 以下の補助定理の証明も補って理解したが, 本稿では, その証明を省略する.

定義 2.2. 集合$\{1,\cdots,n\}$の写像σを次のように定める.
$\sigma(i)$ =「i番目の箱に入っている免罪符の番号」

系 2.3.
(1) σはn次の置換である.
(2)$\sigma^k(i)$は,「囚人iがk回目に引く免罪符の番号」である.

定義 2.4. n次の置換σが, 異なる$j_1,j_2,\cdots,j_k \in \{1,2,\cdots,n\}$に対して,

$$\sigma(j_1)=j_2,\sigma(j_2)=j_3,\cdots,\sigma(j_k)=j_1$$

となるとき, $\sigma=(j_1,j_2,\cdots,j_k)$と書き, 長さ$k$の巡回置換という.

系 2.5. n次の長さkの巡回置換$\sigma=(j_1,j_2,\cdots,j_k)$に対し,
(1) $\sigma=(j_2j_3,\cdots,j_k,j_1)=\cdots=(j_k,j_1,\cdots,j_{k-1})$
(2) どの$j\in\{j_1,j_2,\cdots,j_k\}$に対しても$j,\sigma(j),\cdots,\sigma^{k-1}(j)$は互いに異なり, $\sigma^k(j)=j$である.

補助定理 2.6. 任意の置換は互いに素な巡回置換の積に表される.

補助定理 2.7. 戦略1を使った場合, 次の3条件は互いに同値である.
(1) 囚人iが免罪符を引けない.
(2) 全員が免罪符を引けない.
(3) σが長さnの巡回置換である.

補助定理 2.8. σが巡回置換でない確率は$1-\frac{1}{n}$である.

定理 2.1.の証明. (1)は, 補助定理 2.7 の(1)⇔(2)から導かれる. (2)は, 補助定理 2.7 の(1)⇔(3)と補助定理 2.8 から導かれる.

3 女王陛下, ご自身の冠の色は?

この節では[1]の第6話の「女王陛下, ご自身の冠の色は?」という問題を考察する. まず, その問題と解答を要約して以下に示す.

問題の要約:三人が目隠しをして, 別の一人がそれぞれ三人に赤か白の冠を載せるゲームをする. その後, 目隠しを外して自分以外の冠を見て, 三人別々に自分の冠の色を答える. わからないと答えてもよいが, 三人ともわからない場合は負け. 誰かが答えて正解なら三人の勝ちだが, 一人でも間違えると負けになる. ここである考えが思い浮かび, その戦略によると勝率は$\frac{3}{4}$になる. どのような案だろうか.

解答の要約:その戦略は「他の2人の冠の色が同じなら, その反対の色を答える. 2人の色が赤と白なら『わからない』と答える」というもの. 全員が同じ色なら全員が外れて負けになるが, それ以外は勝ちになる. 3人の色のとり方が2^3で, 全員が同じ色なのはこのうちの2通りなので, 勝率は$\frac{2^3-2}{2^3}=\frac{3}{4}$となる.

この戦略は「誤り訂正符号」の「ハミング符号」を利用している．赤を1，白を0と解釈すると，3人の色のとり方は3ビットの2進数で表現できる．負けとなる「全員が同じ色」を表す2進数は，000 と 111 で，この2つの2進数の集合 C が次の（条件1）（$k=3$ のとき）を満たすことから，勝率が $\frac{2^3-2}{2^3}$ となる．

（条件1）どんな k ビットの2進数 s にも，C のある要素 t が存在して，s と t の違いは1ビット以内である．

［1］は，この戦略を7人の場合にも適用している．すなわち，（条件1）（$k=7$ のとき）を満たす C の例を挙げてそれを用いて，勝率が $\frac{2^7-c_0}{2^7}=\frac{7}{8}$ となると説明している．ただし，c_0 は C の要素数で具体的には $c_0=16$ である．さらに，［1］の解答に次の記述がある．
「例えば長さ $k=2^m-1$ のハミング符号も存在するが，その場合，$c_0=2^{k-m}$ だから，勝率は $1-\left(\frac{1}{2}\right)^m$ となる．」
以下に，この部分について考察し，その結果を示す．

［1］では，$k=7$ の場合のハミング符号を具体的な16個の2進数の集合として定義しているが，一般の k については定義していない．しかし，文脈から，（条件1）と次の（条件2）を満たす k ビットの2進数の集合 C を意識していると考える．

