

“Always Terminates” and “Always Correct” Cannot Be Traded for Each Other

— Checking a matrix product with a random vector never calls an equal pair unequal in **4000** trials (one-sided error) — the separator is whether one asks about the probability of error or about the number of rounds until it stops — [Paper 844]

Yuuki YAMAGISHI (山岸 勇輝)

Yamagishi Complexity Torus Lab, Japan

September 2026

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

— *From thinking to syncing.* —

Abstract

Procedures that use randomness are usually just called “fast”. This paper counts that there are two kinds, and that they cannot be traded for each other. No new theorem or law is claimed. First, the error falls on one side only: over **4000** equal pairs, “unequal” was said **0** times (Section 2). Second, unequal pairs can be missed: one round misses with a share of **0.510250**, and five rounds still with **0.027000** (Section 2). Third, the bound is exactly attained: over the field of two the misses match 2^{-k} within sampling error and do not fall below it (Section 2). Fourth, a larger modulus lowers it: one round misses with **0.500500** modulo **2** and **0.083750** modulo **11** (Section 2). Fifth, and this is the core. Making it always correct makes the stopping time unreadable: drawing until a witness averages **1.942000** rounds but reaches **15**, and on an equal pair nothing appears in **500** draws (Section 3). Sixth, the separator is whether one asks about the probability of error or about the number of rounds until it stops: one and the same operation yields two different promises (Section 4). **Keywords:** randomised algorithm, one-sided error, Monte Carlo, Las Vegas, miss rate, model.

Scope of this paper (scope note): No new theorem or law is claimed: checking a matrix product with a random vector (Freivalds), that its error is one-sided, that k repetitions push the miss rate down to the order of 2^{-k} , and that randomised procedures divide into Monte Carlo and Las Vegas kinds, are all known.No real implementation is treated: cryptography and numerical practice are not entered; matrices of size 12 were run modulo 2 through 11 .Complexity theory is not entered: relations among probabilistic complexity classes are not the subject.The quality of the randomness is not discussed: periods and biases of pseudo-random generators are not treated.Fast multiplication is not treated: methods for computing the product itself faster are not entered.Relation to earlier papers: Paper 552 showed that what sets the protection is how many are drawn, not what fraction of the lot. This paper stands beside it: there how many draws lower the misses, here what is given up in exchange for lowering them.Paper 300 showed that whether two things share a root is decidable: the probability of error and the number of rounds are distinct roots by that criterion.What is added is confirming 0 false alarms in 4000 trials, measuring that the bound 2^{-k} is exactly attained modulo 2, measuring that a larger modulus lowers the one-round miss along $1/p$, counting that the witness-waiting side has no upper bound and never stops on an equal pair, and placing the separator on probability versus stopping time.

1. Notation and the Question

Setting: for $n \times n$ matrices A , B and C , the question is whether $AB = C$.Instead of multiplying, a random vector x is drawn and the following is checked.

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

If they are equal, the two sides always agree.If they differ, some draws of x still agree.Here $n = 12$, with entries modulo 2 (and modulo 3, 5, 11).

Question: what promises can be made out of one such operation?

2. The Side That Errs but Always Stops

Computation 2.1: 4000 genuinely equal triples were built and tested.

counted	value
trials	4000
times “unequal” was said	0

Observation 2.2

the error falls on one side only. Calling a correct product wrong cannot happen in principle, because when $AB = C$ both sides agree for every x .

Computation 2.3: a single entry of C was altered, and the miss rate over k rounds counted (modulo 2, 4000 trials each).

k	miss	bound 2^{-k}	sampling error
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

Observation 2.4

the bound is not loose; it is exactly attained. At every k the miss sits within three sampling errors of 2^{-k} , falling on both sides of it, because modulo 2, with a single altered entry, exactly half of all x are annihilated by the difference.

Computation 2.5: the modulus was varied and the one-round miss counted.

modulus	miss	$1/p$
2	0.500500	0.500000
3	0.323500	0.333333
5	0.206500	0.200000
11	0.083750	0.090909

Observation 2.6

whether the bound is attained depends on the setting. Modulo 11, a single round already misses only 0.083750: “the bound is one half” is a statement about the worst setting; change the setting and the truth is better.

