確率と論理学

竹内泉

論理学

本発表では現代論理学のことを云う

論理学と

- 論理
- 伝統論理学
- 数理論理学

を混同しないように

哲学と数学と論理学

- 哲学:何であるかを問う……概念の探究
- 数学:どうなっているかを問う……構造の探究
- 論理学:どう使われるかを問う……行為の探究

伝統論理学は哲学の一分野
数理論理学は数学の一分野

確率とは何か

これは哲学的設問である

- 数学や論理学からは答は得られない

しかし、この問いに答えるのに

- 内部構造:どうなっているか…数学
- 対外関係:どう使われるか…論理学

は有益であろう

確率と確率論

確率は様々な科学で用いられる
確率論とは確率に関する数学

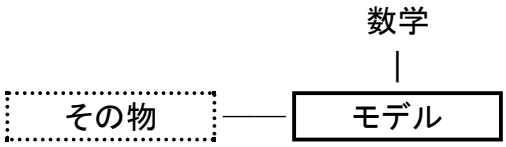
諸科学で確率を用いる際には、確率論を通してそれを用いる
→ 諸科学では確率を用いると確率論を用いるとはほぼ同義
稀に確率を用いず確率論のみを用いる時もある

確率論と諸科学

- 数学…確率論を提供する
- 諸科学…確率論を利用する
    - 量子力学
    - 原子核物理学
    - リスク工学
    - 金融工学
    - 意志決定理論
    - 暗号学
- 論理学…確率論の利用を観察する

