

検定を全部通り、それでも点は十五枚の平面に乗っている

— 「ランダム」には別根があり、統計検定も圧縮も RANDU を見抜けない：三つ組にすると、六万個の点がわずか十五枚の平行平面に並ぶ — [論文223]

山岸 勇輝 (Yuuki YAMAGISHI)

Yamagishi Complexity Torus Lab, Japan | 山岸勇輝ラボ

2026年8月

— From thinking to syncing. —

要旨

「ランダムである」は、検定を通ることと短く書けないことという二つの別の意味を持つ。本稿は、前者を全部通り、後者を派手に破っている列を数で示す。新しい数学定理も新しい法則も主張しない。第一に、どの検定も通る。RANDU の平均は **0.501293**、連の z は **-0.543**、直列相関は **-0.000029**、バイトのカイ二乗は **256.9**（期待 **255**）であり、現代の生成器と見分けがつかない（第2節）。第二に、圧縮も見抜けない。zlib にかけると RANDU は **0.9993** 倍にしかならず、現代の生成器の **1.0004** とほとんど同じである（第3節）。第三に、対で見ても、ほとんど何も出ない。連続する二つの小さな関係を探すと、値の種類は RANDU で **25353**、比較用で **59878**——わずかな痕跡はあるが、警報を鳴らすほどではない（第4節）。第四に、これが本稿の芯である。三つ組にすると $x_{i+2} - 6x_{i+1} + 9x_i$ の取る値はちょうど **15** 種類、しかも整数 **-5** から **9** までであり、整数からのずれは **0** であった——六万個の点が十五枚の平行平面に乗っている（第5節）。第五に、実際に持っている情報は **70** バイトである。**60002** バイトを作る手続きは **66** バイト + 種 **4** バイトで書け、比は **0.00117**——最良の圧縮器が達した **0.9993** の千分の一である（第6節）。

本稿の射程（scope note）：新しい数学定理も新しい法則も主張しない——マルサリアの「乱数は主に平面に落ちる」、コルモゴロフ複雑性、その計算不可能性は、いずれも標準的である。乱数生成器を設計しない——扱うのは既存の二つと現代の一つだけである。検定の一覧を作らない——四つの検定と一つの圧縮器を使うだけで、通らない検定が存在すること自体は当然である（格子構造を狙えば見抜ける）。コルモゴロフ複雑性を計算しない——計算できるのは上界だけである。暗号論的な安全性を扱わない。論文220 との関係：220 では三つの対がすべて独立なのに三つまとめては従属であった——本稿の RANDU も対では綺麗で、三つ組で崩れる。同じ形が、確率と乱数生成の二つの場所に現れている。また 220 では「探索は小さい関係を排除できるだけで問いを決められない」と書いた——本稿の第7節はその非対称の一般形である。加えたのは四つの検定と圧縮で三つの生成器が区別できないことを測ったこと、対では痕跡がほとんど出ないことを測ったこと、三つ組の値がちょうど十五種類の整数であることを示したこと、短い手続きの長さや圧縮結果の比を出したことである。

1. 記法と位置づけ

「ランダム」には少なくとも四つの言い方がある。検定を通ること（統計的）、短く書けないこと（コルモゴロフ）、次を当てられないこと（予測不能）、そしてそういう仕組みから出たこと（過程についての言明）である。本稿が比べるのは最初の二つである。

用いる生成器は $x_{i+1} = 65539 x_i \bmod 2^{31}$ (RANDU) と $x_{i+1} = (1103515245 x_i + 12345) \bmod 2^{31}$ 、それに現代の生成器である。

位置づけ：論文220では、三つの対がすべて独立なのに三つまとめると従属であった——本稿でも対では綺麗で、三つ組で崩れる。論文221では、検査（対角化できるか）を通ったことが何も保証しなかった——ここでも同じである。