（条件2）C の要素数は 2^{k-m} である．

本研究では，（条件1）と（条件2）を満たす C の具体的な作り方を補う．さらに，当たる確率を上げるためには，c_0 が小さいことが望ましいので，上の2条件を満たす C が，要素数が最小となる C であることも確認する．すなわち，次の定理 2.1 の証明を考える．これ以降は，行列とベクトルの成分は0か1であることを約束する．また，k ビットの2進数 $x_1\cdots x_k$ と k 次の行ベクトル $(x_1\ \cdots\ x_k)$ を同一視する．「＋」と「¯」は次のように定義する．

$$0+0=0 \quad 0+1=1 \quad 1+0=1 \quad 1+1=0$$
$$\bar{0}=1 \qquad \bar{1}=0$$

定理 3.1. k と m は $k=2^m-1$ を満たす自然数とする．
（1）k ビットの2進数の集合 C で（条件1）および（条件2）を満たすものが存在する．
（2）k ビットの2進数の集合 C の要素数が 2^{k-m} 未満のとき，（条件1）は成り立たない．

定理 3.1（1）の証明. $(m,k)=(3,7)$ の場合を示す．
3次の行ベクトルのうち，1が2回以上現れるものは $2^3-(3+1)=4$ 個あるが，これらを並べてできる 4×3 行列を A とし，C^* を次のようにおく．

$$C^*=\{vG \mid v \text{は } 4 \text{ 次の行ベクトル}\} \qquad (*1)$$

ただし，G は4次の単位行列と A を横に並べた 4×7 行列で，次の形である．

$$G=\begin{bmatrix}1&0&0&0&x_{1,1}&x_{2,1}&x_{3,1}\\0&1&0&0&x_{1,2}&x_{2,2}&x_{3,2}\\0&0&1&0&x_{1,3}&x_{2,3}&x_{3,3}\\0&0&0&1&x_{1,4}&x_{2,4}&x_{3,4}\end{bmatrix}$$

この C^* が（1）の2条件を満たすことを示せばよい．
本稿では，G が次の G_1 のときの C^* が（条件1）を満たすことのみを示す（本研究では，一般の G の場合に（条件1）を満たすこと，および，一般の C^* が（条件2）を満たすことの証明も補って理解しているが本稿では省略する）．

$$G_1=\begin{bmatrix}1&0&0&0&1&1&0\\0&1&0&0&0&1&1\\0&0&1&0&1&0&1\\0&0&0&1&1&1&1\end{bmatrix}$$

2^7 個の7ビットの2進数（7次の行ベクトル）から任意に1個をとり，それを

$$v=(x_1\quad x_2\quad x_3\quad x_4\quad x_5\quad x_6\quad x_7)$$

とおく．（1）より，次の w は C^* に属する

$$w=(x_1\quad x_2\quad x_3\quad x_4)G$$
$$=(x_1\quad x_2\quad x_3\quad x_4\quad P\quad Q\quad R)$$

ただし，$P=x_1+x_3+x_4$，$Q=x_1+x_2+x_4$，$R=x_2+x_3+x_4$ とする．$(x_1\quad x_2\quad x_3\quad x_4)$ を固定すると，v のとり方は x_5,x_6,x_7 に応じて8通りある．この8通りと w を表 2.1 にまとめて比較する．

表 3.1：w と v の比較

v	x_1	x_2	x_3	x_4	P	Q	R
w	x_1	x_2	x_3	x_4	P	Q	R
	x_1	x_2	x_3	x_4	P	Q	$\bar{R}$
	x_1	x_2	x_3	x_4	P	$\bar{Q}$	R
	x_1	x_2	x_3	x_4	$\bar{P}$	Q	R
	x_1	x_2	x_3	x_4	P	$\bar{Q}$	$\bar{R}$
	x_1	x_2	x_3	x_4	$\bar{P}$	Q	$\bar{R}$
	x_1	x_2	x_3	x_4	$\bar{P}$	$\bar{Q}$	R
	x_1	x_2	x_3	x_4	$\bar{P}$	$\bar{Q}$	$\bar{R}$

表 3.1 の v の1行目から4行目までは w と v の違いが1ビット以内であることは表より明らかである．
5行目の v が，w と異なるのは右から1列目と右から2列目である．この2列に x_2 が現れるが，右から3列目には現れない．この x_2 に着目し，$u=(x_1\quad \overline{x_2}\quad x_3\quad x_4)G$ と v を比較する．$u\in C^*$ なので，v と u の違いが1ビット以内であればよい．

$$u=(x_1\quad \overline{x_2}\quad x_3\quad x_4)G$$
$$=(x_1\quad \overline{x_2}\quad x_3\quad x_4\quad P\quad \bar{Q}\quad \bar{R})$$

であり，確かに v との違いは第2ビットのみである．
6行目から8行目までも同様に考えると，$G=G_1$ のときに（条件1）を満たすことが示される．

定理 3.1（2）の証明は本研究では補って理解したが，本稿では省略する．

参考文献

［1］坂井公：『パズルの国のアリス　美しくも難解な数学パズルの物語』．日経サイエンス社，東京，2014．