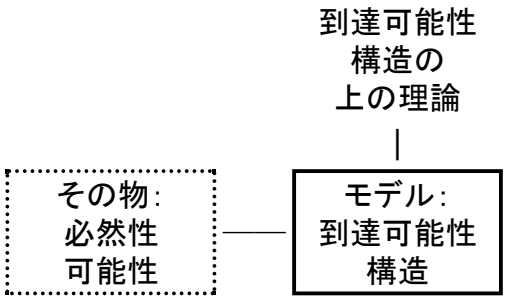
数学とモデル

数学は、ある物を調べる際には、その物ではなくモデルを使ってその構造を調べる



数学とモデル

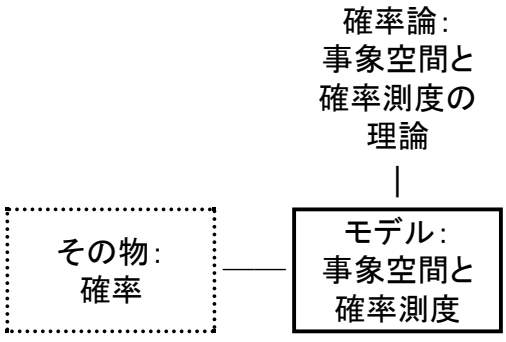
必然性と到達可能性構造の関係



個体同定が議論の俎上にある場合には、よいモデルではない

数学とモデル

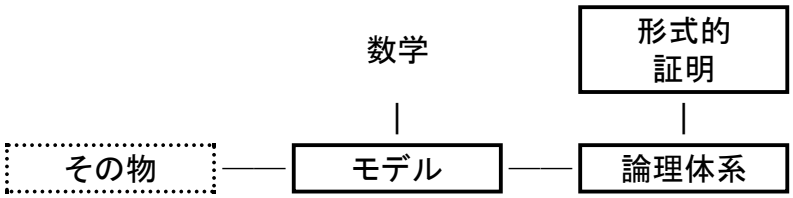
確率と確率論の関係



モデルとしての不都合は発見されていない

数学とモデルと論理学

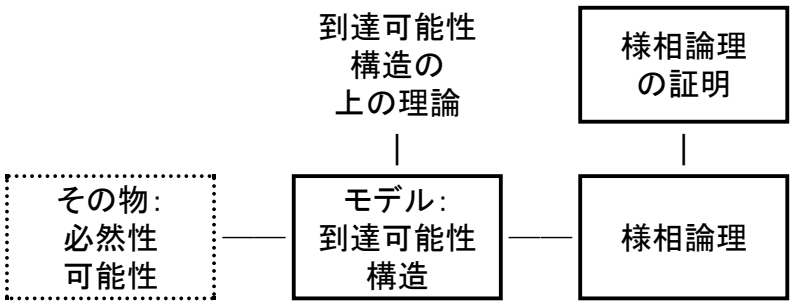
論理学は、形式的論理体系によって理論を模倣する



数学を全て模倣する必要はない
その時注目している特定科学が利用する理論の部分だけ模倣すればよい

数学とモデルと論理学

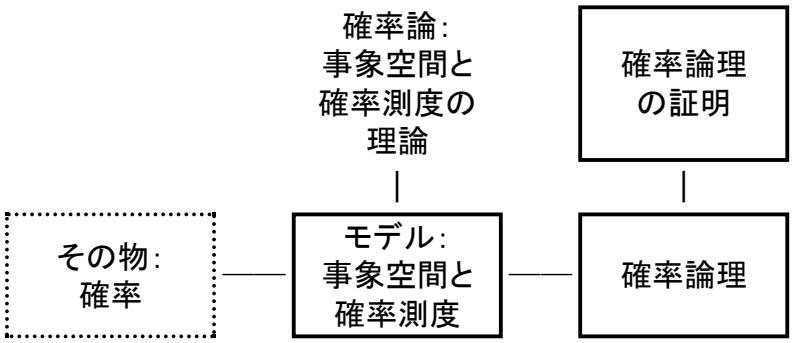
必然性と様相論理の関係



モデルは到達可能性構造でなくともよい

数学とモデルと論理学

確率と確率論と確率論理の関係



諸科学と確率

確率に対しては世界観が二つある

- 世界は決定論的であるが、人間は全てを知り得ない為、確率を用いる
- 世界は決定論的ではなく、確率的に変化する

（普通の）科学は、どちらであるかを語らない

- 唯、量子力学のみは、世界は決定論的ではない、と積極的に主張する

論語「子不語怪力乱神」

確率論と諸科学と論理学

- 数学…確率論を提供する
- 諸科学…確率論を利用する
  - 量子力学
  - 原子核物理学
  - リスク工学
  - 金融工学
  - 意志決定理論←※
  - 暗号学←※
- 論理学…確率論の利用を観察する

※の学問分野では論理学が利用されている

確率の暗号学への応用に於ける論理学の役割

学術的価値

- 暗黙の推論の明示化

産業的価値

- 証明の流通
  - 安全性の証明は流通させる必要がある
  - 確率論の証明は難解で、その侭では流通しない
  - 形式的証明ならば機械検証が可能である

例題

m の値を確率変数 x で隠蔽する

- m∈{0,1} は隠したい値
- x∈{0,1} は確率変数
- y=m⊕x

y を知っただけで m を推測できるか

暗黙の推論

y=m⊕x
y を知っただけで m を推測できるか

- x=1 の確率が p>1/2 なら m=¬y という推測は確率 p>1/2 で当たる
- x=0 の確率が p>1/2 なら m=z という推測は確率 p>1/2 で当たる
- x=1 の確率が丁度 1/2 なら、y から m の値を推測することは出来ない

形式化

p が成り立つ (p=1 である) 確率が

- 1/2 より大きいことを Mp と書く
- 丁度 1/2 であることを Hp と書く
- 0 ではないことを Ep と書く

p と q、r、…が独立であることを I(p;q,r,…) と書く

公理化

公理として古典論理の他に以下を置く

- ¬E0
- p⇔q がトートロジーなら |– Mp⇔Mq 、|– Ep⇔Eq
- Mp, Mq |– E(p·q)
- I(p;x,y,...), Hp |– M(p·q+¬p·r) ⇔ M(p·r+¬p·q)
  但し q、r には x、y、…しか現れない

推測できないことの形式化

y から m を推測しようとする函数を f( ) と書く
I(x;m), Hx |– ¬M(m⇔f(m⊕x))
を導出する

導出

m⇔f(m⊕x)
= x·m·(1⇔f(1⊕1)) + x·¬m·(0⇔f(0⊕1))
+ ¬x·m·(1⇔f(1⊕0)) + ¬x·¬m·(0⇔f(0⊕0))
= x·(f(0)·m+f(1)·¬m) + ¬x·(f(0)·¬m+f(1)·m)

故に

M(m⇔f(m⊕x)) |– M(x·(f(0)·m+f(1)·¬m) + ¬x·(f(0)·¬m+f(1)·m))

公理により

I(x;m), Hx, M(x·(f(0)·m+f(1)·¬m) + ¬x·(f(0)·¬m+f(1)·m))
|– M(x·(f(0)·¬m+f(1)·m) + ¬x·(f(0)·m+f(1)·¬m))

導出

故に

I(x;m), Hx, M(m⇔f(m⊕x))
|– M(x·(f(0)·¬m+f(1)·m) + ¬x·(f(0)·m+f(1)·¬m))

公理により

I(x;m), Hx, M(m⇔f(m⊕x))
|– M(x·(f(0)·m+f(1)·¬m) + ¬x·(f(0)·¬m+f(1)·m))
· M(x·(f(0)·¬m+f(1)·m) + ¬x·(f(0)·m+f(1)·¬m))
|– E((x·(f(0)·m+f(1)·¬m) + ¬x·(f(0)·¬m+f(1)·m))
· (x·(f(0)·¬m+f(1)·m) + ¬x·(f(0)·m+f(1)·¬m)))
|– E0 |– 0

導出

故に

$I(x;m), Hx \vdash \neg M(m \Leftrightarrow f(m \oplus x))$