ランダムネスの源を求めて
—計算の視点から

大阪大学大学院理学研究科名誉教授
杉田　洋

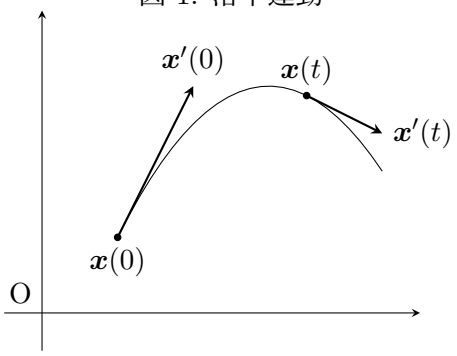
「コルモゴロフのランダムネスの定義というのがあるんです．x がランダムであるとは，x を記述するのに x 自身より短い記述法がないことをいうんだそうです」 大学院生だった頃のある日，セミナーの後で W 先生がこう仰いました．ランダムネスって数学で定義できるんだ... 私はとても驚きました．

英単語 “random” のコアイメージは「考えを挟まないこと」だそうです．無作為ということですね．この講演の主な目的は，この “random” のコアイメージと W 先生の仰ったコルモゴロフのランダムネスの定義が，どんなふうに結び付くのかをお話することです．そして最後に，ランダムネスと確率論の基本的な関係について少しお話します．

1　ラプラスのランダムネス

1812 年，ラプラスは「確率の解析的理論」を著します．その本の中でラプラスは「偶然は存在しない」と述べています．ニュートン力学の大成功を見て当時のヨーロッパの科学者たちは森羅万象は運動方程式で決定論的に支配されていると考えました．だからすべては必然であり，偶然はそもそも存在しないわけです．

図 1: 落下運動

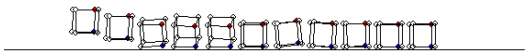


$\boxed{\boldsymbol{x}(0),\, \boldsymbol{x}'(0)} \longrightarrow \boxed{\text{運動方程式}} \longrightarrow \boxed{\boldsymbol{x}(t),\, \boldsymbol{x}'(t)}$

[*] 日本数学会 2024 年度秋季総合分科会市民講演会 (2024 年 9 月 7 日)

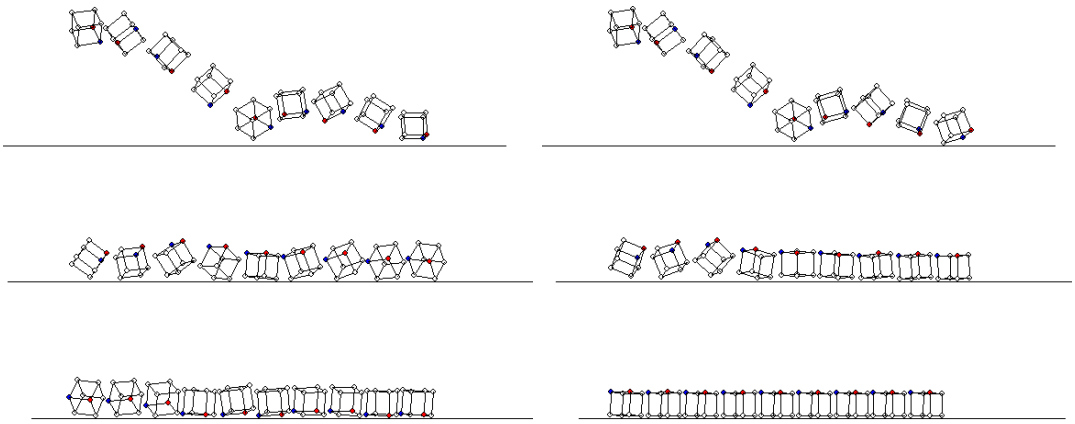
ただし，森羅万象を予測あるいは制御するためには，初期値を正確に計測あるいは設定して運動方程式—巨大な連立微分方程式—を解かなくてはなりません．ラプラスはそれが完全に遂行できる知性—いわゆる**ラプラスの魔**—にとっては偶然は存在しない，といっているのであり，それが完全には遂行できない人間にとっては，予測あるいは制御することができない現象が存在する，と主張します．つまり，そのような現象には考えを挟むことができません．そこでラプラスはそれを**ランダムな現象**と呼んだのです．

例 1. サイコロの運動について考えます．



上の図はごく低いところからサイコロを静かに落とした場合のシミュレーションです[注1]．この場合は出る目を制御できます．考えを挟めるわけです．もちろんこれはサイコロの本来の使われ方ではありません．

例 2.



