

ランダムはどこにあるか？

大人のための数学講座 in 京都

2012年10月13日 京都大学

宮部賢志

京都大学 数理解析研究所

自己紹介

❖ 宮部賢志（みやべけんし）

❖ 岐阜県岐阜市出身

❖ 研究分野

アルゴリズム的ランダムネス，
ゲーム論的確率論，計算可能解析，
アルゴリズム的確率，など

今日のテーマ

❖サイコロはランダムか？

話の流れ

- ❖ 20世紀における
アルゴリズム的ランダムネスの理論
- ❖ 19世紀における
ランダムネスの理論誕生前夜

ランダムを定義しよう

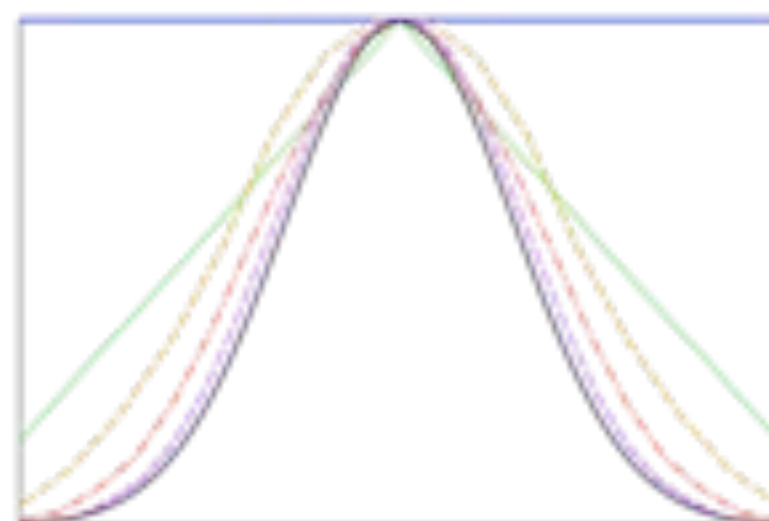
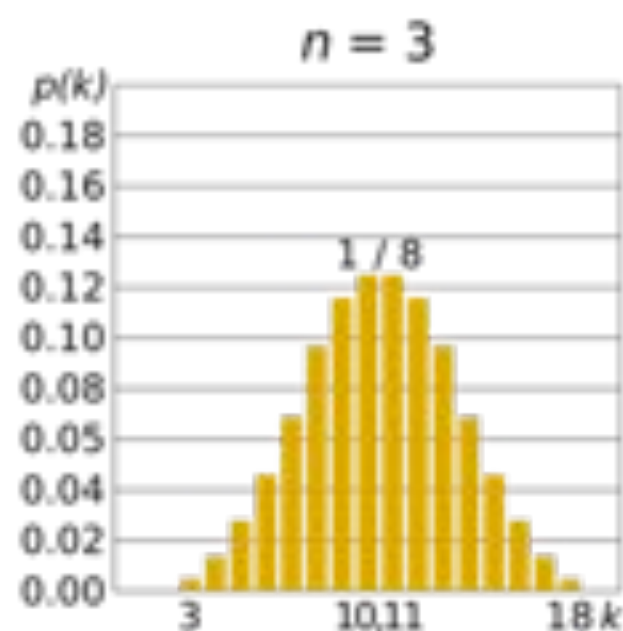
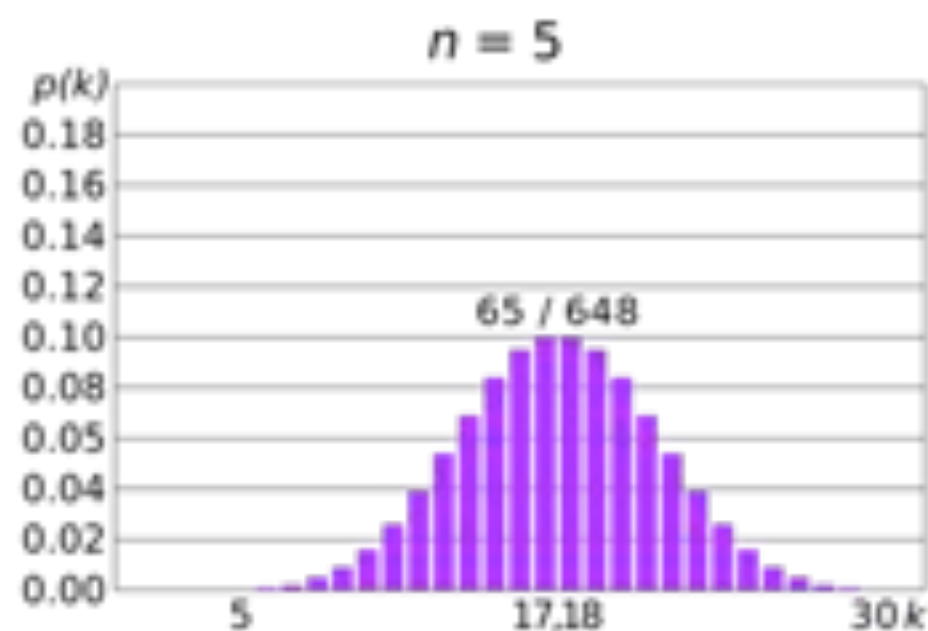
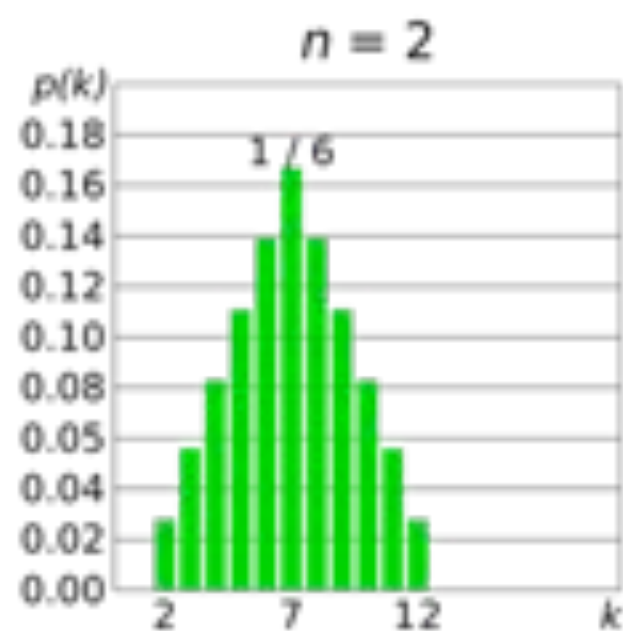
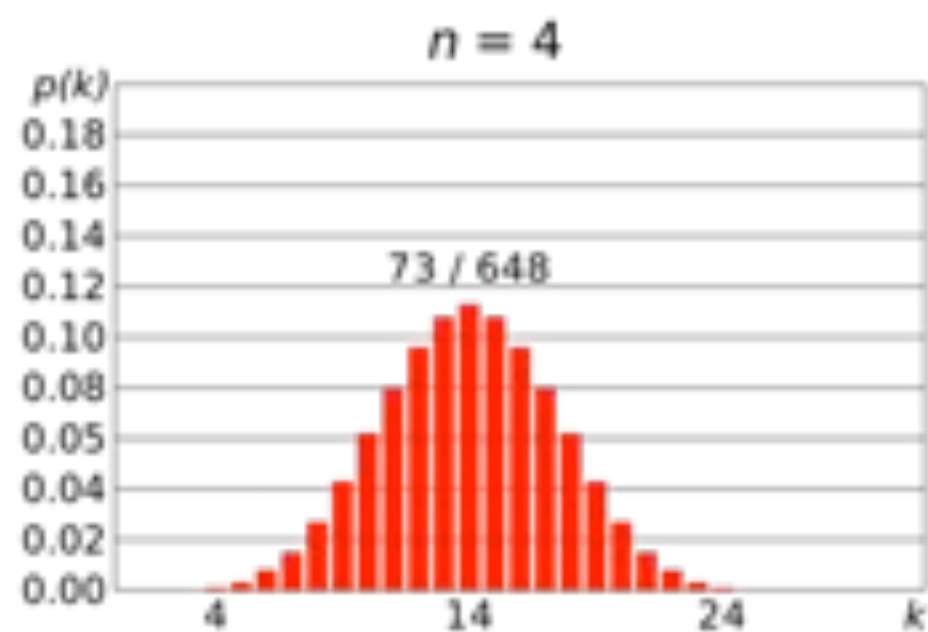
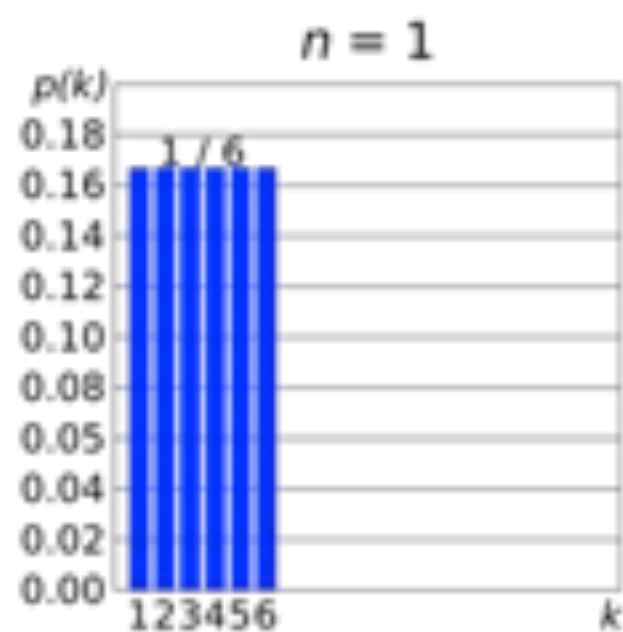
大数の法則

~~~~~

大数の法則 (J. Bernoulli 1713)

非常に多くの回数コインを投げると，表と裏の相対頻度は非常に高い確率で  $\frac{1}{2}$  に近い.





# 大数の強法則

大数の強法則 (Borel 1909)

無限回コインを投げると、表と裏の相対頻度は確率 1 で  $\frac{1}{2}$  に収束する.

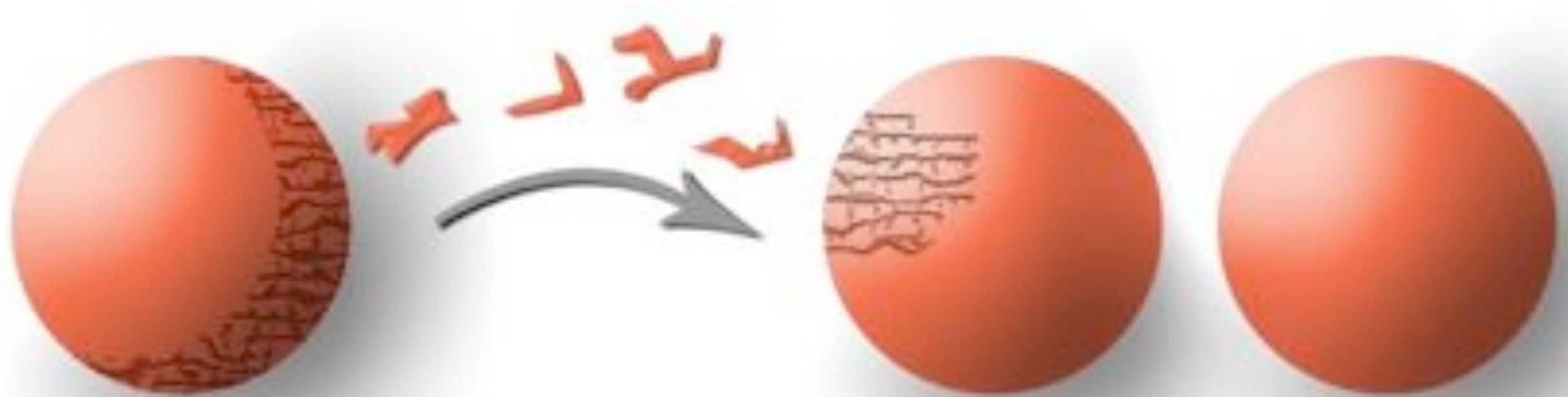
大数の弱法則 (J. Bernoulli 1713)

