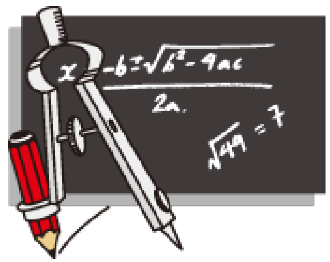
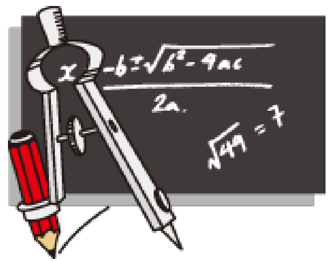


応用数学III
(1) 確率の基礎

木村真一

講義のスケジュール



(1)　確率の基礎

(2)　確率変数と確率分布

(3)　いろいろな確率分布

(4)　多次元確率分布

(5)　大数の法則と中心極限定理

(6)　確率過程の基礎１

(7)　確率過程の基礎２

(8)　フーリエ解析

(9)　相関関数

(10)　群・環・体の定義

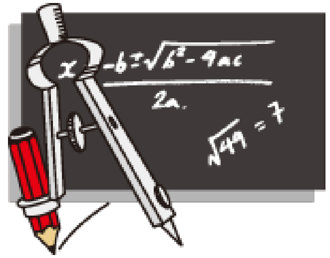
(11)　準同型写像

(12)　Nを法とする合同式

(13)　線形代数１

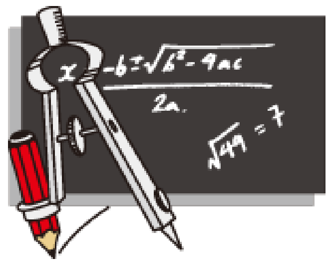
(14)　線形代数２

この講義での目標



- 情報通信・情報処理技術にとって重要な以下の項目について基本を理解しよう。
  - 確率
  - 確率過程
  - 代数
  - 線形代数
- 対象とする項目がそれぞれ大きいので、基本的な概念とそれぞれの項目での論理的な思考の仕方を中心に理解してください。
- それぞれ内容として大きいのでスケジュールが予定から多少前後する可能性があります。
- それぞれなぜ重要なのでしょうか。

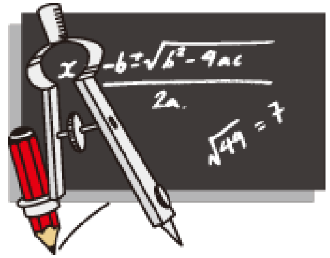
確率



- 確率は情報数学の入り口
  - いつもおきていることを教えてくれるよりも、起こりそうにないことを教えてくれる方が、情報として価値が高いですよね。
  - 例えばコイン投げで、どちらがでるかわかっていれば、半分の確率で損する所が救われる。
  - 競い合っている選挙候補、下馬評では完全に互角。どちらが当選したかを伝える情報は、同じように五分五分だった状態を、どちらか教えてくれる。

  - ですから、情報数学では情報の量を確率で議論します。
  - 確率の基本的な性質を理解することは情報を考える基礎になります。

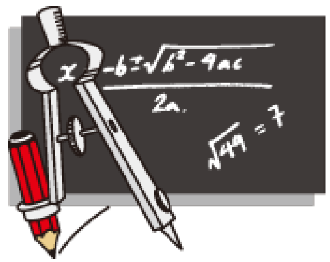
確率過程



- さて、ある電文が届きましたが一部かけてしまっています。四角に一文字入れて単語を完成してください。
  - 1）ア□ガオ　　2）ハ□シャ　　3）ナ□アギ
- ？考えてみたらなんでうめることができるのでしょう？
- そう言えば、言葉を途中まで聞けば最後まで聞かなくてもわかったりしますよね。

- そう、単語として意味を持つということは、ある並びがきたらその次に何が来るか、おおよそ予想がつきます。
- つまり順番や記号や状態の変わり方に、確率的は性質があることになります。これは確率の若干の拡張です。
- このような現象を扱う数学的手法のことを確率過程といいます。