サイコロの本来の使われ方をした場合の 2 つのシミュレーションです．これらはわずかに初期値が異なります．初期速度，初期角速度は同じですが初期位置が右の方が相対的に 1/200 だけ高く設定されています．わずかの初期値の違いで出る目が変わります．こんなふうですから，サイコロの目を予測したり制御したりすることはおよそ不可能です．考えを挟むことができないのでランダムな現象といえるでしょう．

このようにラプラスのランダムネスは「考えを挟めないこと」といえます．もっとも，サイコロの初期値を非常に精密に測定あるいは設定できる特別な装置を用いて，さらにサイコ

[注1] 例 1 と例 2 は市民講演会ではアニメーションでお見せしました．

ロや床の素材を耐久性のある特別なものにして，系全体を真空状態に置いて...，など手間暇を掛ければサイコロをいくらか高い場所から落としても出る目を予測あるいは制御できるかもしれません．ですから「どこまで考えを挟めるか」はそれを追求するためにどれだけ手間暇を掛けるのかに依存します．それに伴ってランダムといえるかどうかが決まります．

20 世紀初頭に量子力学が発見され，極微の世界ではニュートン力学は破綻することが明らかになりました．ですからラプラスのランダムネスの思想も極微の世界では通用しません．しかし数学ではその思想は生き続けることになります．

2　硬貨投げの記録はどれか?

サイコロよりも記述が簡単な硬貨投げを基にランダムネスを考えていきましょう．

問題 1. 硬貨を 3 回投げて表（= 1）と裏（= 0）を記録した．それは次の

(a) 101　　(b) 111　　(c) 001

のうちどれか?

硬貨を投げたのは私です．だから私はどれか知っていますが，投げた回数があまりに少ないので私以外の人にはどれだか分からないでしょう．どれも普通にあり得ますから．

次に硬貨を投げた回数を 100 にして同じ質問をします．

問題 2. 硬貨を 100 回投げて表と裏を記録した．それは次の

(a)	1010101010	1010101010	1010101010	1010101010	1010101010
	1010101010	1010101010	1010101010	1010101010	1010101010
(b)	1110110101	1011101101	0100000011	0110101001	0101000100
	0101111101	1010000000	1010100011	0100011001	1101111101
(c)	0010010000	1111110110	1010100010	0010000101	0100011000
	0010001101	0011000100	1100011001	1000101000	1011100000

のうちどれか?

今度はいかがでしょうか．長さを 100 にすると，それぞれの $\{0,1\}$ 列はそれなりに特徴が表れてくる気がしませんか．(a) は “10” のパターンを 50 回繰り返したものです．(b) (c) は (a) のような目立った特徴はありません．(b) と (c) は何が違うのか．ここでヒントを差し上げます．「(c) は円周率の小数部分 $\pi - 3$ の 2 進小数展開 100 桁である」

さあ，どれが硬貨投げの記録だと思いますか．ここでは三つの回答例について考えます．

ヒロミ (a) は規則的でランダムでない．(c) $\pi - 3$ の 2 進小数展開の通りに表裏が出たとは思えない．消去法によって硬貨投げの記録は (b).

カオル (a) (c) はコンピュータプログラムで出力可能．だからランダムではない．消去法によって硬貨投げの記録は (b).