2. どの検定も通る

検算 2.1：60002 個を作り、四つの検定にかける。

生成器	平均	連の z	直列相関	バイトのカイ二乗
RANDU	0.501293	-0.543	-0.000029	256.9
比較用	0.500159	-0.143	-0.000639	256.0
現代の生成器	0.500654	—	0.000053	—

（自由度 255 のカイ二乗の期待値は 255。）

観察 2.2

どの欄も三つを区別しない。RANDU は最も悪名高い生成器であり、それでもこの四つの検定を通る。

3. 圧縮も見抜けない

検算 3.1：バイト列にして zlib にかける。

生成器	元の大きさ	圧縮後	比
RANDU	60002	59961	0.9993
比較用	60002	60028	1.0004
現代の生成器	60002	60028	1.0004

観察 3.2

どれも縮まない。圧縮も一つの検定であり、他の検定と同じように取り逃がす——「圧縮できない＝ランダム」は、その圧縮器に見える構造が無いと言っているにすぎない。

4. 対で見ても、ほとんど何も出ない

検算 4.1：連続する二つのあいだの、係数の小さい関係を総当たりで探す。

生成器	値の種類（最小）	そのときの係数
RANDU	25353	$c_1 = -3$
比較用	59878	$c_1 = 1$

観察 4.2

RANDU のほうが低い（25353 対 59878）が、これはかすかな痕跡であって崩壊ではない。どちらも値の種類は数万あり、二つずつ見ているかぎり警報は鳴らない。

5. 芯：三つ組にすると、十五枚の平面

RANDU は $x_{i+2} = 6x_{i+1} - 9x_i \pmod{2^{31}}$ を厳密に満たす。ゆえに $x_{i+2} - 6x_{i+1} + 9x_i$ は（0 と 1 に正規化すれば）整数しか取れない。

検算 5.1：

測ったもの	値
三つ組の個数	60000
$x_{i+2} - 6x_{i+1} + 9x_i$ の取る値の種類	15
その値	$-5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9$
整数からのずれ（最大）	0
比較用の生成器で同じ探索をすると	59874 種類

観察 5.2

六万個の点が、十五枚の平行平面にすべて乗っている。三次元の空間に置いたとき、点は空間を埋めていない——そして第2節から第4節までのどの検定も、これに気づかなかった。

観察 5.3

論文220 と同じ形である。あちらでは三つの対がすべて独立で三つまとめると従属、ここでは対では綺麗で三つ組で崩れる——確率論と乱数生成という別の場所に、同じ抜け方が現れている。

6. 実際に持っている情報は、七十バイトである

検算 6.1 :

測ったもの	値
作られたバイト数	60002
それを作る手続き	66 バイト （+種 4 バイト）
比	0.00117
zlib が達した比	0.9993

観察 6.2

最短の記述は、最良の汎用圧縮器が達した長さの千分の一である。短い記述は確かに存在する——そしてどの検定もそれを見つけなかった。

7. 越えられない非対称

観察 7.1

短い手続きを示せば、複雑さの上界が得られる。下界はそうはいかない——コルモゴロフ複雑性は計算不可能である（チャイティン）。

示せること	どうやって
短い記述がある	一つ挙げればよい（第6節でやった）
短い記述がない	一般には不可能

観察 7.2

ゆえに検定は「これは短く書ける」と言えても、「これは短く書けない」と決して言えない。通ったことは「まだ構造が見つかっていない」という意味しか持たない——論文220で「探索は小さい関係を排除できるだけで問いを決められない」と書いたことの、一般形である。

8. 分離子と柵

観察 8.1（分離子）

四つの「ランダム」を分けているのは誰に対してランダムかである。

言い方	誰に対してか
検定を通る	その検定の一覧に対して
圧縮できない	その圧縮器に対して
短く書けない	あらゆる手続きに対して（計算不可能）
そういう仕組みから出た	過程についての言明であって、列についてではない