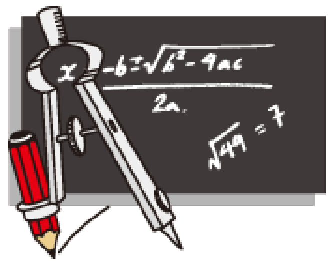
代数



- 話は変わって情報の暗号化の話。最近物騒ですから..。
- 最近よく使われる公開鍵暗号では、素因数分解や整数で割った余りなどが活用されているという話を聞いたことがありますか。
- 計算機はかけ算をする事は得意ですが、かけた結果からのもとのかけ算は何だったたか考えるのは苦手です。これを暗号化に使います。
- そう言えばかけ算、割り算の記号は習いましたが、整数で割った余りってどうやって書くのでしょう....。

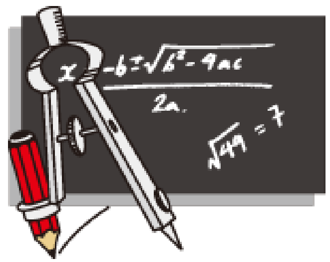
- こうしたことを理解するためには「代数学」の助けが必要です。
- ここでは、暗号化の基礎を理解するために「フェルマーの小定理」を理解することを目指します。

線形代数



- 線形代数については他の講義でしっかり勉強されたと聞きました。
- 実際にどう役に立つのか、余り意識されなかったかもしれませんが、情報処理を考える時に線形代数はものすごく役に立ちます。
- もし時間があれば、代数について勉強したついでに、線形代数についても、実際に使うという観点で少しだけ復習をしてみたいと思います。

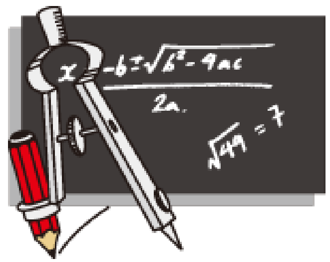
標本点



- まずはじめは基本的な概念と言葉の定義です。
- 退屈かもしれませんが、数学として論理を進めるためには定義が重要なので、お付き合いください。

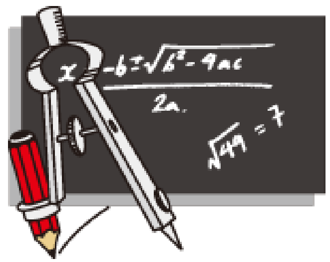
- 標本点ω：
  - これから確率で扱おうとする個々の現象です。
  - 例えばサイコロの出た目ならば１から6までの数字のいずれかになります。
  - つまり $\omega = 1$ であったり、$\omega = 3$ であったりできます。

標本空間



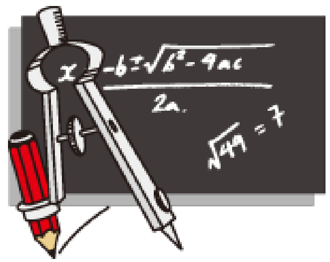
- 標本空間Ω：
  - 標本点の全体を集めた集合です。
  - サイコロならば１から6までの数字全て。
  - これを $\Omega = \{1,2,3,4,5,6\}$ と表します。
  - 標本点のとの関係として、ある標本点ωが標本空間Ωに属する、あるいは標本空間Ωの要素であるということを $\omega \in \Omega$ と表現します。

事象



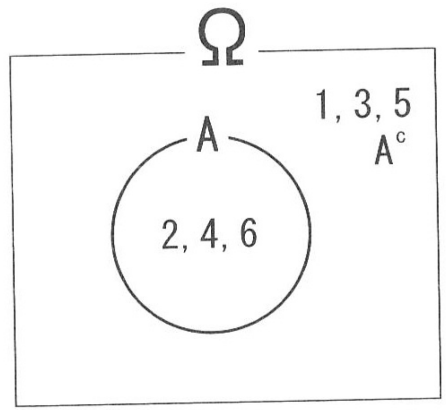
- 事象：
  - 標本空間の中の標本点の部分集合のことです。
  - 起きる事柄をある理屈に従って分類したものと思っていただいて結構です。
  - 事象は部分集合ですから、標本空間と同じように集合として表現します。
    - たとえば偶数の目が出るという事象： $A = \{2, 4, 6\}$
  - もちろん要素が一つでも結構。
    - 1の目が出るという事象： $B = \{1\}$
  - 理屈は適当でも結構。
    - 2と5が好きだから、 2と5の目が出るという事象：$C = \{2, 5\}$

