The probability of singularity

Bogdan Grechuk • 21 Aug 2026

This post continues my series on favorite theorems of the twenty-first century. For an overview of the categories and my earlier selections, see this introductory post.

My choice for 2004 in probability theory is a theorem of Terence Tao and Van Vu giving a dramatically improved upper bound for the probability that a random matrix with entries in $\{-1, 1\}$ is singular. Their paper was received by the *Journal of the American Mathematical Society* in 2004 and published in 2007 (Tao and Vu 2007).

Recall that an $n \times n$ matrix A is *invertible*, or *non-singular*, if there exists a matrix A^{-1} such that

$$AA^{-1} = A^{-1}A = I_n.$$

Equivalently, A is invertible if

$$\det(A) \neq 0.$$

Otherwise, A is called *singular*.

Let

$$M_n = (\xi_{ij})_{1 \leq i,j \leq n}$$

be an $n \times n$ random matrix whose entries are independent and satisfy

$$P(\xi_{ij} = 1) = P(\xi_{ij} = -1) = \frac{1}{2}.$$

Equivalently, M_n is chosen uniformly at random from all $n \times n$ matrices with entries in $\{-1, 1\}$. Put

$$P_n = P\big(\det(M_n) = 0\big).$$

There are several obvious ways for M_n to be singular. For example, if two rows are equal or are negatives of one another, then the rows are linearly dependent. The same is true for two columns.

For a fixed pair of rows, the probability that they are equal up to sign is

$$2^{1-n}.$$

There are $\binom{n}{2}$ pairs of rows and the same number of pairs of columns. Since intersections between these events contribute only lower-order terms, we obtain

$$P_n \geq (1 + o(1))\, n^2 2^{1-n}.$$

It has long been conjectured that these elementary coincidences account for almost all singular matrices. More precisely,

$$P_n = (1 + o(1))\, n^2 2^{1-n}. \tag{1}$$

The conjecture appears explicitly, for example, in work of Odlyzko (Odlyzko 1988). It predicts that, conditioned on M_n being singular, with probability tending to 1 the matrix has two rows or two columns equal up to sign.

Even proving that P_n tends to zero is nontrivial. In 1967, Komlós (Komlós 1967) proved that

$$P_n = o(1).$$

In 1995, Kahn, Komlós, and Szemerédi (Kahn et al. 1995) obtained the first exponential upper bound,

$$P_n = O(0.999^n).$$

Tao and Vu subsequently improved this to

$$P_n = O(0.958^n)$$

in (Tao and Vu 2006). Their next paper produced a much larger improvement.

Theorem 1 (Tao–Vu) *As $n \to \infty$,*

$$P_n \leq \left(\frac{3}{4} + o(1)\right)^n.$$

The proof combines probability, Fourier analysis, and additive combinatorics. Regard the rows of M_n as independent random vectors

$$X_1, \ldots, X_n \in \{-1, 1\}^n.$$

If the matrix is singular, then these vectors lie in some proper linear subspace. After a reduction to a sufficiently large finite field, it is enough to study hyperplanes.

For a hyperplane V, define

$$\rho(V) = P(X \in V),$$

where X is uniformly distributed on $\{-1, 1\}^n$. If

$$V = \{x : a_1 x_1 + \cdots + a_n x_n = 0\},$$

then

$$\rho(V) = P\big(a_1\varepsilon_1 + \cdots + a_n\varepsilon_n = 0\big),$$

where the ε_i are independent random signs. Thus, estimating $\rho(V)$ becomes a Littlewood–Offord problem about the concentration of random signed sums.

The main difficulty is that there are enormously many possible hyperplanes, so a direct union bound is much too weak. Tao and Vu divide the hyperplanes according to their concentration. Hyperplanes with small concentration are individually unlikely, while hyperplanes with large concentration must have strong additive structure. Inverse results from additive combinatorics show that the coefficients $a_1, \ldots, a_n$ of such an exceptional hyperplane are largely contained in a low-rank generalized arithmetic progression. This rigidity makes the exceptional hyperplanes sufficiently rare to count.

For the remaining hyperplanes, a Fourier-analytic comparison gives the required exponential saving. The constant $3/4$ ultimately arises from the elementary inequality

$$|\cos t| \le \frac{3}{4} + \frac{1}{4}\cos(2t).$$

This connection between singular random matrices and the additive structure of concentrated random sums became one of the central ideas in the subsequent development of the subject.

In 2010, Bourgain, Vu, and Wood (Bourgain et al. 2010) improved the bound to

$$P_n \le \left(\frac{1}{\sqrt{2}} + o(1)\right)^n.$$

In 2020, Tikhomirov (Tikhomirov 2020) determined the optimal exponential rate:

$$P_n = \left(\frac{1}{2} + o(1)\right)^n.$$

Equivalently,

$$\lim_{n\to\infty} P_n^{1/n} = \frac{1}{2}.$$

This result shows that no mechanism of singularity is exponentially more likely than the equality of two rows or columns up to sign. It does not, however, prove the sharper conjecture (1). The factor n^2 is invisible at the exponential scale, since

$$\big(n^2 2^{1-n}\big)^{1/n} \longrightarrow \frac{1}{2}.$$

Thus, the conjecture that

$$P_n = (1 + o(1))\, n^2 2^{1-n}$$

remains open.

Although the numerical estimate in Theorem 1 has since been surpassed, the theorem remains a landmark. Its proof revealed that rare linear dependencies in random matrices can be understood through inverse Littlewood–Offord theory and the additive structure of the coefficients defining the corresponding hyperplanes.

References

Bourgain, Jean, Van H. Vu, and Philip Matchett Wood. 2010. “On the Singularity Probability of Discrete Random Matrices.” *J. Funct. Anal.* 258 (2): 559–603.

Kahn, Jeff, János Komlós, and Endre Szemerédi. 1995. “On the Probability That a Random ± 1-Matrix Is Singular.” *J. Amer. Math. Soc.* 8 (1): 223–40.

Komlós, János. 1967. “On Determinant of $(0, 1)$ Matrices.” *Studia Science Mathematics Hungarica* 2: 7–21.

Odlyzko, Andrew M. 1988. “On Subspaces Spanned by Random Selections of ± 1 Vectors.” *J. Combin. Theory Ser. A* 47 (1): 124–33.

Tao, Terence, and Van Vu. 2006. “On Random ± 1 Matrices: Singularity and Determinant.” *Random Structures & Algorithms* 28 (1): 1–23.

Tao, Terence, and Van Vu. 2007. “On the Singularity Probability of Random Bernoulli Matrices.” *J. Amer. Math. Soc.* 20 (3): 603–28.

Tikhomirov, Konstantin. 2020. “Singularity of Random Bernoulli Matrices.” *Ann. of Math.* 191 (2): 593–634.