非常に多くの回数コインを投げると、表と裏の相対頻度は非常に高い確率で  $\frac{1}{2}$  に近い.

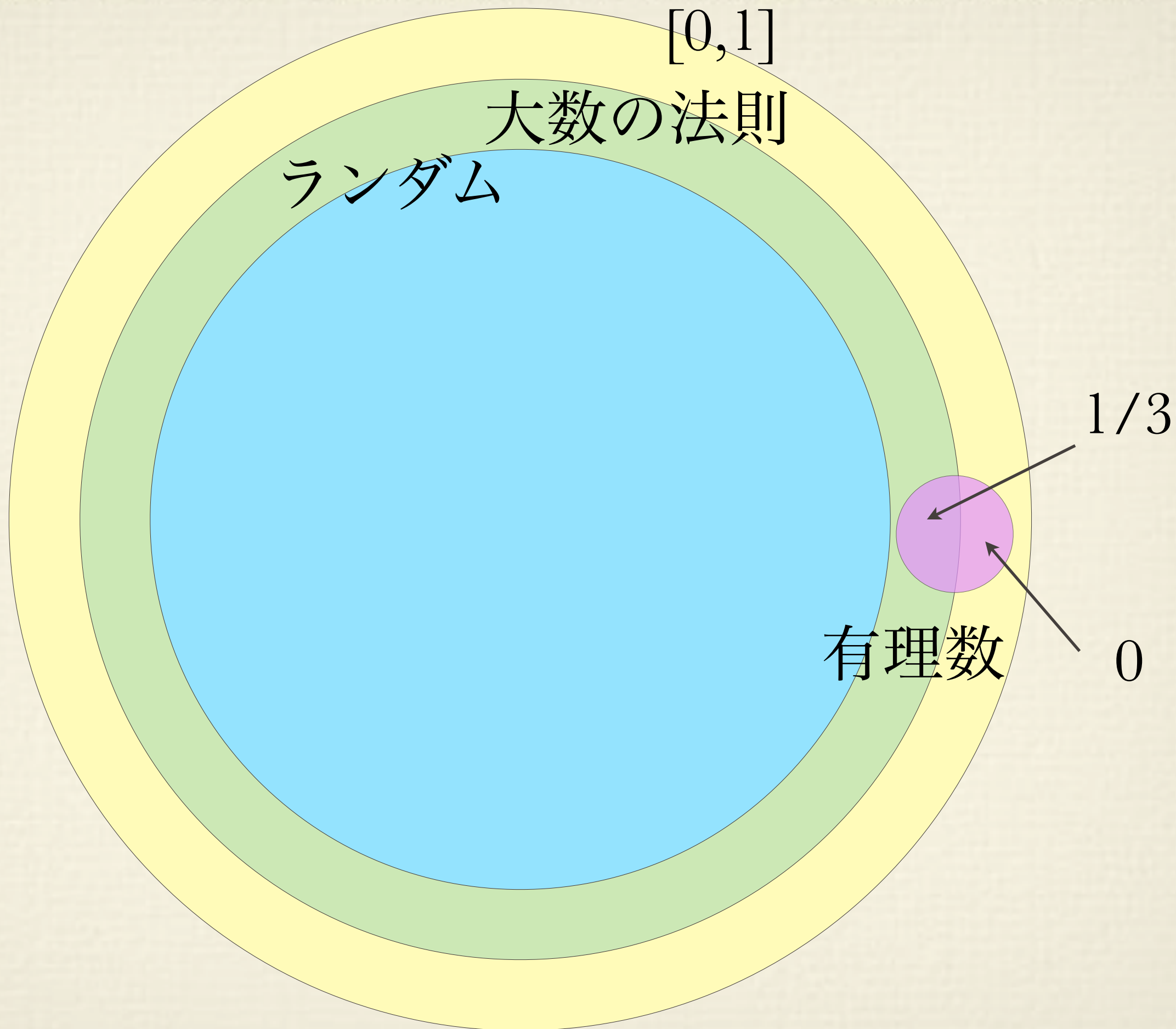


# 測度論

# Banach-Tarski paradox



球を3次元空間内で、有限個の部分に分割し、  
それらを回転・平行移動操作のみを使って  
うまく組み替えることで、  
元の球と同じ半径の球を2つ作ることができる





# von Mises

---

- ❖ どんな適当な部分列をとっても極限頻度が $1/2$ に収束するものをcollectiveと呼ぼう
- ❖ 1919年

[illegible]

-  111111111111111111111111111111...  
 010101010101010101010101010101010101010101...  
 01011101011101010101111111111111110111...  
 001001000011111101101010100010001000...



# Church-Turingの提唱

---

- ❖ 「計算可能」
  - = 「帰納的関数で計算可能」
  - = 「Turingマシンで計算可能」
- ❖ 「適当な」部分列を「計算可能に選択された」部分列，にしてみたら？



# Villeの反例

---

- ❖ 重複対数の法則を満たさないcollectiveが存在する
- ❖ 1939年

そもそもランダムとは？

[illegible]

- ❖ 無作為に選ぶ=>典型性
- ❖ 偶然にまかせる=>予測不可能性
- ❖ でたらめ, 規則がない=>圧縮不可能性



# 圧縮できない列がある