3. The Side That Is Always Right but May Not Stop

Computation 3.1: the same operation was repeated until a witness proving inequality appeared (modulo 2, 2000 trials).

counted	value
mean rounds	1.942000
median	1
smallest	1
largest	15
share above 5 rounds	0.025500

Observation 3.2

this is the core. The mean is short and there is no ceiling. Against a mean of 1.942000 the largest is 15, more than seven times it: each round is independent, so runs that keep missing survive with positive probability.

Computation 3.3: a witness was sought the same way on an equal pair.

counted	value
draws	500 (cut off)
witnesses found	0

Observation 3.4

on the equal side this method never stops.No witness can exist, so no amount of drawing produces one:
“always correct” does not mean “always answers”.

Computation 3.5: the two promises were laid side by side.

method	rounds until it stops	probability of error
stop after $k = 5$	always 5	0.027000
draw until a witness	no ceiling	0.000000

Observation 3.6

one column is always left undetermined.One fixes the rounds and keeps a probability; the other kills the probability and loses the rounds. These are the two promises makeable from the same single operation.

4. The Separator

Observation 4.1

the separator is whether one asks about the probability of error or about the number of rounds until it stops.Driving the first to 0 leaves the second undetermined; fixing the second leaves the first above 0. It is a trade about which one to leave open, not a ranking.

Observation 4.2

placed beside Paper 552.552 showed that what sets the protection is how many are drawn, not what fraction of the lot. There how many draws lower the misses; here what is given up in exchange. The value side and the cost side of the same “miss”.Paper 300 showed that whether two things share a root is decidable: probability and stopping time are distinct roots by that criterion.

Observation 4.3

what is not said. Real implementations, complexity theory, the quality of randomness and fast multiplication are not treated. What is shown is that one operation yields two promises, each leaving something undetermined.

5. Census and Closing

1. 0 false alarms in 4000 (Computation 2.1): one-sided error.
2. one round misses **0.510250** (Computation 2.3): modulo 2.
3. five rounds still **0.027000** (Computation 2.3): never 0.
4. the bound 2^{-k} is attained (Observation 2.4): within sampling error.
5. modulo 11 gives **0.083750** (Computation 2.5): the setting decides.
6. mean **1.942000** rounds (Computation 3.1): the core.
7. largest is 15 (Computation 3.1): over seven times the mean.
8. equal side: 0 in 500 draws (Computation 3.3): it does not stop.
9. one column stays undetermined (Computation 3.5): it is a trade.
10. probability, or stopping time (Observation 4.1): the separator; Papers 552, 300.

Closing: “Always terminates” and “always correct” cannot be traded for each other. Checking a matrix product with a random vector never calls an equal pair unequal across 4000 trials, and on an unequal pair misses with a share of 0.510250 after one round and 0.027000 after five, because equality agrees for every x , while inequality still leaves agreeing draws. Drawing until a witness instead removes the error entirely, but against a mean of 1.942000 rounds the largest reaches 15, and on an equal pair no witness appears in 500 draws, because the rounds are independent and, where no witness can exist, none ever will. The bound 2^{-k} is exactly attained modulo 2, while modulo 11 a single round already misses only 0.083750, so whether the bound is attained depends on the setting. Placed among the earlier papers: beside Paper 552’s “what sets the protection is how many are drawn”, counting the cost of that protection, and treating probability and stopping time as distinct roots by the criterion of Paper 300. To be honest: only matrices of size 12 modulo 2 through 11 were run; no real implementation was treated.

References

1. Motwani, R., & Raghavan, P. (1995). *Randomized Algorithms*. Cambridge University Press.

2. Yamagishi, Y. (2026). *The Three Hundredth Census: Whether Two Things Share a Root Is Decidable* [Paper 300]. YOI:
<https://www.yamagishiyuuki.com/yoi/300>; DOI: 10.5281/zenodo.22171914
3. Yamagishi, Y. (2026). *What Sets the Protection Is How Many Are Drawn, Not What Fraction of the Lot* [Paper 552]. YOI:
<https://www.yamagishiyuuki.com/yoi/552>; DOI: 10.5281/zenodo.23014193

— *From thinking to syncing.* —

Yuuki YAMAGISHI (山岸 勇輝)

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