

「必ず終わる」と「必ず正しい」は、取り替えられない

— 行列の積が合っているかを乱数の縦ベクトルで確かめると、等しい行列では **4000** 回試して一度も「違う」と言わない（片側の誤り） — 分離子は、間違いの確率を問うか、終わるまでの回数を問うか — [論文844]

山岸 勇輝 (Yuuki YAMAGISHI)

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

2026年9月

YOI: <https://www.yamagishiyuuki.com/yoi/844>

— *From thinking to syncing.* —

要旨

乱数を使う手順は「速い」とだけ言われがちである。本稿は、そこに二つの型があり、取り替えられないことを数える。新しい定理も法則も主張しない。第一に、誤りは片側にしか出ない。等しい行列を **4000** 回試して、「違う」と言った回数は **0** である（第2節）。第二に、違う行列は見逃すことがある。**1** 回では **0.510250**、**5** 回でも **0.027000** の割合で見逃す（第2節）。第三に、その上限はちょうど達成される。法 **2** では見逃しが 2^{-k} と標本誤差の範囲で一致し、下回らない（第2節）。第四に、法を大きくすると下がる。**1** 回あたりの見逃しは法 **2** で **0.500500**、法 **11** で **0.083750** である（第2節）。第五に、これが本稿の芯である。必ず正しくしようとする、終わりが読めなくなる。証拠が出るまで引くと平均 **1.942000** 回だが最大 **15** 回まで伸び、等しい側では **500** 回引いても出ない（第3節）。第六に、分離子は、間違いの確率を問うか、終わるまでの回数を問うかである。同じ一回の操作から、二つの別の約束が作れる（第4節）。キーワード：乱択、片側誤り、モンテカルロ、ラスベガス、見逃し、模型。

本稿の射程（射程注記）：新しい定理も法則も主張しない。行列の積を乱数の縦ベクトルで確かめる手（フライバルズ）、その誤りが片側にしか出ないこと、 k 回繰り返すと見逃しが 2^{-k} の桁まで下がること、乱数を使う手順がモンテカルロ型とラスベガス型に分かれることは、いずれも既知である。実在の実装を扱わない。暗号や数値計算の実際には入らない。大きさ 12 の行列を法 2 から 11 で回しただけである。計算量の理論に入らない。確率的な計算のクラスの関係は主題ではない。乱数の質を論じない。擬似乱数の周期や偏りは扱わない。速い掛け算を扱わない。行列の積そのものを速く計算する方法には入らない。既刊との関係：論文552 は、守りを決めているのが抜く個数であってロットの何割かではないことを示した。本稿はその隣に置く。あちらは何個見れば見逃しがどれだけ減るかを数え、こちらは見逃しを減らす代わりに何を諦めるかを数える。論文300 は同根か別根かが判定できることを示した。間違いの確率と、終わるまでの回数は、その基準で別根である。加えたのは、片側の誤りが 4000 回で 0 件だと確かめたこと、法 2 で上限 2^{-k} がちょうど達成されると測ったこと、法を変えると 1 回あたりの見逃しが $1/p$ に沿って下がると測ったこと、証拠を待つ側の回数に上限が無く、等しい側では終わらないことを数えたこと、分離子を「間違いの確率か、終わるまでの回数か」に置いたことである。

1. 記法と問い

設定： $n \times n$ の行列 $A \cdot B \cdot C$ について、 $AB = C$ かどうかを確かめたい。掛け算をせずに、乱数の縦ベクトル x を引いて次を見る。

$$A(Bx) \stackrel{?}{=} Cx$$

等しければ必ず一致する。違っていても、 x の引き方によっては一致してしまう。本稿は $n = 12$ 、成分を法 2（と法 3・5・11）で置いた。

問い：一回の操作から、どんな約束が作れるのか。

2. 間違えるが、必ず終わる側

計算 2.1：本当に $AB = C$ の行列を 4000 回作って試した。

数えたもの	値
試した回数	4000
「違う」と言った回数	0

観察 2.2

誤りは片側にしか出ない。合っているものを「違う」と言うことは、原理として起こらない。 $AB = C$ ならどの x でも両辺が一致するからである。

計算 2.3： C の一か所だけを変えた行列を渡し、 k 回試して見逃す割合を数えた（法 2・各 4000 回）。

k	見逃し	上限 2^{-k}	標本誤差
1	0.510250	0.500000	0.007904
2	0.251000	0.250000	0.006856
3	0.121250	0.125000	0.005161
4	0.064250	0.062500	0.003877
5	0.027000	0.031250	0.002563

観察 2.4

上限は緩くない。ちょうど達成されている。どの k でも見逃しは 2^{-k} と標本誤差 3 個ぶんの中に収まり、上にも下にも出る。法 2 で一か所だけ違う行列なら、差の行列に掛けて 0 になる x がちょうど半分だからである。

計算 2.5：法を変えて、1 回あたりの見逃しを数えた。

法	見逃し	$1/p$
2	0.500500	0.500000
3	0.323500	0.333333
5	0.206500	0.200000
11	0.083750	0.090909