全体事象・空事象・補事象



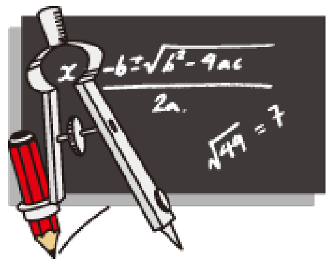
- 集合の議論を思い出してください。事象とは集合ですから全体集合、空集合が当然定義できます。

- 全体事象：
  - 標本空間の全ての標本点を含む事象
- 空事象ϕ：
  - 全く標本点を含まない事象
- 補事象：
  - ある事象が起きない事象
  - ある事象の標本点を全体事象から除いたもの



$$\Omega = \{1,2,3,4,5,6\}, A = \{1,2,3\} \Rightarrow A^c = \{4,5,6\}$$

和事象・積事象

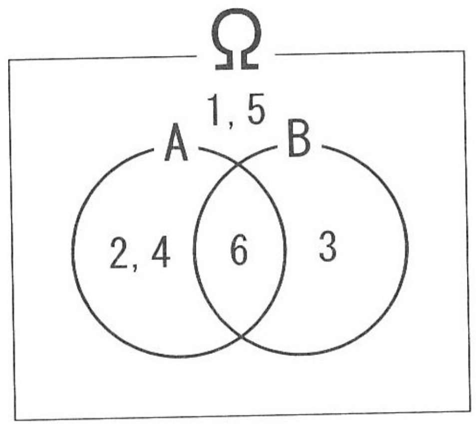


- **和事象：**
  - 二つの事象の少なくとも一つは起きる事象
  - 二つの事象の標本点を全て含む事象

$$A = \{2,4,6\}, B = \{3,6\} \Rightarrow A \cup B = \{2,3,4,6\}$$

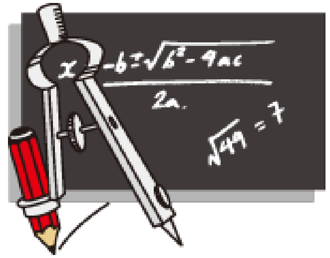
- **積事象：**
  - 二つの事象が同時に起きる事象
  - 二つの事象に共通する標本点の事象

$$A = \{2,4,6\}, B = \{3,6\} \Rightarrow A \cap B = \{6\}$$



- **排反事象：**
  - 同時に起こりえない事象
  - 積事象が空事象である　$A \cap B = \phi$

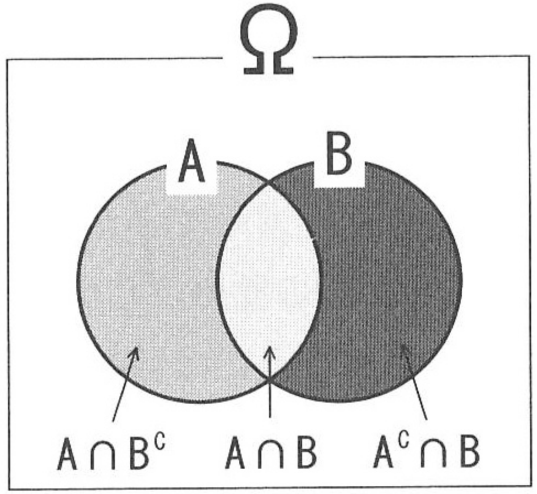
ド・モルガンの法則と結合・分配法則



- **ド・モルガンの法則**

$$(A \cup B)^c = A^c \cap B^c$$

$$(A \cap B)^c = A^c \cup B^c$$



- **結合法則**

$$(A \cup B) \cup C = A \cup (B \cup C) = A \cup B \cup C$$

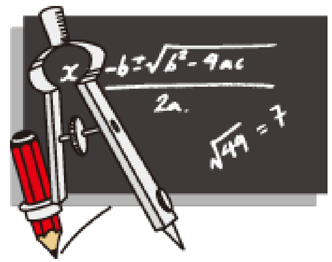
$$(A \cap B) \cap C = A \cap (B \cap C) = A \cap B \cap C$$