~~~~~

問題

どんな優秀な圧縮プログラム

(例えばzip,lzh,cab,rar,7z) であってでも,
圧縮できないデータが存在することを
証明せよ.

定義

(圧縮) 関数 $C : 2^* \rightarrow 2^*$ が可逆であるとは、すべての $\sigma \in 2^*$ に対して、

$$U \circ C(\sigma) = \sigma$$

となるような関数 $U : 2^* \rightarrow 2^*$ が存在することを言う.

σ が C で圧縮できるとは、

$$C(\sigma) < |\sigma|$$

となることを言う.

定式化

~~~~~

## 問題

任意の可逆圧縮関数  $C$  に対して，少なくとも 1 文字は圧縮できるならば，ある  $\sigma \in 2^*$  が存在して，

$$C(\sigma) \geq |\sigma| + 1$$

となることを示せ．



# 解答 1

ある可逆圧縮関数  $C : 2^* \rightarrow 2^*$  があって,  $\tau \in 2^*$  は  $C$  で圧縮できるとする. 更にすべての  $\sigma \in 2^*$  に対して,

$$C(\sigma) \leq |\sigma|$$

となるとしよう. 今,  $\{\tau_n\}$  を  $\tau_0 = \tau$  および

$$\tau_{n+1} = C(\tau_n)$$

で定義する.

$$U(\tau_{n+1}) = U \circ C(\tau_n) = \tau_n$$

より, 任意の  $n$  で  $\tau_{n+1} \neq \tau_n$ . しかしこれは起こり得ない.

# 解答 2

~~~~~

ある可逆圧縮関数 $C : 2^* \rightarrow 2^*$ があって, $\tau \in 2^*$ は C で圧縮できるとする. 長さ $|\tau|$ 未満の文字列の数は,

$$\sum_{n=0}^{|\tau|-1} 2^n = 1 + 2 + \cdots + 2^{|\tau|-1} = 2^{|\tau|} - 1$$

であり, それらと τ を圧縮した文字列の長さがすべて $|\tau|$ 未満であるということは起こり得ない.

Kolmogorov複雑性

~~~~~

$f : \subseteq 2^* \rightarrow 2^*$  を関数とする.

$\sigma \in 2^*$  の  $f$  に関する **Kolmogorov 複雑性**を,

$$K_f(\sigma) = \min\{|\tau| : f(\tau) = \sigma\}$$

で定義する.

.



# 万能マシン

次を満たすような接頭万能マシン  $U$  が存在する.

任意の接頭計算可能関数  $f$  に対して, ある文字列  $\rho_f$  が存在して, すべての  $\sigma$  に対して,

$$U(\rho_f \sigma) = f(\sigma).$$

これより,

$$K_U(\tau) \leq K_f(\tau) + |\rho_f|.$$

今後は,  $K = K_U$  とし, これを Kolmogorov 複雑性と呼ぶ.

# 接頭関数

$A \subseteq 2^*$  が**接頭** (prefix-free) もしくは**反鎖** (anti-chain) であるとは,

$$\sigma, \tau \in A \text{ ならば } \sigma \neq \tau$$

を満たすことを言う.

関数  $f : \subseteq 2^* \rightarrow 2^*$  が**接頭**であるとは, その定義域が prefix-free であることを言う.

接頭関数ならば, プログラムがどこで終わりののかが分かる.



# 基本的な性質 1

任意の  $\sigma$  に対して,

$$K(\sigma) \leq |\sigma| + K(|\sigma|).$$

任意の  $c$  に対して, 十分に長い  $c$  圧縮不可能な文字列が存在する. すなわち,

$$K(\sigma) \geq |\sigma| - c.$$

任意の  $c$  に対して, 十分に長い文字列で次をみたすものが存在する. すなわち,

$$K(\sigma) \geq |\sigma| + K(|\sigma|) - c.$$



# 証明

次のような接頭計算可能関数  $f$  を考える. 入力  $\sigma$  に対し,  
 $U(\sigma_1) \downarrow$  となるような  $\sigma_1 \preceq \sigma$  を探す. もし見つければ,  $\sigma = \sigma_1 \sigma_2$  とおいて,

$$|\sigma_2| = |U(\sigma_1)|$$

であるときには,  $f(\sigma) = \sigma_2$  とする.

$U$  が接頭関数なので,  $f$  も接頭関数. 任意の  $\sigma$  に対し,

$$K_f(\sigma) \leq K(|\sigma|) + |\sigma|.$$

# 基本的な性質 2

Kraft-Chaitin の不等式

$$\sum_{\sigma \in 2^*} 2^{-K(\sigma)} \leq 1.$$

Counting Theorem

$$\max\{K(\sigma) : |\sigma| = n\} = n + K(n) \pm O(1).$$

一般に,

$$|\{\sigma : |\sigma| = n, K(\sigma) \leq n + K(n) - r\}| \leq 2^{n-r+O(1)}.$$



# Martin-Löf ランダムネス

