確率の話（おもしろ数学教室講演）

楠岡成雄

古い話で恐縮ではあるが，2001 年 10 月 17 日に藤岡市において毎年行われている「藤岡市おもしろ数学教室」において「確率の話」と題して，中学生を相手に講演を行った．その内容について書いてくれと「数学通信」編集長より要望があったのであるが,「数学通信」第５巻第３号に書いた記事と大きな重複があるため辞退していた．ただ，講演後，藤岡市より，聴講した中学生の有志による感想文を３０枚弱ほど頂いた．講演した時は，反応がよくわからなかったが，それを読み，反省させられる点もあったので，それについて書かせてもらった．

1　講演の当初の企画

第３節に，講演のために用意しあらかじめ配った予稿に，講演時にどのようなことを行ったかを若干書き加えたものをあげているので，講演がどのようなものであるかは知りたい方は見ていただきたい．

講演では,「確率現象を解析する道具としての確率論」ではなく，乱数を人工的に発生させランダムネスを利用していくということが実際に行われているということを紹介することを目的として

１．乱数暗号

２．ゼロ和ゲーム（じゃんけんを例としてあつかった）

３．モンテカルロ法（さい投げで正方グラフの調和方程式を解く）

の３つの話題を取り扱った．

このような順で話をしたのは，おそらく中学生にとり理解しやすいと思った方から徐々に，一番の目的のモンテカルロ法に話を進めたかったからである．それぞれの場合に実際に，最前列の生徒に用意したさいころを投げてもらい，やり方の手順を説明した．また，３では擬似乱数発生によるシュミレーションの例も見せ，擬似乱数発生がいかに重要かつ難しいかという話もした．

2　感想文から得た生徒の反応

まず意外だったのは，もっとも分かり易かったのは，じゃんけんの例であったことである.「私はいつも癖を見破られてじゃんけんで負けてしまうのですが，さいころを振って何を出すか決めれば負けることはない，というのはその通りだと思った」といった感想があっ

た．乱数暗号の話は，まず暗号の作り方，また暗号から原文を構成する方法を，実際にさいころを振りながら説明し，こうすれば原文が「FUJIOKA」であるか「OKINAWA」のどちらかであるかは全くわからないということを説明したつもりであったが，難しすぎたようである．この説明には約 10 分ほど費やしたのであるが，本当に理解してもらうには短すぎたようである．感想文を見ると，興味を持ってくれた人はかなりいたようなので，これは中学生に対する講演の題材としては適当であったようである．ただ,「確率」というものを論理的に考えるということを経験していない中学生に説明するには，簡単な例から初めて，同じことを繰り返し説明する必要があったのであろう．

じゃんけんの話は納得できた人が多かったということではあったが，利得を「グーで勝つと 3 ポイント，チョキ・パーで勝つと 6 ポイント相手からもらう」という風に変えればどうなるかという話をしたとたんに難しいと感じたようである.「グーで勝っても得にならないから，グーを出す確率を小さくするのがよいと思った」という感想があったが，なるほど単純に考えれば，そういう結論もあるのかと感心した．このような答えを予想しておれば，この考え方を手がかりとして,「でもそうすれば相手はチョキを多く出すようにするとパーで負けることが多くなり，不利になる．だからパーを出す確率を小さくしなければいけない.」というように説明すれば，より説得力があったと思う．正確な結論を得るための数学的な考察はそのようにいろいろと考えさせてからの方がよりわかりやすかったであろう．ここに割いた時間は 20 分ほどであったが，これもやはりじっくりと時間をかけるべきであったように思う．

最後のモンテカルロ法の話題が，実は講演の目的であった．どのようにすればよいかをさいころを振って説明したが，その原理は説明が不可能と思い説明しなかった．一次方程式の未知数が多いこともあり，この話にどのくらい興味を持ってもらえるか不安だったが，少数ではあるがおもしろいと思ってくれた人がいたようである．

最近，高校生相手に「確率論」の講演を行う機会があったが，ほとんどの場合それは「数学に強い興味を持つ高校生」相手であった．今回，一般の中学生を相手の講演で，未だにどのように講演すべきであったか，わからないのでいるが，非常に貴重な体験であった．このような機会を与えてくれた藤岡市教育委員会にこの場を借りてお礼を申し上げる．