- **分配法則**

$$(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$$

$$(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$$

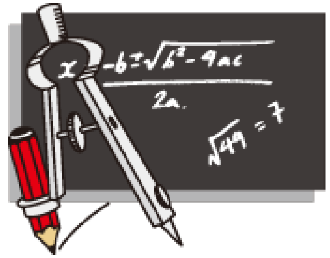
確率の定義



- 事象Aの起こりやすさに対応する量として、次のような性質を有する量P(A)を、確率と呼びます。
  - 事象Aに対してP(A)は実数であり、0≦P(A)≦1が成り立つ。
  - 全事象に対する確率は１である。P(Ω)=1
  - お互いに排反な事象A_1,A_2,.....A_nに対して次が成り立つ。

$$P\left(A_1 \cup A_2 \cup \cdots \cup A_n\right) = P\left(A_1\right) + P\left(A_2\right) + \cdots + P\left(A_n\right)$$

質問



- １から6の数字が書かれたサイコロで、それぞれの目が同じ確率で出るとすると、１の目が出る確率はいくらですか。

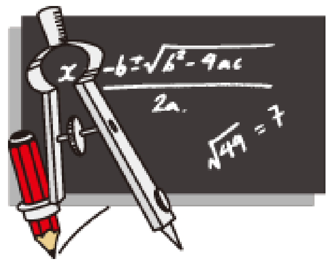
- 次をそれぞれ証明してください

$$P(\phi) = 0$$

$$P(A^c) = 1 - P(A)$$

$$A \subset B \Rightarrow P(A) \leq P(B)$$

確率モデル



- 組み合わせ的な確率の定義
  - 確率現象の結果がN個の場合に分れ、
    どの場合も同程度に起こりやすいとき、
  - （一つの場合が起こる確率）＝１／N

    適用範囲が制限されている。

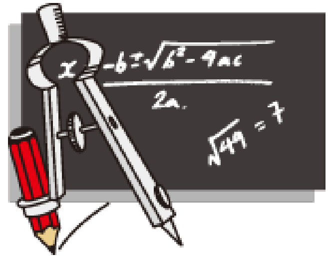
- 頻度による確率の定義
  - 十分多くの観察を繰り返し行ったとき
  - （事象の確率）＝（事象の起こった回数）÷（実験回数）

    確率が個別の現象に依存

- 確率論では、確率そのものを定義しない。
- その代わりに確率が満たすべき条件を公理として与える。

  ➡ 確率モデル

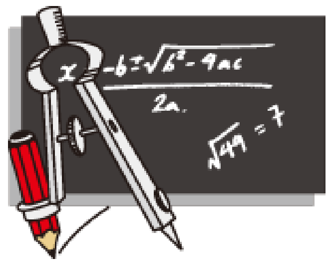
確率の定義



- 事象Aの起こりやすさに対応する量として、次のような性質を有する量P(A)を、確率と呼びます。
  - 事象Aに対してP(A)は実数であり、0≦P(A)≦1が成り立つ。
  - 全事象に対する確率は１である。P(Ω)=1
  - お互いに排反な事象A_1,A_2,.....A_nに対して次が成り立つ。

$$P\left(A_1 \cup A_2 \cup \cdots \cup A_n\right) = P\left(A_1\right) + P\left(A_2\right) + \cdots + P\left(A_n\right)$$