シノブ どれも同じ確率 $1/2^{100}$ で起こるので判定できない．

ヒロミは (a) (c) はどちらも考えが挟まっている，と感じているのでしょう．**カオル**が「考えを挟む」ということを数学的に扱うために「コンピュータプログラム」に注目したのはよい考えだと思います．**カオル**の判断基準は**ヒロミ**の直感を客観化したものといえるでしょう．そして—お分かりと思いますが—私が実際に硬貨を投げて記録した $\{0,1\}$ 列は彼らのいう通り (b) です．しかしじつは (b) もプログラムで出力できます．いささか意表を突くやり方ですが，

```
print('1110110101 1011101101 0100000011 0110101001 0101000100
0101111101 1010000000 1010100011 0100011001 1101111101')
```
(1)

というプログラムを書いて (b) をそのまま出力（印字）すればよいのです．これは**カオル**の判断基準も完全に正しいわけではないことを示しています．

最後の**シノブ**の意見に賛同する人も多いのではないでしょうか．もし「これから硬貨を 100 回投げることを何回も行う．このとき (a) (b) (c) のうちどれが一番早く実現されるか?」という問題であれば**シノブ**の意見は完全に正しいです．しかし問題 2 のような場合は**統計的仮説検定**を用いて判定するのが一般的です．仮説「与えられた $\{0,1\}$ 列は硬貨投げの結果である」をどういう基準で検定するか，が問題です．**ヒロミ**と**カオル**の回答はその基準を直感的あるいは定性的に与えていますが，定量的な基準が望まれるところです．

3　コルモゴロフの乱数

この節ではいよいよコルモゴロフの乱数についてお話します．前節で述べた「仮説検定の定量的な基準」を定めるためには，ランダムネスを何らかの数量で測ることが必要です．1960 年代，コルモゴロフはこのことに成功しました [注2]．

問題 3. 100 回の硬貨投げを実現せよ．

これは簡単ですね．硬貨を 100 回投げればよいだけです．実際，私は問題 2 で硬貨を 100 回投げました．しかし投げる回数を非常に大きくすると簡単にはいきません．

[注2] ほぼ同時期に，ソロモノフ，チャイティンもそれぞれ独立に同じゴールに到達しています．

問題 4. 10^8 回（1 億回）の硬貨投げを実現せよ．

もちろん，硬貨を 10^8 回投げればよいのですが，それには膨大な時間が掛かり実際には実行できないでしょう．時間を見積もってみます．硬貨を投げる速さを 1 回 / 秒とすると，10^8 回投げるのに必要な時間は 10^8 秒，つまり 27,778 時間，およそ 3 年 2 ヵ月です．これは 1 日 24 時間働き続けた場合ですから 1 日 8 時間労働とすればおよそ 9 年半です．その労働に見合う報酬は時給 $1000+\alpha$ 円としておよそ 2,800 万円．逆にいうと，9 年半で 2,800 万円分の手間暇を掛ければ問題 4 に応えることができます．

問題 5. 10^8 回の硬貨投げを**コンピュータ**で実現せよ．

同じ 10^8 回の硬貨投げですが，今度はコンピュータを使って実現せよ，という問題です．これはコンピュータによる**乱数生成**の問題です．結論を先に述べますと，コンピュータで 10^8 回の硬貨投げを実現することはできません．皆さんは「できないのは当たり前．コンピュータは与えられたプログラムの通りに動作し，ランダムな動作はできないから」という説明を聞いたことがあるかもしれませんね．前節の**カオル**の回答の根拠にもなっています．ここでは，その「当たり前」を掘り下げて考えます．

コンピュータは**入力データ**を**出力データ**に変換する装置です．

$$\boxed{\text{入力データ}} \rightarrow \boxed{\text{コンピュータ}} \rightarrow \boxed{\text{出力データ}}$$

入力データとしてはキーボードからの文字列，マウスやタッチパネルからの座標データ，ビデオカメラからの音声や映像，出力データとしては文書，画像，音声，映像，など様々な種類がありますが，それらはすべて有限の長さの $\{0,1\}$ 列として処理されます．すなわちコンピュータは有限 $\{0,1\}$ 列を有限 $\{0,1\}$ 列に変換する装置，数学的には関数，と見ることができます．