~~~~~

次のような集合を考える.

$$R = \{A \in 2^\omega : (\exists c)(\forall n)K(A \upharpoonright n) > n - c\}.$$

この時,

$$\mu(R) = 1.$$

この集合に含まれる列を **Martin-Löf ランダムな列** と呼ぶ.

MLランダムネスの同値性

- ❖ 典型性 $\Rightarrow$ Martin-Löf 1966
- ❖ 予測不可能性 $\Rightarrow$ Schnorr 1971
- ❖ 圧縮不可能性 $\Rightarrow$ Schnorr 1973, Levin 1973,
Chaitin 1975

停止確率

~~~~~

定義 (停止確率, Halting probability)

$$\Omega_U = \sum_{U(\sigma) \downarrow} 2^{-|\sigma|} < 1.$$

定理 (Chaitin)

$U$  が接頭万能マシンであるとき,  $\Omega_U$  は ML ランダムである.



[illegible]

ある万能接頭マシンの停止確率の最初の文字列

$$\Omega_{U_2} = 0.0000000100000001000000110001000001$$
$$1010001111110010111011101000001$$
$$0000 \dots$$

by Calude et al. (2002)

•



ランダムは  
どこにあるか

---

# ラプラスの悪魔

~~~~~

- ❖ もしもある瞬間における全ての物質の力学的状態と力を知ることができ、かつもしもそれらのデータを解析できるだけの能力の知性が存在するとすれば、この知性にとっては、不確実なことは何もなくなり、その目には未来も（過去同様に）全て見えているであろう。『確率の解析的理論』（1812）

プロイセン統計局(1805)

[illegible]

❖ 多数のさまざまな組み合わせから起きる出来事には、多数の偶然の結果として得られた観察によって、周期的な繰り返しや、一定の割合が見られるのである。 スタール

(1796)

法則

~~~~~

- ❖ イギリス－法則を，それ自体所与の事実として考える．彼らの思考には法則が個人の意思の産物であるという含みがある．
- ❖ ドイツ－法則を，慣習や言語と同じレベルの社会の産物と見なした．固定されず，進化と変化のうちにある．
- ❖ 19世紀終わりの『大百科事典』の「法則」の項



# 2つの確率