加法定理



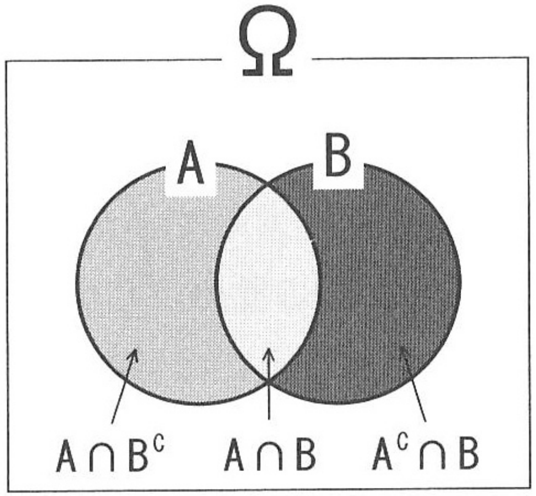
- 和事象の定義から考えて、和事象の確率について以下の関係があることがわかります。

$$P(A \cup B) = P(A \cap B^c) + P(A \cap B) + P(A^c \cap B)$$

$$P(A) = P(A \cap B^c) + P(A \cap B)$$

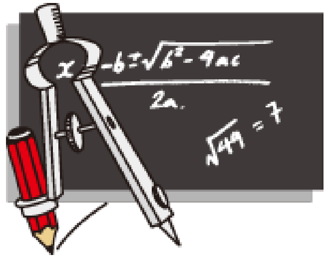
$$P(B) = P(A \cap B) + P(A^c \cap B)$$

$$P(A \cup B) = P(A) + P(B) - P(A \cap B)$$

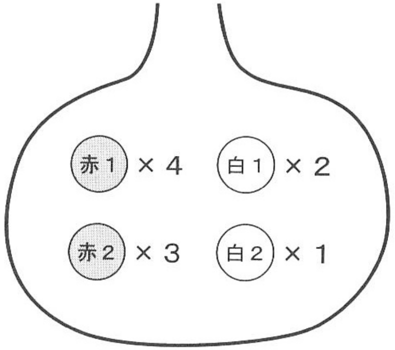


- これを加法定理といいます。

条件付き確率

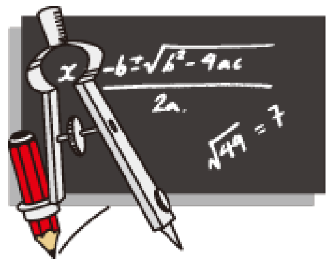


- 次のような例を考えましょう
  - 袋の中に赤玉と白玉が入っている
  - それぞれの玉には数字の１か2が書いてある。
  - 玉を取り出したとき、赤色で１であるとき標本点(赤,1)と表す。
  - 取り出した玉が赤であるという事象は{(赤,1),(赤,2)}
これをA={(赤,*)}と表す。
  - 取り出した玉に１であるという事象は{(赤,1),(白,1)}
これをB={(*,1)}と表す。
  - ここで一つ玉を取り出したとき、
それが赤であったとき、
玉に１と書かれている確率



- これを事象Aのもとで事象Bが起きる条件付き確率といいます

条件付き確率



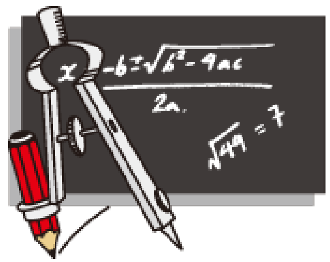
- この条件付き確率は次のように定義されます。

$$P(B|A) = \frac{P(A \cap B)}{P(A)}$$

  - 事象Aが起きた上で事象Bが起きる確率は、両方の事象が同時に起きる確率から事象Aが起きる確率を除いたもの

  - というか、数学的にはこれが定義であって先ほどの説明はその解釈です。
  - 上記のような数を定義すると、これは $0 \le P(B|A) \le 1$ という条件を満たしますので確率として取り扱えます。