観察 2.6

上限が達成されるかどうかは、置き方で決まる。法を 11 にすると 1 回でも 0.083750 まで下がる。「上限 1/2」は最悪の置き方についての数で、置き方を変えれば実際はもっと良い。

3. 必ず正しいが、終わりが読めない側

計算 3.1：同じ操作を、「違う」と言い切れる証拠が出るまで繰り返した（法 2・2000 回）。

数えたもの	値
平均の回数	1.942000
中央値	1
最小	1
最大	15
5 回を超えた割合	0.025500

観察 3.2

これが本稿の芯である。平均は短いが、上限が無い。平均 1.942000 回に対して最大は 15 回で、平均の 7 倍を超える。一回ごとに独立だから、いつまでも当たらない列が確率として残るからである。

計算 3.3：等しい行列で、同じように証拠を探した。

数えたもの	値
引いた回数	500（打ち切り）
見つかった証拠	0 件

観察 3.4

等しい側では、この手は終わらない。証拠が在りえないので、いくら引いても出ない。「必ず正しい」は「必ず答える」を意味しない。

計算 3.5：二つの約束を並べた。

やり方	終わるまで	間違いの確率
$k = 5$ 回で打ち切る	必ず 5 回	0.027000
証拠が出るまで引く	上限なし	0.000000

観察 3.6

どちらかの欄に必ず不定が入る。片方は回数が決まって確率が残し、もう片方は確率が消えて回数が決まらない。同じ一回の操作から作れる約束は、この二つである。

4. 分離子

観察 4.1

分離子は、間違いの確率を問うか、終わるまでの回数を問うかである。前者を 0 にすると後者が決まらず、後者を決めると前者が 0 にならない。どちらを不定にするかの取引であって、どちらが優れているかではない。

観察 4.2

論文552 の隣に置く。552 は、守りを決めているのが抜く個数であってロットの何割かではないことを示した。あちらは何個見れば見逃しがどれだけ減るかを数え、こちらは見逃しを減らす代わりに何を諦めるかを数える。同じ「見逃し」の、値の側と代償の側である。論文300 は同根か別根かが判定できることを示した。間違いの確率と終わるまでの回数は、その基準で別根である。

観察 4.3

言わないこと。実在の実装も、計算量の理論も、乱数の質も、速い掛け算も扱わない。示したのは、一回の操作から作れる約束が二つあり、どちらも何かを不定にするということである。

5. 点呼と結び

1. 4000 回で誤警報 0 件（計算 2.1）：片側の誤り。
2. 1 回の見逃しは **0.510250**（計算 2.3）：法 2。
3. 5 回でも **0.027000**（計算 2.3）：0 にはならない。
4. 上限 2^{-k} は達成される（観察 2.4）：標本誤差の中。
5. 法 11 なら **0.083750**（計算 2.5）：置き方で変わる。
6. 証拠までの平均 **1.942000** 回（計算 3.1）：本稿の芯。
7. 最大は 15 回（計算 3.1）：平均の 7 倍超。
8. 等しい側では 500 回でも 0 件（計算 3.3）：終わらない。
9. どちらかの欄が不定になる（計算 3.5）：取引である。
10. 間違いの確率か、終わるまでの回数か（観察 4.1）：分離子・論文552・300。

結び：「必ず終わる」と「必ず正しい」は、取り替えられない。行列の積を乱数の縦ベクトルで確かめると、等しい行列では 4000 回試して一度も「違う」と言わず、違う行列では 1 回で **0.510250**、5 回でも **0.027000** の割合で見逃す。等しければどの x でも両辺が一致し、違っていても一致してしまう x が残るからである。いっぽう証拠が出るまで引けば間違いは 0 になるが、平均 **1.942000** 回に対して最大は 15 回まで伸び、等しい側では 500 回引いても証拠が出ない。一回ごとに独立で、証拠が在りえない側では在りえないままだからである。上限 2^{-k} は法 2 でちょうど達成されるが、法 11 なら 1 回でも **0.083750** まで下がり、達成されるかどうかは置き方で決まる。既刊との位置：論文552 の「守りを決めているのは抜く個数である」の隣に、その守りの代償を数えて置き、論文300 の規律で確率と回数を別根として扱った。正直に言えば、大きさ 12 の行列を法 2 から 11 で回しただけで、実在の実装は扱っていない。

参考文献

1. Motwani, R., & Raghavan, P. (1995). *Randomized Algorithms*. Cambridge University Press.
2. 山岸勇輝 (2026). 『三百本目の点呼 — 同根か別根かは、判定できる』[論文300]. YOI: <https://www.yamagishiyuuki.com/yoi/300> ・ DOI: 10.5281/zenodo.22171914

3. 山岸勇輝 (2026). 『守りを決めているのは抜く個数であって、ロットの何割かではない』 [論文552]. YOI:
<https://www.yamagishiyuuki.com/yoi/552> ・ DOI: 10.5281/zenodo.23014193

— *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)