~~~~~

主観確率	信念の度合い	probability
客観確率	性質による傾向	chance

ポアソンの検定と信頼性測定

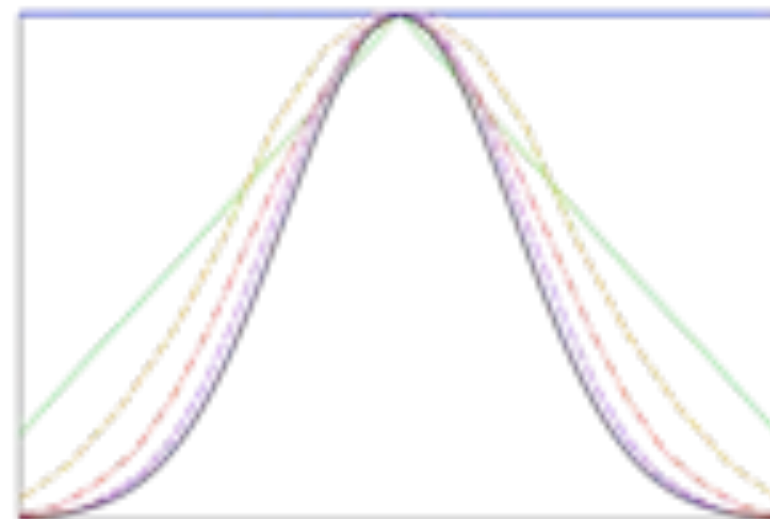
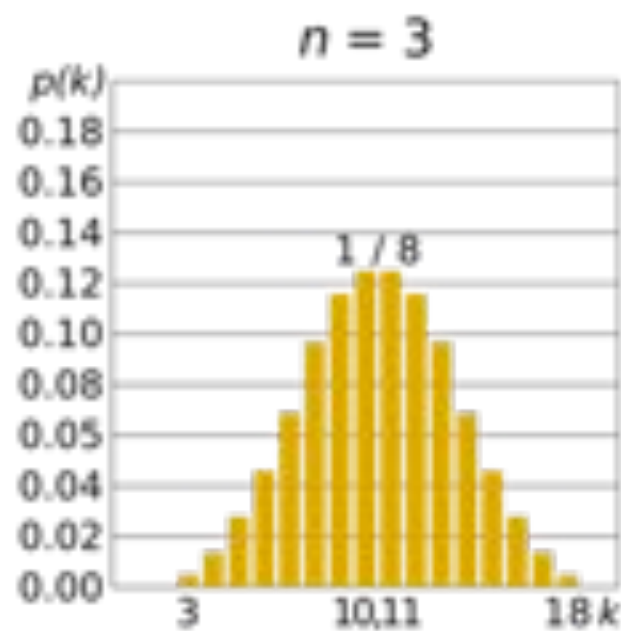
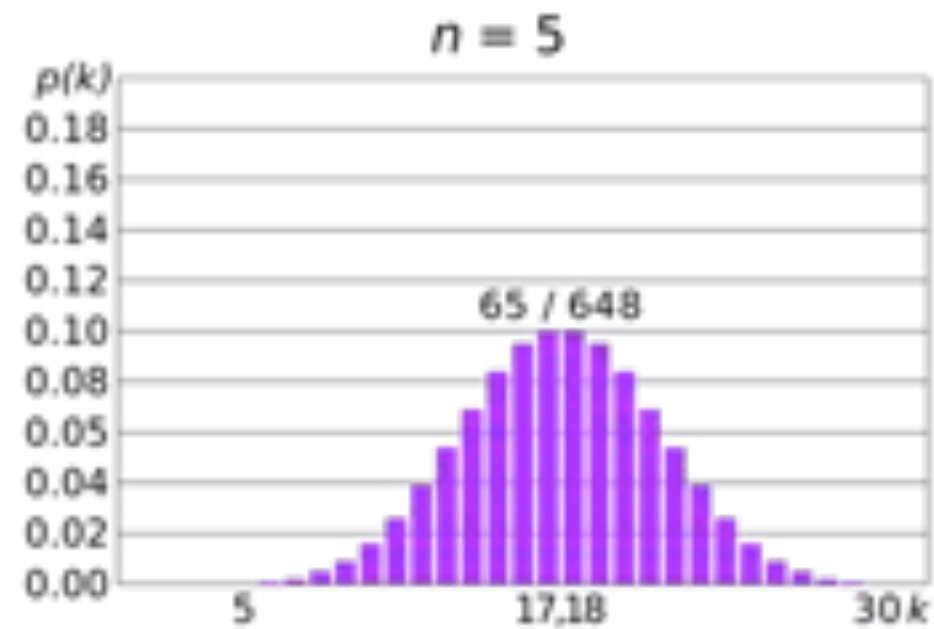
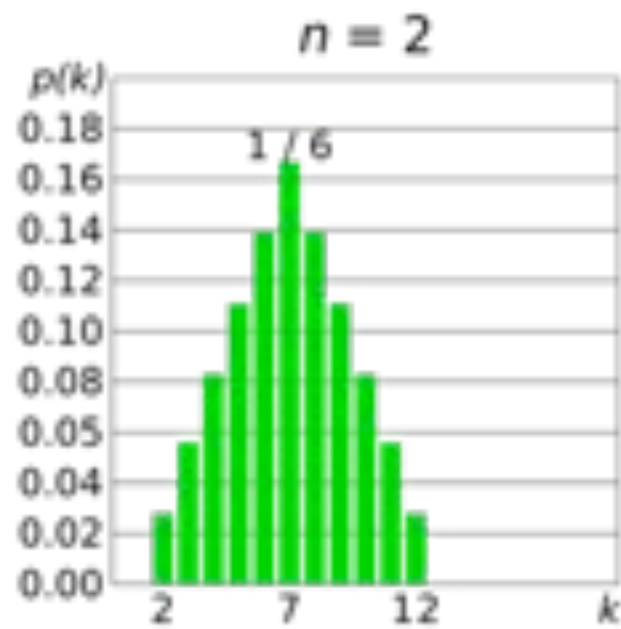
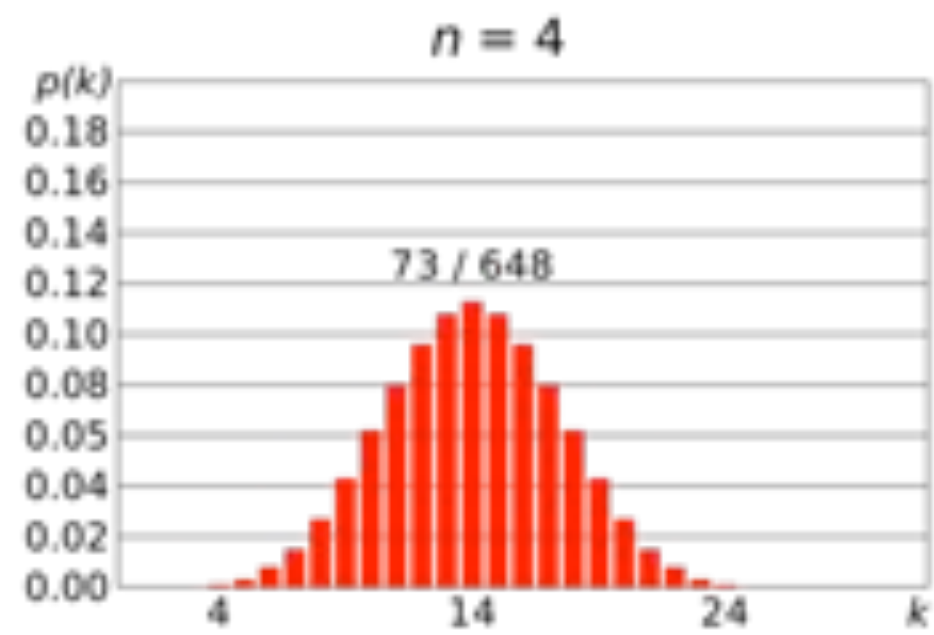
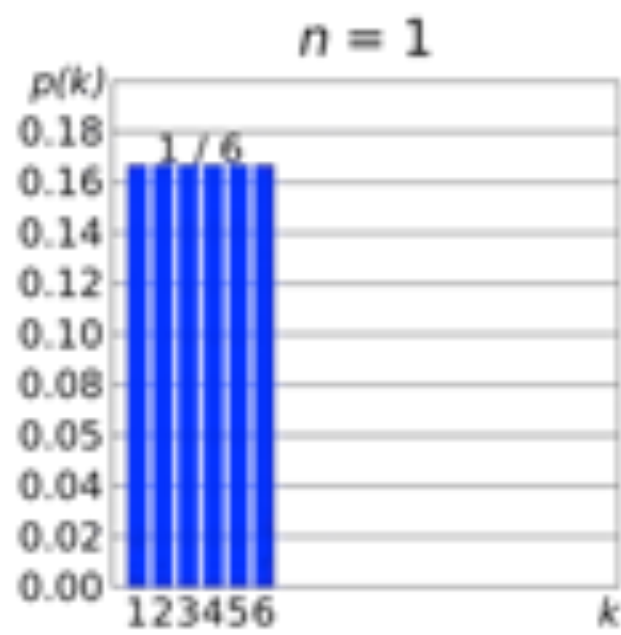
- ❖ 陪審員の信頼性を「モデル化」する
 - 客観確率
- ❖ その信頼性をデータから「推測」する
 - 客観確率についての主観確率

大数の法則

- ❖ 大数の法則
- ❖ ポアソンの大数の法則(1830s)
- ❖ ポアソンの少数の法則

平均人

- ❖ 兵士の胸囲の分布
- ❖ 二項分布
- ❖ ケトレ(1830s)



独立した微小な原因

- ❖ 独立した微小な原因
- ❖ コイン投げの繰り返しで二項分布を得る
- ❖ 測定誤差
- ❖ 自殺と犯罪における原因リスト
- ❖ 様々な原因が兵士の胸囲を決定している

統計的運命論

- ❖ 「恐ろしいほどの正確さで犯罪が再生産されている」
- ❖ 「我々は何人が他人の血で手を汚し，何人が貨幣偽造者になり，何人が毒殺者となるかを，将来の出生や死亡を前もって計算できるのと同じように，あらかじめ知ることができるのである」
- ❖ 「国家予算案よりもはるかに規則正しい，断頭台・徒刑場・刑務所用の支出」
- ❖ ケトレ(1829,1832)

自由意志

- ❖ 「自由意志はいまではまるで理論の中にしか存在していないかのように思われる」
ケトレ(1936)

「決定論」の出現

- ❖ 異なった行動の間でなされる選択は、あらゆる場合に、心理的条件その他の諸条件によってすべて説明されうる。（18世紀末）
- ❖ 生起するあらゆる物事は因果の連鎖を形成する。（1850-1870年代）