3　講演内容について

以下講演の際に配った予稿に少し説明を加えたものをあげておく．

はじめに

確率という概念は古くからある概念であり，曖昧にではあるが日常よく用いられている．確率を数学的に考えるということは，歴史の上では最初に賭博に関する考察として現れた．実際サイ投げやコイン投げといったことは純粋な試行実験として今でも用いられる．確率の考え方が不確実な現象を解析する上で役に立つであろうことは容易に想像できる（ここで，わかりやすい例として株価のグラフを示した）．しかし，不確実な現象を考えるときは多くの場合，この不確実性は本来は無い方が良い，邪魔なものである．ところが，確率の応用としてこの不確実性をむしろ利用しようとする考えがある．

この講演では，それらの例として

１．暗号
２．じゃんけんで負けない方法（ゼロ和ゲーム）
３．さい投げで１次方程式を解く（数値計算への応用，モンテカルロ法）
を紹介していく．
また，時間があれば乱数についても話をする予定である．

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

暗号の作り方には昔から色々なものが考案されているが，ここでは置き換えによる暗号の作り方と乱数暗号について解説する．

（置き換えによる方法）　今，次のような表を考える..

A	B	C	D	E	F	G	H	I	J	K	L	M	N
N	L	P	Q	O	J	K	I	V	W	U	Y	Z	X
O	P	Q	R	S	T	U	V	W	X	Y	Z	空白	－
S	T	R	D	E	C	G	H	F	A	B	M	空白	－

この表によって　ＦＵＪＩＯＫＡ　は　ＪＧＷＶＳＵＮ　に置き換わり，その３進数化は

１０１　０２１　２１２　２１１　２０２　２１０　１１２

となる．このような暗号は短い文に１度きり使う限りは解読されないが，何度も用いたり長文に用いるとその規則を見破られ可能性が高い．そのため傍受されると暗号が破られる可能性が高い．

（乱数に基づく暗号）

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．

		F	U	J	I	O	K	A
①	３進数化	０２０	２１０	１０１	１００	１２０	１０２	００１
②	乱数	００１	１２２	２２２	０２１	００２	０１２	１１０
③	暗号	０２１	００２	０２０	１２１	１２２	１１１	１１１
④	乱数の補数	００２	２１１	１１１	０１２	００１	０２１	２２０

３進和

	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．④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④の３進和で求めることができる．従って，暗号の受信者は④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２１個の数字の列がどの列も同じ確率 $(1/3)^{21}$ で現れるので，③の暗号に現れる２１個の数字の列も同じ確率で現れるためである．

		O	K	I	N	A	W	A
①	３進数化	１２０	１０２	１００	１１２	００１	２１２	００１
②	乱数	２０１	２００	２２０	０１２	１２１	２０２	１１０
③	暗号	０２１	００２	０２０	１２１	１２２	１１１	１１１

たとえば，原文が ＦＵＪＩＯＫＡ であったか，ＯＫＩＮＡＷＡ であったかはベイズの定理を用いて推測すると，同じような確からしさとなり，区別できない．

今日では乱数暗号はあまり用いられなくなったが，文字列がどれだけの情報をもつかという考え方はシャノンによる情報量という概念に発展していった．これは通信の理論ではなくてはならないものとなっている．

ゼロ和ゲーム

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．

じゃんけんを２人でして，負けた方が勝った方にポーカーチップを渡すというゲームをすることにしよう．もし，どの場合も負けた方は勝った方にポーカーチップを１枚だけ渡すとすると,「グー」,「チョキ」,「パー」はどれも対等なので，でたらめに同じ確率 1/3 で出せば，多分負けないであろう．実際，利得表を作ると次のようになる