乗法定理

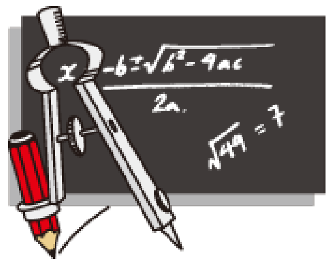


- 変形すると次のように言えます。

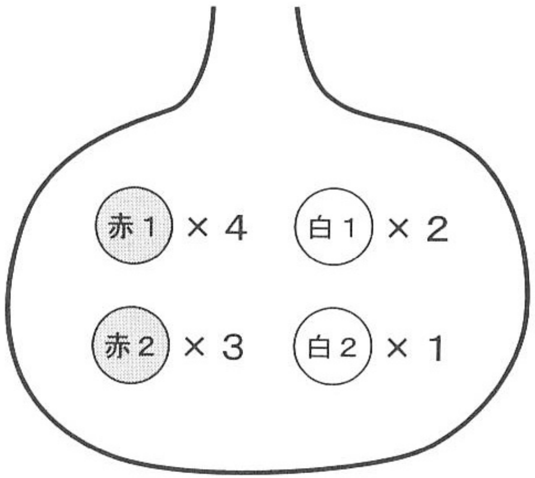
$$P(A \cap B) = P(B|A)P(A)$$

  - 事象Aと事象Bが同時に起きる確率というのは、事象Aが起きたもとで事象Bが起きる確率と、とにかく事象Aが起きる確率の合成
- これを乗法定理といいます。
- これにより積事象の確率を分解することができます。

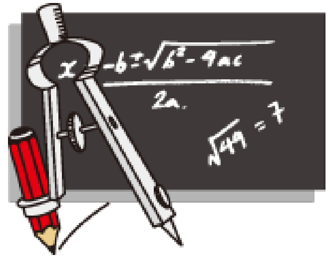
例



- 先ほどの袋から玉を取り出すくじについて図のような例を考えましょう。
- 取り出した玉が赤であったとき、そこに１とかかれている確率はいくらですか。



独立性

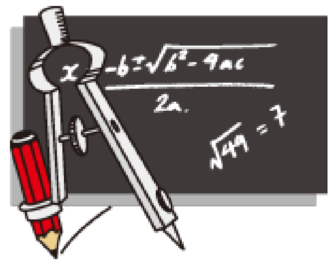


- 次のような例を考えましょう。
  - サイコロを2回振ります。
  - １回目に出る目がiで、2回目にでる目がjである標本点を{(i,j)}とします。
  - 先ほどと同様に１回目がiである事象Aは{(i,*})とし、2回目がjである事象Bは{(*,j)}とします。
  - この時の事象Aのもとで事象Bである条件確立を求めます。

$$P\left(B|A\right)=P\left(\left\{(*,j)\right\}/\left\{(i,*)\right\}\right)=\frac{P\left(\left\{(*,j)\right\}\cap\left\{(i,*)\right\}\right)}{P\left(\left\{(i,*)\right\}\right)}=\frac{P\left(\left\{(i,j)\right\}\right)}{P\left(\left\{(i,*)\right\}\right)}$$

$$=\frac{1/36}{1/6}=\frac{1}{6}$$

独立性



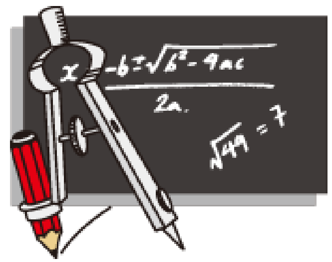
- ここで、$P(\{*,j\}) = 1/6$ ですから

  $P(B|A) = P(B)$ となります。
- このようなとき事象Aと事象Bは独立であるといいます。
- 事象Aがおきても、おきなくても、事象Bがおきる確率とは関係がないということなので、意味から明らかです。
- ちなみに、乗法定理から2つの事象AとBが独立ならば、次の関係が成り立ちます、