社会科学の決定論

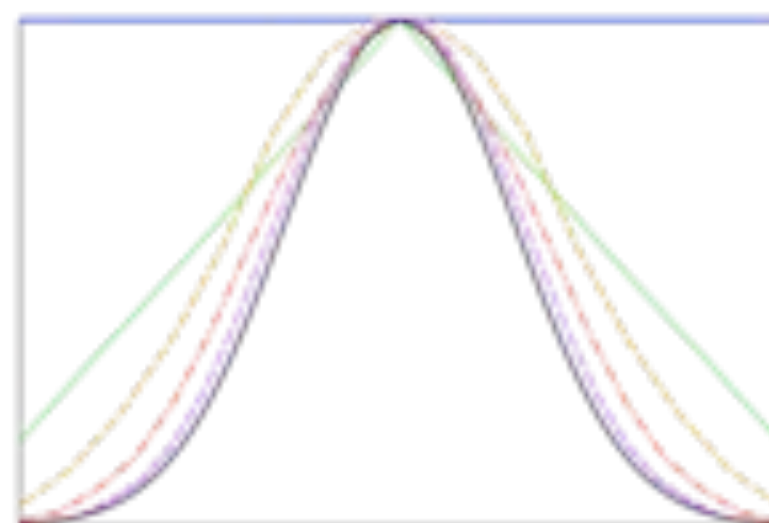
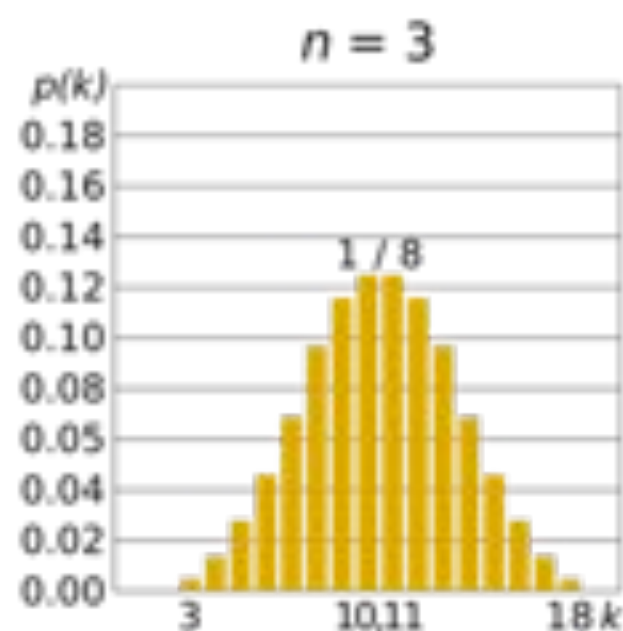
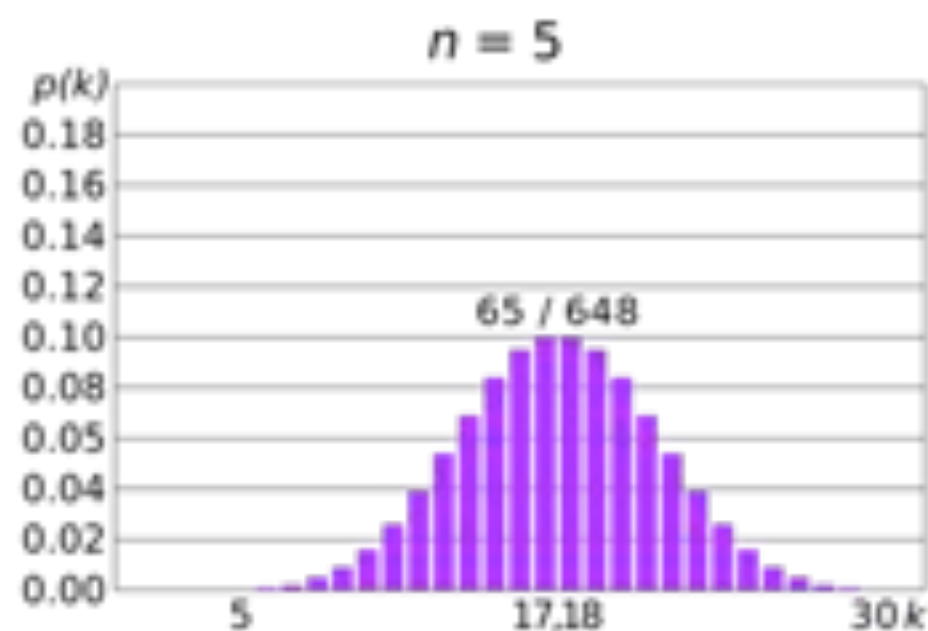
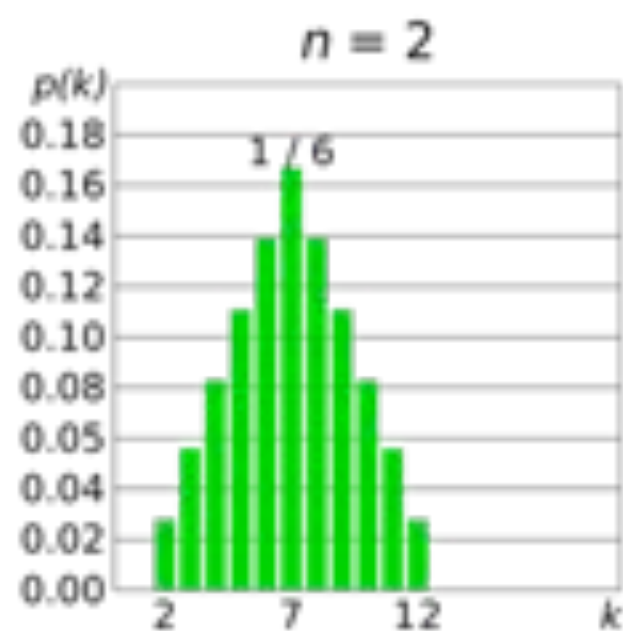
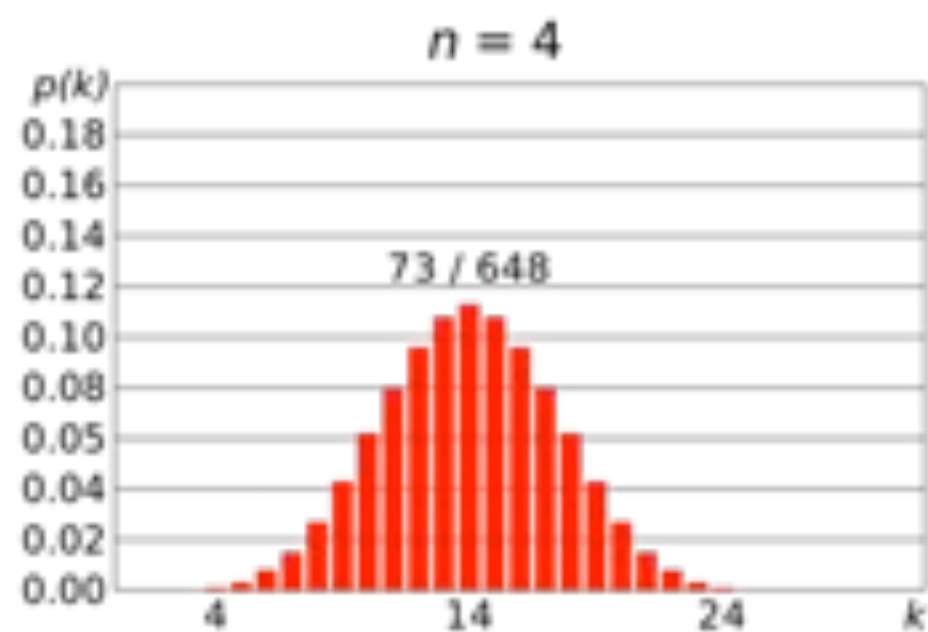
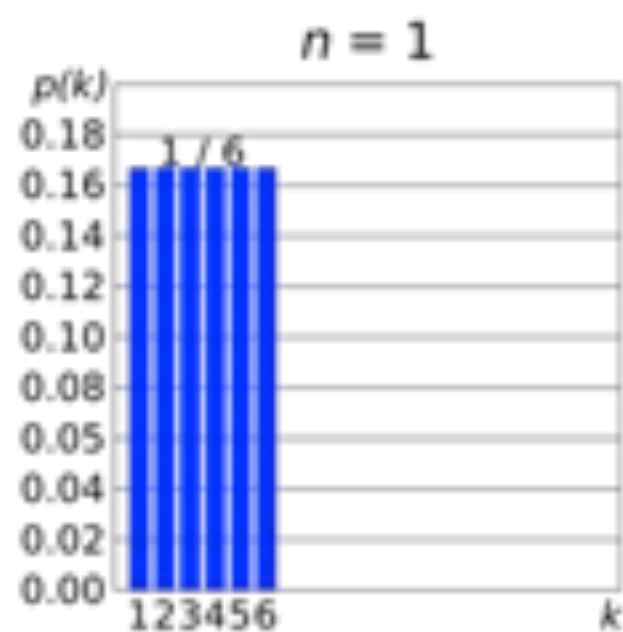
- ❖ 「ある人の人生の一時間を取り出せば，人体測定学の織天使はその人にこれまで起きたことすべてを，またこれから起こるであろうことすべてを計算できるだろう」
コリンズ（1871）