問題 5 ではコンピュータの出力として 10^8 回の硬貨投げを求めているわけですから，すべての 10^8 ビット[注3]の $\{0,1\}$ 列が出力データとして得られなければなりません．そのためには 10^8 ビット以上の入力データが少なくとも一つ必要になります．このことを証明しましょう．

10^8 ビットの出力データの総数は 2^{10^8} です．もし 10^8-1 ビット以下の入力に限ると，その総数は，一般に m ビットの入力データの総数は 2^m 個ですから，

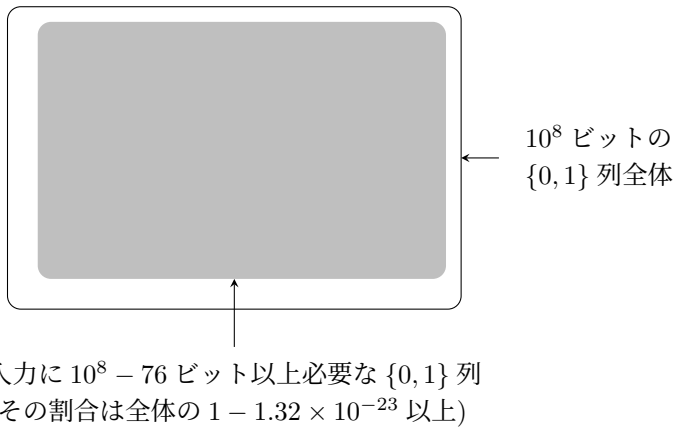
$$2^0+2^1+\cdots+2^{10^8-1}=2^{10^8}-1$$

で一つ足りません．だから 10^8 ビット以上の入力データが少なくとも一つ必要なのです．

[注3] ビットは情報量の単位．ここでは $\{0,1\}$ 列の長さのことです．

さらに，10^8-77 ビット以下の入力に限ると，その総数は $2^{10^8-76}-1<2^{10^8}/2^{76}$ となりますから，全体の $1-2^{-76}=1-1.32\times10^{-23}$ を越える場合が出力できないことが分かります．なお，1.32×10^{-23} という割合は水 18 g を全体（$=1$）とすると水分子 8 個分に相当します．しかし 10^8 ビット（あるいは 10^8-76 ビット以上）のデータを人間がキーボードから入力することは事実上不可能です．1 ビット / 秒の速さでタイプすると 10^8 秒，ぶっ通しで 3 年 2 ヵ月も掛かるからです．コンピュータへの入力を人間が行う以上，問題 5 は問題 4 と同じ困難に陥ります．

図 2: 乱数



結果として，10^8 ビットの $\{0,1\}$ 列全体は，コンピュータで出力可能なごく少数の $\{0,1\}$ 列と，出力（じつは入力）が事実上不可能な大多数の $\{0,1\}$ 列，に分かれます（図 2）．コルモゴロフは後者の $\{0,1\}$ 列をランダムな $\{0,1\}$ 列すなわち乱数と呼びました．

定義 1. (i) 有限 $\{0,1\}$ 列 x をコンピュータで出力するための入力（有限 $\{0,1\}$ 列）のうち最も短いものを q_x とする．q_x の長さを $K(x)$ と表し x の**コルモゴロフ複雑度**という．
(ii) x の長さが $n\gg1$ のとき $K(x)\approx n$ を満たす x を**乱数**という．

定義 1 (i)： q_x を定義するためには基準となるコンピュータを定める必要がありますが，計算論では一つの**万能チューリング機械**を想定します．(ii)： (1) のように x をそのまま出力するプログラム p_x をコンピュータに入力（インストール）すれば x が出力される．x の長さが n ならば p_x の長さは $n+c$（$c>0$ は定数）ですから $K(x)\le n+c$ です．$n\gg1$（n は 1 よりずっと大きい）や $\approx$（ほぼ等しい）は曖昧な記述ですが，あえて曖昧なままにしておきます．乱数と非乱数の間に厳格な境界線を引くことに本質的な意味はないからです．

x が乱数でないとき，q_x は x より短い $\{0,1\}$ 列ですが，入力 q_x から x が出力されるわけですから，q_x は x と同等の情報を持っています．これは q_x が x を**圧縮したデータ**である