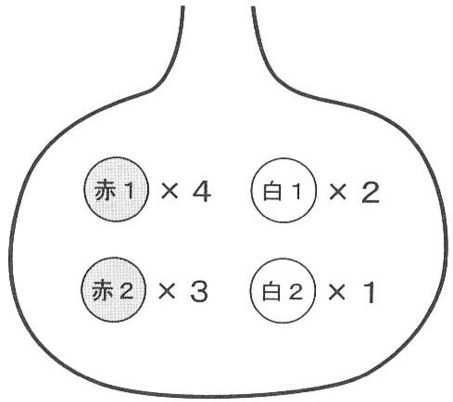
$$P(A \cap B) = P(A)P(B)$$

- これは3つ以上に事象についても成り立ちます。

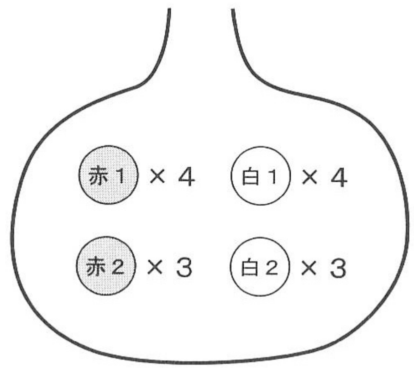
独立性の例題



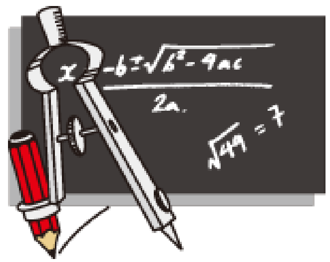
- 先ほどのように袋から玉を一つとり出す例で
- 右の袋から１つ取り出したときに
  {*,1}と{赤,*}は独立ですか？



- 右の袋から１つ取り出したときに
  {*,1}と{赤,*}は独立ですか？

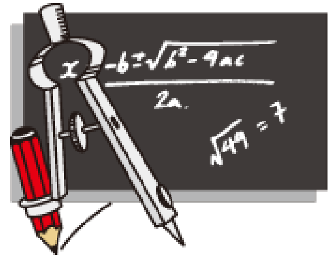


逆方向の条件付き確率



- B1とB2という2つの袋があるとします。
- B1には赤玉3つと白玉1つが入っています。
- B2には赤玉2つと白玉2つが入っています。
- 目の前にどちらかの袋が出されたとき、一つ取り出したら赤玉だった。
- さて目の前の袋がB1であるか、B2であるか推測したいがそれぞれ確率は？

逆方向の条件付き確率



- まず事象B1・B2のもとで事象Aの確率はわかります。

$$P(A|B_1) = 3/4, P(A|B_2) = 1/2$$

- また、単にB1を選ぶかB2を選ぶかの確率は、五分五分でしょう。ですから....

$$P(B_1) = P(B_2) = 1/2$$

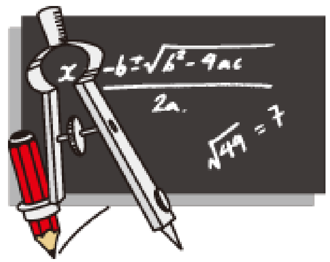
- さてこれらがわかれば、乗法定理から

$$P(A \cap B_1) = P(B_1)P(A|B_1) = 1/2 \times 3/4 = 3/8$$

$$P(A \cap B_2) = P(B_2)P(A|B_2) = 1/2 \times 1/2 = 1/4$$

- とわかります。それなら....

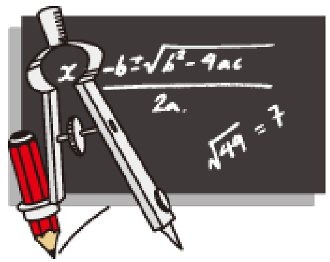
逆方向の条件付き確率



$$
\begin{aligned}
P(A) &= P(A \cap \Omega) \\
&= P\left(A \cap \left(B_1 \cup B_2\right)\right) \\
&= P\left(\left(A \cap B_1\right) \cup \left(A \cap B_2\right)\right) \\
&= P\left(A \cap B_1\right) + P\left(A \cap B_2\right) \\
&= 3/8 + 1/4 = 5/8
\end{aligned}
$$

- つまり、二つの袋のいずれかが提示される確率が等しいならば、赤玉を引く確率は5/8。
- これは理にかなっている。
- さらにそれならば......