自由意志の復活

- ❖ Kolmogorovによる公理主義的確率論
- ❖ 量子力学

統計法則の自律性

- ❖ 「ある家系における凡庸さへの回帰という現象は、生物の特徴が標準的な統計法則である誤差法則に従って分布するという事実から推論できる。」 ゴルトン



中心極限定理

定理 (中心極限定理)

独立同分布の確率変数列 $\{X_n\}$ に対して, $m = E(X_n)$, $v = \text{Var}(X_n)$ とおく.

$$Z_n = \frac{1}{\sqrt{n}} \sum_{k=1}^n (X_k - m)$$

とおくと, Z_n は, 平均値 0, 分散 v の正規分布に従う確率変数 Z に法則収束する.

収束の概念たち

X_n が X に**概収束** (almost sure convergence) するとは,

$$P\left(\lim_{n \rightarrow \infty} X_n = X\right) = 1$$

となることをいう.

任意の $f \in C_b(\mathbb{R})$ に対して,

$$\lim_{n \rightarrow \infty} E(f(X_n)) = E(f(X))$$

が成立するとき, X_n は X に**法則収束** (convergence in law) するという.

確率の頻度論 1

~~~~~

- ❖ 「確率は心に感じるものであり，環境に本来的に備わっている属性ではない．」 De Morgan (1838)
- ❖ 確率論とは「我々の，一つの命題に対する信念の大きさ（その命題と関係している他の諸命題についての我々の信念の大きさによりさまざまでありうる）が従っている規則を考察することである．」

De Morgan (1847)



# 確率の頻度論 2

~~~~~

- ❖ 頻度計算における「根本概念」は，「個々の規則性と集計されたものの規則性を結びつける」系列 (series) という概念である．確率は系列として考えなければ無意味である．いかなる確率も系列にのみ関連づけるべきである．ある出来事的确率は，系列におけるその相対頻度に他ならない．Venn (1866)

確率の頻度論 3

- ❖ 頻度論から傾向説へ. パース(1890s)
- ❖ ネイマン, ピアソンの信頼区間と仮説検定の理論(1930s)