ことを意味します．一方，x が乱数だと q_x は x とほぼ同じ長さですから圧縮したデータとはいえません．つまり，乱数であるとは圧縮不可能であることなのです．さあ，冒頭の W 先生の言葉を思い出しましょう．「x がランダムであるとは，x を記述するのに x 自身より短い記述法がないことをいう」はまさに x が圧縮不可能であることを表していたのですね．問題 1 の $\{0,1\}$ 列は長さが 3 なのでデータ圧縮の対象ではありません．問題 2 の $\{0,1\}$ 列 (a) (c) はそれぞれ「“10” のパターンを 50 回繰り返したもの」「$\pi-3$ の 2 進小数展開の 100 桁」という短い記述ができますからランダムではなさそうです．それに対して (b) は恐らくそれ自身より短い記述がないと思われるので，長さは 100 と短いですが，ランダムであるといってもよいかもしれません．

$K(x)$ はすべての有限 $\{0,1\}$ 列 x に対して定義されますが，じつは計算可能ではありません．つまり任意の x を入力として $K(x)$ を出力とするプログラムは存在しないのです．x が乱数かどうかは $K(x)$ の値で判断するわけですから，$K(x)$ が計算できないとなると，任意の x が乱数かどうかを判定するアルゴリズムは存在しないことになります．たとえば問題 2 では，ヒント「(c) は $\pi-3$ の 2 進小数展開の 100 桁」を知らないで (c) が乱数でないことを確実に知る方法はないかもしれません．だからヒントなしでは (c) も硬貨投げの記録だと判断されたかもしれません．また，乱数でない x の例はいくらでも書き出せますが，乱数の例は（圧倒的多数を占めるにも拘らず）一つも書き出すことができません．乱数は「乱数であること」を証明できないのですから仕方ありません．

コルモゴロフの乱数は「考えを挟めない $\{0,1\}$ 列」ということができるでしょう．乱数に考えを挟めないのは，それをコンピュータで出力するための入力データがあまりに長大なので入力できないからでした．ただし，手間暇を掛けて長大な入力を行うのであればそれに伴い乱数は減ります．

ラプラスのランダムネスとコルモゴロフの乱数はとても似たものに見えてきます．

ラプラスのランダムネス	コルモゴロフの乱数
考えを挟めないこと	考えを挟めない $\{0,1\}$ 列
初期値の測定・設定から運動方程式によって未来を予測・制御	入力データからコンピュータによって出力データを得る
初期値の測定・設定が困難，複雑な運動方程式が解けない	入力データがあまりに長大なので入力できない
手間暇を掛けるとランダムネスは減る	手間暇を掛けると乱数は減る

例 1 はサイコロの運動でしたが，ごく低いところから落とすため，考えが挟めるのでラ

ンダムではありませんでした．それが高いところから落とすと，考えが挟めなくなりランダムになります（例 2）．問題 3 は硬貨投げの回数が 100 なので実行可能でしたが，投げる回数を 10^8 にすると，コンピュータを用いたとしても，事実上実行は不可能になります（問題 4，問題 5）．これら二つの現象の共通点は何でしょう．それは，あるカギとなる数量が小さいときはランダムネスは認識されない，そしてその数量が大きくなると考えを挟むための手間暇が増えて，だんだん手に負えなくなって，ついには考えが挟めなくなるということ．そのようなときランダムネスが認識される．これがラプラスとコルモゴロフに共通するランダムネスの本質です．

4　乱数の性質

乱数は「コンピュータで出力できない」「乱数であるかどうか判定できない」など，ネガティブな特性ばかりが目立ちます．分かっているのは「長い $\{0,1\}$ 列の圧倒的多数が乱数である」ということくらいです．しかしこのことが乱数の具体的な性質を探る決定的な手掛かりになります．