		自分		
		グー	チョキ	パー
相手	グー	0	-1	1
	チョキ	1	0	-1
	パー	-1	1	0

たとえばもし，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と，相手がグーを出すとき利得の期待値は

$$0 \times (1/3) + (-1) \times (1/3) + 1 \times (1/3) = 0$$

相手がチョキを出すとき利得の期待値は

$$1 \times (1/3) + 0 \times (1/3) + (-1) \times (1/3) = 0$$

相手がパーを出すとき利得の期待値は

$$(-1) \times (1/3) + 1 \times (1/3) + 0 \times (1/3) = 0$$

となり勝つこともないが負けることもないことがわかる．

ではグーで勝ったときはポーカーチップを３枚，チョキ・パーで勝ったときは６枚もらえるとしたらどうだろう．この時の利得表は

		自分		
		グー	チョキ	パー
相手	グー	0	-3	6
	チョキ	3	0	-6
	パー	-6	6	0

となる．先と同じようにどの手も 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

$$0 \times (1/3) + (-3) \times (1/3) + 6 \times (1/3) = 1$$

相手がチョキを出すとき利得の期待値は

$$3 \times (1/3) + 0 \times (1/3) + (-6) \times (1/3) = -1$$

相手がパーを出すとき利得の期待値は

$$(-6) \times (1/3) + 6 \times (1/3) + 0 \times (1/3) = 0$$

となるので，相手はチョキを出せば勝てることになる．

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，$p+q+r = 1$ あり，

相手がグーを出すとき利得の期待値は　$-3q + 6r$

相手がチョキを出すとき利得の期待値は $3p - 6r$

相手がパーを出すとき利得の期待値は　$-6p + 6q$

となる．$p = 2/5, q = 2/5, r = 1/5$ とおくと，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．

サイ投げで１次方程式を解く

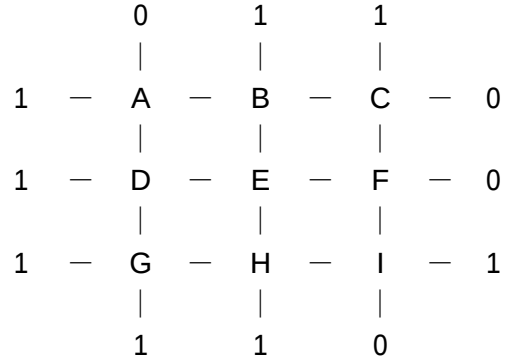
９つの未知数 A,B,C,D,E,F,G,H,I を未知数とする９元の一次方程式

(1)$B + 0 + 1 + D = 4A$,　(2)$C + 1 + A + E = 4B$,　(3)$0 + 1 + B + F = 4C$,

(4)$E + A + 1 + G = D$,　(5)$F + B + D + H = 4E$,　(6)$0 + C + E + I = 4F$,

(7)$H + D + 0 + 1 = 4G$,　(8)$I + E + G + 1 = 4H$,　(9)$1 + F + H + 0 = 4I$.

を考えよう．見るのも嫌になるかも知れないが，この方程式は次のようなグラフに関係した方程式である．



A,B,C,D,E,F,G,H,I の値それぞれが，それと線で結ばれている４つの値の平均と等しいということを表したのが (1)〜(9) の式である．

この方程式のＤの値を知りたい．どうすればよいか．９元の一次方程式は頑張れば手で解けるかもしれない．実際の応用では，未知数の数は 10^{15} に及ぶ場合があり，スーパーコンピュータを用いても普通のやり方では解けない．サイ投げで解く方法については講演の中で述べる．(実際にさいころ２個を何回も振り，ランダムウォークを発生させてその手順を実行して見せた．その後，乱数発生による数値実験の結果を見せた．)

乱数

上のような１次方程式をサイ投げで解こうとすると，グラフが巨大である場合何億回もさいころを振る必要があり，事実上不可能である．サイ投げの結果現れるような数の列を乱数と呼ぶ．乱数を高速に発生させるにはどうすればよいか，いろいろな方法が考えられている．放射性物質が発生させる放射線をカウントしたり，熱の生成する雑音を使用したりという方法が考えられているが，このような方法で得られる ０，１ よりなる乱数列で性質の良いものはせいぜい１秒間に数百万程度とされており，精度の高い計算にはあまり十分の早さではない．このため，コンピュータによる乱数発生というものが研究されている．ただしこれは厳密な意味での乱数には決してならないので擬似乱数と呼ばれている．擬似乱数の発生には，整数論をはじめとする色々な数学のアイデアが用いられている．

（くすおかしげお，東京大学大学院数理科学研究科）