観察 8.2（柵）

「この列はランダムである」という言い方を囲っている柵は、どの相手に対してかを言うことである。柵の外では、この文は偽ですらなく、空である——220 の「独立を確かめた」、222 の「黒体のピークはここ」と同じ形である。

観察 8.3

そして最も広く使われる検定ほど、最も見抜けない。平均・連・相関・カイ二乗・圧縮は、いずれも一次元か二次元の性質しか見ていない——RANDU の欠陥は三次元で初めて現れる。220 では相関が二十組のうち成り立つ十四組の中にあった：確かめやすい条件ほど、破れにくい。

9. 点呼と結び

本稿が測ったことを並べる。

1. どの検定も通る（検算2.1）：連の z は **-0.543**。
2. 圧縮も見抜けない（検算3.1）：**0.9993** 対 **1.0004**。
3. 対では痕跡だけ（検算4.1）：**25353** 対 **59878**。
4. 三つ組で十五枚の平面（検算5.1）：整数 **-5** から **9**、ずれ **0**。
5. 情報は七十バイト（検算6.1）：比 **0.00117**。
6. 上界は示せ、下界は示せない（観察7.1）。

結び：平均は **0.5**、連の数も正しく、相関はほぼ零、バイトの分布も一様、圧縮しても縮まない。どの検定も「ランダムである」と答える。それでも、三つずつまとめて空間に置いた瞬間に、六万個の点は十五枚の平面に整列する——そして全体は七十バイトで書ける。検定が見落としたのではない：検定は、見るように作られ

たものしか見ない。「ランダムである」と言えるのは相手を決めたときだけであり、相手を決めないその文は、内容を持っていない。そして構造が「ある」ことは示せても、「ない」ことは決して示せない——通ったという知らせは、列についてではなく、こちらの道具についてのものである。

参考文献

1. von Neumann, J. (1951). Various techniques used in connection with random digits. *National Bureau of Standards Applied Mathematics Series*, 12.
2. Kolmogorov, A. N. (1965). Three approaches to the quantitative definition of information. *Problems of Information Transmission*, 1.
3. Chaitin, G. J. (1966). On the length of programs for computing finite binary sequences. *Journal of the ACM*, 13.
4. Martin-Löf, P. (1966). The definition of random sequences. *Information and Control*, 9.
5. Marsaglia, G. (1968). Random numbers fall mainly in the planes. *Proceedings of the National Academy of Sciences*, 61.
6. Knuth, D. E. (1997). *The Art of Computer Programming, Volume 2: Seminumerical Algorithms*. Third edition. Reading: Addison-Wesley.
7. Li, M., Vitányi, P. (2008). *An Introduction to Kolmogorov Complexity and Its Applications*. Third edition. New York: Springer.
8. 山岸勇輝 (2026). 「収束する」は四つの別の主張であり、分けているのは何を捨てることを許すかである [論文197]. Zenodo. 10.5281/zenodo.22107590
9. 山岸勇輝 (2026). 近づいているのに、一歩も近づいていない [論文216]. Zenodo. 10.5281/zenodo.22119579
10. 山岸勇輝 (2026). 平らな板が、焦点を結ぶ [論文219]. Zenodo. 10.5281/zenodo.22119788
11. 山岸勇輝 (2026). 「独立」は四つあり、たがいに何も言わない [論文220]. Zenodo. 10.5281/zenodo.22119838
12. 山岸勇輝 (2026). 最後の桁を一つ変えると、固有値が 0.16 動く [論文221]. Zenodo. 10.5281/zenodo.22120012
13. 山岸勇輝 (2026). 太陽は、緑にも橙にも赤外にも輝いている [論文222]. Zenodo. 10.5281/zenodo.22120199

— *From thinking to syncing.* —

山岸 勇輝 (Yuuki YAMAGISHI)

© 2026 Yamagishi Complexity Torus Lab, Japan · Licensed under Creative Commons Attribution 4.0 International (CC BY 4.0)