ランダムネスと確率論　ランダムネスの性質は**確率論**を用いて分析するのが一般的です．「そんなこと当たり前ではないか」という声が聞こえてきそうですが，じつはぜんぜん当たり前ではありません．

ランダムネスを定義したり計算したりする上で確率は必要ありません．そのことはコルモゴロフ複雑度 $K(x)$ が確率と関係なく定義されることから明らかです．逆に確率を定義したり計算したりする上でランダムネスは必要ありません．たとえば 10^8 ビットの $\{0,1\}$ 列 $x=(x_1,\ldots,x_{10^8})$ を入力（変数）とする関数 $S(x)=x_1+\cdots+x_{10^8}$ に対して [注4]，

$$p=\frac{1}{2^{10^8}}\#\left\{x\in\{0,1\}^{10^8}\;\middle|\;\left|\frac{S(x)}{10^8}-\frac{1}{2}\right|\le\frac{1}{2000}\right\} \tag{2}$$

は「硬貨を 10^8 回投げるとき，表の出る相対頻度と $1/2$ との差が $1/2000$ 以下である確率」を表しています．ご覧のように確率 p はランダムネスと関係なく定義できるし，さらに計算もできます．要約すれば，図式 入力 → 関数 → 出力 において [注5]，入力に注目するのがランダムネス，出力に注目するのが確率論です．

このように「ランダムネスと確率は理論上関係ない」のです．それにも拘わらず，ランダムネスの分析に確率論が利用できるところが面白いと思います．

[注4] 式 (2) にある $\{0,1\}^{10^8}$ は 10^8 ビットの $\{0,1\}$ 列全体の集合を，また $\#C$ は集合 C の元の個数を表します．

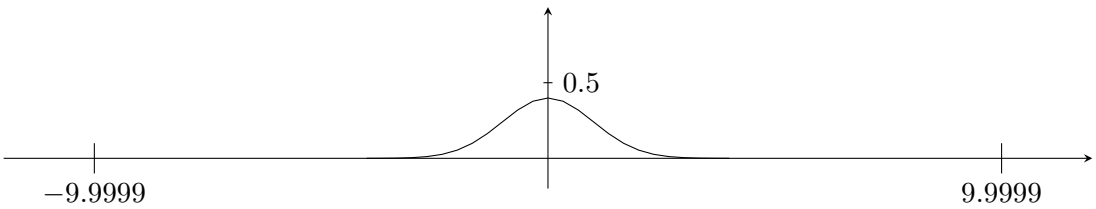
[注5] 「関数」はラプラスの場合は運動方程式，乱数の場合はコンピュータ，そして確率論の場合は（たとえば $S(x)$ のような）**確率変数**です．

確率論の援用　式 (2) で定まる確率 p の近似値は確率論の**中心極限定理**によって非常に精密に計算することができます:

$$p \approx \int_{-9.9999}^{9.9999} \frac{1}{\sqrt{2\pi}} e^{-\frac{x^2}{2}} dx = 1 - 1.53 \times 10^{-23}. \tag{3}$$

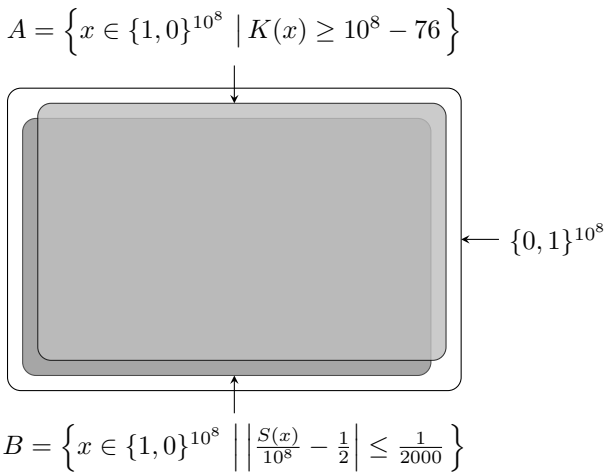
式 (3) の積分に現れる関数は**標準正規分布**の確率密度関数 (図 3) です．右辺の 1.53×10^{-23} という割合は水 18 g を全体とすると水分子 9 個分に相当します．

