高校生のための現代数学講座
「確率の考え方」
講義 (2)　鎌谷研吾

東京大学
玉原国際セミナーハウス
2010 年 7 月 24 日

「確率の応用例」

1　じゃんけんの問題

じゃんけんをするとき、くせがあってそのくせを読みとられてしまうと、長くじゃんけんを続けると負ける率が高くなる。くせのないようにじゃんけんを行うには、でたらめに出す手を選ぶという方法がある。

問題４の１を見てみよう。このゲームの利得表を作ると以下のようになる。

		自分		
		グー	チョキ	パー
相手	グー	0	-100	100
	チョキ	100	0	-100
	パー	-100	100	0

（正確にできた）さいころを振り１, ４が出ればグー、２, ５が出ればチョキ、３, ６が出たらパーを出すことにする。相手がグーを出すときの利得は、もし、じゃんけんを何度もやると、ベルヌイの大数の法則により 0 円である頻度が全体の $\frac{1}{3}$, -100 円である頻度が $\frac{1}{3}$, $+100$ 円である頻度が $\frac{1}{3}$ となり、全体としてみると１回の勝負で得る利得はおおよそ

$$0 \times \frac{1}{3} + (-100) \times \frac{1}{3} + 100 \times \frac{1}{3} = 0$$

となる。これは　**利得** $\times$ **確率**の和　である。これを**期待値**と呼ぶ。１度切りの勝負では期待値の意味ははっきりしない。相手がチョキ、パーを出す時も同様である。

相手がどのような戦略を繰り出しても、相手が何を出すかと、振ったさいころの目は関連がないので、この関係は変わらない。つまり、どのようにやっても負けない（しかし勝つこともない）のである。

では問題４の２の場合はどうであろうか。この時の利得表は

		自分		
		グー	チョキ	パー
相手	グー	0	-300	600
	チョキ	300	0	-600
	パー	-600	600	0

となる。先と同じようにどの手も $\frac{1}{3}$ の確率で出すと、

相手がグーを出すとき利得の期待値は

$$0 \times \frac{1}{3} + (-300) \times \frac{1}{3} + 600 \times \frac{1}{3} = 100$$

相手がチョキを出すとき利得の期待値は

$$300 \times \frac{1}{3} + 0 \times \frac{1}{3} + (-600) \times \frac{1}{3} = -100$$

相手がパーを出すとき利得の期待値は

$$(-600) \times \frac{1}{3} + 600 \times \frac{1}{3} + 0 \times \frac{1}{3} = 0$$

従って、相手はチョキを出し続ければ勝てることになる。実は一般論として、上手く確率を選べば、すべての場合の利得の期待値を 0 にできることが知られている。

では、グーを確率 p で、チョキを確率 q で、パーを確率 r で出すことにすると、

$$p + q + r = 1$$

であり、

相手がグーを出すとき利得の期待値は　$-300q + 600r$

相手がチョキを出すとき利得の期待値は　$300p - 600r$

相手がパーを出すとき利得の期待値は　$-600r + 600q$

となる。$p = \frac{2}{5}, q = \frac{2}{5}, r = \frac{1}{5}$ とおくと、利得の期待値はすべて 0 となる。この戦略で長くじゃんけんをすると、グー、チョキを多く出すということを知られてしまうが、それでも勝つことも負けることもない戦略となる。

2　乱数による暗号

暗号は現在いろいろなところで用いられており、日常的なものとなりつつある。しかし、かっては、主に軍事や外交において電波で情報を送るために用いられていた。ここでは簡単のために、アルファベットで書かれた文章を情報の送信者から受信者へ情報を送ることを考える。アルファベット２６文字に「空白」も文字と考えて加えると、２７文字となり、３の３乗なので、０, １, ２の３文字で３進数的に表記することができる。

A 001	B 002	C 010	D 011	E 012	F 020	G 021	H 022	I 100
J 101	K 102	L 110	M 111	N 112	O 120	P 121	Q 122	R 200
S 201	T 202	U 210	V 211	W 212	X 220	Y 221	Z 222	空白 000

乱数に基づく暗号は 1917 年に G.Vernam により考案されたものでバーナム暗号とも呼ばれる。この暗号は解読表（乱数表）を知らなければ、絶対に解読することが出来ない。乱数暗号は以下のようにして作る。

		N	U	M	A	T	A
(1)	３進数化	112	210	111	001	202	001
(2)	乱数	001	122	222	021	002	101
(3)	暗号	110	002	000	022	201	102
(4)	文章化	L	B	空白	H	S	K
(5)	乱数の補数	002	211	111	012	001	202

この結果、”NUMATA” は ”LB HSK” に変換される。

	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

ここで (2) の乱数はさいころを振り、１, ４が出たら１, ２, ５が出たら２, ３, ６が出たら０という風にして作った数列である。(1), (2) から (3) は３進和（２つの数を足して３以上になったら３を引く）で作ったものである。(5) の乱数の補数は (2) の乱数との３進和が０となるような数である。この時、(1) は (3) と (5) の３進和で求めることができる。従って、暗号の受信者は (5) の数の列を知っていれば、暗号を解くことができる。(3) の数の列には規則性が全くない。それは (2) で現れる 18 個の数字の列がどの列も同じ確率 $\left(\frac{1}{3}\right)^{18}$ で現れるので、(3) の暗号に現れる 18 個の数字の列も同じ確率で現れるためである。