逆方向の条件付き確率



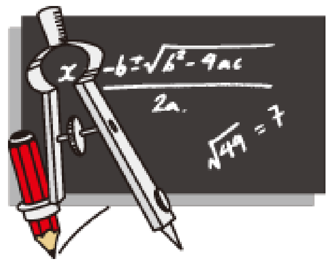
- 求めたい確率は

$$P\left(B_1 | A\right) = \frac{P\left(A \cap B_1\right)}{P\left(A\right)} = \frac{3/8}{5/8} = \frac{3}{5}$$

$$P\left(B_2 | A\right) = \frac{P\left(A \cap B_2\right)}{P\left(A\right)} = \frac{2/8}{5/8} = \frac{2}{5}$$

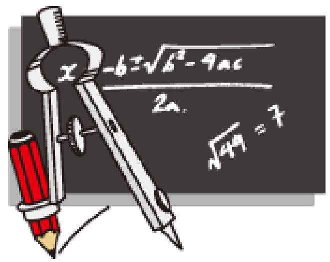
- 二つの袋の赤玉の比率が3対２なのでこれまた理にかなっている。

事前確率と事後確率



- この例で $P(B_1)=P(B_2)=1/2$ は、事象Aがおきる前に推定した確率なので事前確率といいます。
- これに対して $P(A|B_1)=3/4, P(A|B_2)=1/2$ は事象Aの結果を知ったあとでそれぞれの事象がおきる確率なので事後確率といいます。
- つまり、この例では事象Aがおきたことで、事前確率から事後確率に補正したことになります。
- それではこの例をもう少し一般化してみましょう。

全確率の定理



- いくつかの候補となる排反な事象B1,....Ｂｎが定義されたとします。
- なおかつ、事象B1,B2,....Ｂｎが全事象を覆う、つまり

$$B_1 \cup B_2 \cup \ldots\ldots \cup B_n = \bigcup_{i=1}^{n} B_i = \Omega$$

- だとします。
- この時、これらの事象と関係する（独立でない）事象Aが存在して、条件付き確率 $P(A|B_1),\ldots\ldots P(A|B_n)$ がわかるとします。

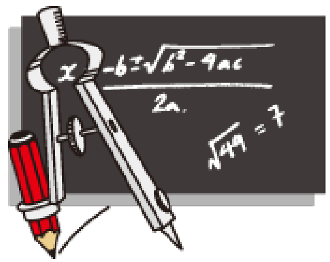
  すると、事象Aがおきる確率を知ることができます。

$$P(A) = P(A\cap\Omega) = P\left(A \cap \bigcup_{i=1}^{n} B_i\right) = P\left(\bigcup_{i=1}^{n}(A\cap B_i)\right)$$

$$= \sum_{i=1}^{n} P(A\cap B_i) = \sum_{i=1}^{n} P(B_i)P(A|B_i)$$

- これを全確率の定理といいます。

ベイズの定理

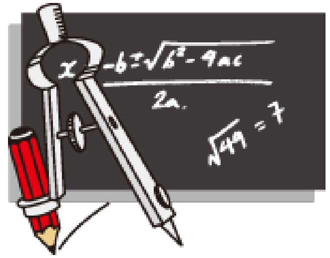


- 事象Aがお互いに排反で全ての場合を覆うn個の原因B1…Bnによって起こるとき、そのうち一つの原因Biによって事象Aがおきる確率は

$$P\left(B_i \middle| A\right) = \frac{P\left(B_i\right)P\left(A \middle| Bi\right)}{\sum_{k=1}^{n} P\left(B_k\right)P\left(A \middle| B_k\right)}$$

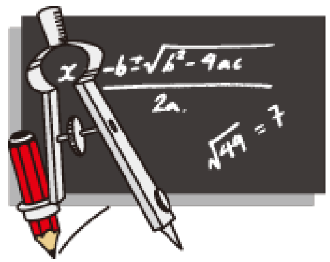
- これをベイズの定理といいます。
- 証明できますか？

例題



- ある電子部品をA,B,C3台の機械で製造していて、各機械の生産量はそれぞれ20%,30%,50%で、不良品のでる確率は5%,3%,2%である。この部品を１個取り出したら不良品であったとき、それが機械Aで製造されたものである確率を求めよ。

まとめ



- 事象、全体事象、空事象、和事象、積事象
- ド・モルガンの法則
- 結合・分配定理、加法定理
- 数学的確率と経験的確率
- 条件付き確率と乗法定理
- 独立性
- 全確率の定理
- ベイズの定理