図 3: 標準正規分布の確率密度関数 $\frac{1}{\sqrt{2\pi}} e^{-\frac{x^2}{2}}$



定理 1. (i) $K(x) \geq 10^8 - 76$ なる乱数 $x \in \{0,1\}^{10^8}$ であって $\left|\frac{S(x)}{10^8} - \frac{1}{2}\right| \leq \frac{1}{2000}$ を満たすものの割合は全体の $1 - 1.85 \times 10^{-23}$ 以上である．
(ii) $\left|\frac{S(x)}{10^8} - \frac{1}{2}\right| \leq \frac{1}{2000}$ を満たす $x \in \{0,1\}^{10^8}$ のうち $K(x) \geq 10^8 - 76$ なる乱数 x の割合は $1 - 3.2 \times 10^{-24}$ 以上である．

図 4: 乱数と中心極限定理（概念図）



定理 1 は，図 4 における集合 A と B がほぼ同一の集合と考えてよいことを主張しています[注6]．つまり $K(x) \geq 10^8 - 76$ なる乱数 $x \in \{0,1\}^{10^8}$ は非常に少数の例外を除いて $\left|\frac{S(x)}{10^8} - \frac{1}{2}\right| \leq \frac{1}{2000}$ を満たすし，逆に $\left|\frac{S(x)}{10^8} - \frac{1}{2}\right| \leq \frac{1}{2000}$ を満たす $x \in \{0,1\}^{10^8}$ は非常に少数の例外を除いて $K(x) \geq 10^8 - 76$ なる乱数である，というわけです．

定理 1 の証明. 集合 A, B は図 4 の通りとする．図 2（下部の説明文）から $\#A/2^{10^8} \geq 1 - 1.32 \times 10^{-23}$，式 (2)(3) から，$\#B/2^{10^8} = 1 - 1.53 \times 10^{-23}$ であるので，

(i)
$$\frac{\#A \cap B}{2^{10^8}} = \frac{\#A + \#B - \#A \cup B}{2^{10^8}} \geq \frac{\#A}{2^{10^8}} + \frac{\#B}{2^{10^8}} - 1 \geq 1 - 1.85 \times 10^{-23},$$

(ii)
$$\frac{\#A \cap B}{\#B} = \frac{\#A \cap B}{2^{10^8}} \Big/ \frac{\#B}{2^{10^8}} \geq 1 - 3.2 \times 10^{-24}.$$

□

一般に，中心極限定理に代表される確率論の**極限定理**によって特定される非常に長い硬貨投げの「ほぼ確率 1 で成り立つ性質」は，そのままほぼ「乱数の性質」といえます．このような認識の下で，はじめて「確率論はランダムネスの分析に役立つ」ことが分かるのです．

参考文献

[1] A.N. Kolmogorov, *Selected works of A. N. Kolmogorov. Vol. III. Information theory and the theory of algorithms*, Edited by A. N. Shiryayev. Translated from the 1987 Russian original by A. B. Sossinsky. Mathematics and its Applications (Soviet Series), 27. Kluwer Academic Publishers Group, Dordrecht, (1993) xxvi+275 pp.

[2] P.S. Laplace, *Théorie analytique des Probabilités*. (1812). (ラプラス，「確率論—確率の解析的理論」，伊藤清解説，樋口順四郎訳，現代数学の系譜 **12**，共立出版，(1986))

[3] 杉田洋，「確率と乱数」，数学書房，(2014 年).

[注6] 集合 A と B はほぼ同一の集合ですが完全に同じ集合ではありません．たとえば $(1,0,1,0,1,0,\ldots) \in \{0,1\}^{10^8}$ は B に属していますが，A には属していません．