Kolmogorov

~~~~~

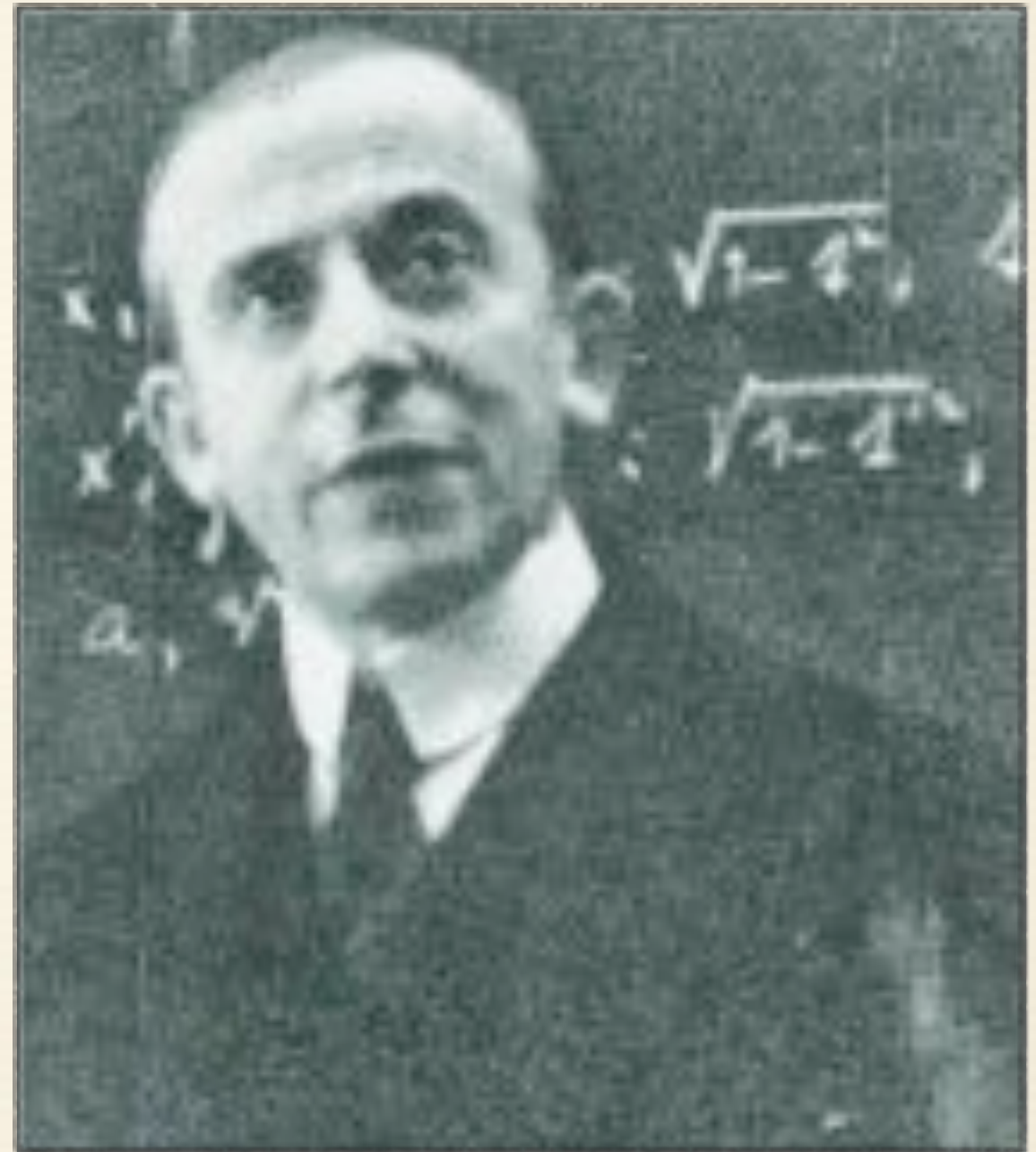
- ❖ Kolmogorov (1903-1987)
- ❖ ロシアの数学者
- ❖ 確率論,  
位相幾何学,  
アルゴリズム情報理論



# von Mises (1883-1953)

---

- ❖ von Mises (1883-1953)
- ❖ 1919年の論文に始まり,  
確率の頻度説の数学的定  
式化を試みた





# von Misesの理論要約

---

- ❖ 「まずCollectiveありき，そして確率がある．」
- ❖ ランダムな概念は，確率が定義できるための条件として使われている．

# Martin-Löf

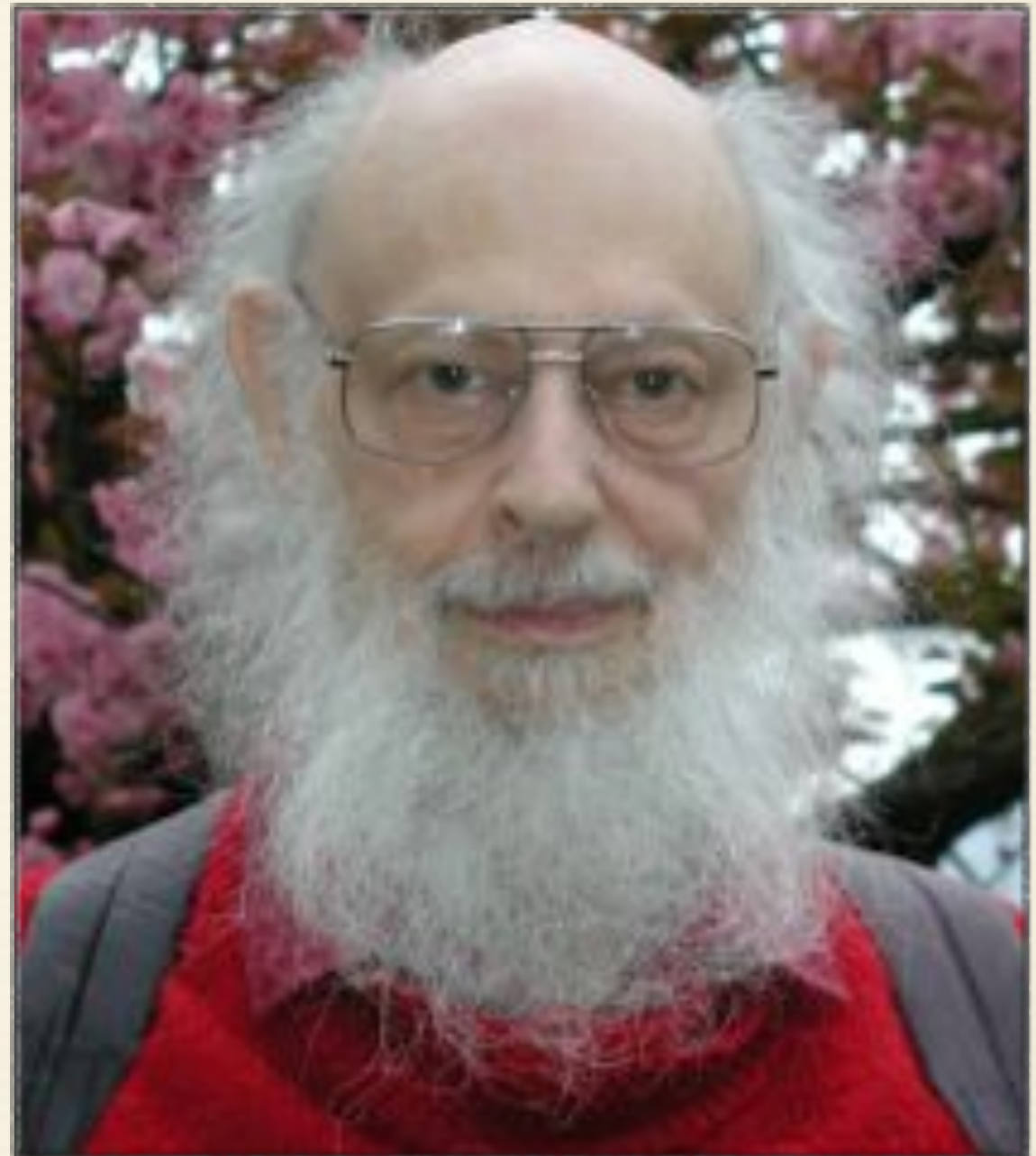
~~~~~

- ❖ Martin-Löf (1942-)
- ❖ 直観主義型理論



Solomonoff

- ❖ Solomonoff (1926-2009)
- ❖ algorithmic probability,
algorithmic information
theory
- ❖ artificial intelligence based
on machine learning



統計の立場から

~~~~~

|                  |                    |                     |
|------------------|--------------------|---------------------|
| 一般的に考えられている立場    | 中心人物               | ランダムネスから見ると？        |
| 頻度説              | Neyman,<br>Pearson | 計算可能性として頻度のみを考慮している |
| 相対頻度に基礎を置く信頼性の尺度 | Fisher             |                     |
| 主観説              | Bayesian           | 計算可能性が考慮されていない      |



# 解釈

---

- ❖ Epicurus (B.C.341?-)  
“If more than one theory is consistent with the data, keep them all.”
- ❖ William of Ockham (1288-1348)  
“Keep the simplest theory consistent with the observations.”
- ❖ 2つの方法の組み合わせ

# ウェルドンのサイコロ

---

- ❖ 1894年
- ❖ “Ordinary dice do not follow the rules usually laid down for them in treatises on probability, because the pips are cut out on the faces, and the fives and sixes are thus more frequent than aces or deuces. This point was demonstrated by W. F. R. Weldon in 25,000 throws of 12 ordinary dice.” Pearson