2002

TR-2002018: How Frequently Is a Matrix Nonsingular?

Xinmao Wang

How frequently is a matrix nonsingular?

Xinmao Wang
Ph.D. Program in Mathematics
Graduate School of CUNY, New York, NY 10016, USA
xwang2@gc.cuny.edu

Summary. In this report, we investigate how frequently an $n \times n$ matrix M of a certain class $\mathfrak{T}$ is nonsingular on the ring $\mathbb{Z}_q$, that is, $\det(M) \bmod q \neq 0$. $\mathbb{Z}_q$ is the ring of integers modulo $q = p^{g+1}$, where p is a prime and $g \geq 0$. A matrix M is strongly nonsingular if M is nonsingular with all its leading principal, that is, northwestern submatrices. This property is required in many algorithms, for example, the complete recursive triangular factorization of M (see, e.g., [S69], [M80], [BA80], [P01]). Therefore, we investigate how frequently M is strongly nonsingular, too.

1 Our Experiment

For any number $n \in \mathbb{Z}_q$, we define $\operatorname{ord}(n)$ to be the largest integer $0 \leq r \leq g+1$ such that $p^r \mid n$. We use Gaussian elimination to compute $\operatorname{ord}(\det M)$ demonstrated as follows:

```
Function OrderOfDeterminant( M )
    r = 0
    For i = 1 To n
        If column i is 0 Then Return g+1
        While p divides all the element in column i
            divide column i by p
            r = r+1
        End While
```

```
        If p divide M(i,i) Then
            find M(j,i) coprime to p
            add row j to row i
        End If
        For j = i+1 To n
            multiply row i by M(i,i)^{-1} mod q
            substract M(i,j) times row i from row j
        Next j
    Next i
    Return r
End Function
```

In the case $\mathfrak{T}$ contains all matrices M, the $M(i,j)$'s are independent under the uniform random distribution on $\mathbb{Z}_{\shortparallel}$. In the case $\mathfrak{T}$ contains all Toeplitz matrices M, the $M(1,j)$'s and $M(i,1)$'s are independent under the uniform random distribution on $\mathbb{Z}_{\shortparallel}$.

See the tables in the Appendix for our experiment results, where $p = 2$.

2 Analysis of Experiment Results

For fixed q and n, we assume that M is singular over $\mathbb{Z}_q$ with a probability p. Next we estimate p. Let x be a random variable such that

$$x = \begin{cases} 1, & \det M = 0 \bmod q; \\ 0, & \det M \neq 0 \bmod q. \end{cases}$$

Let $x_1, \ldots, x_m$ be the observed values of x. By the Central Limit Theorem,

$$\lim_{m \to \infty} \frac{(x_1 + \ldots + x_m) - mp}{\sqrt{mp(1-p)}} = N(0,1)$$

where $N(0,1)$ is the standard normal probability distribution. Therefore, a confidence interval of probability $1 - \alpha$ for p is

$$\left(\bar{x} - Z_{\alpha/2}\sqrt{\bar{x}(1-\bar{x})/m},\ \bar{x} + Z_{\alpha/2}\sqrt{\bar{x}(1-\bar{x})/m}\right)$$

where $\bar{x} = \frac{1}{m}(x_1 + \ldots + x_m)$, Z_α is defined by Probability$(N(0,1) > Z_\alpha) = \alpha$.

Example 1 *For $p = 2, g = 7, n = 50$, we are "99.9%" sure that*

- *Probability(Toeplitz matrix M is nonsingular)* $= 0.993 \pm 0.001$;
- *Probability(Toeplitz matrix M is strongly nonsingular)* $= 0.731 \pm 0.005$.
- *Probability(general matrix M is nonsingular)* $= 0.992 \pm 0.001$;
- *Probability(general matrix M is strongly nonsingular)* $= 0.688 \pm 0.005$.

Acknowledgements. I thank Professor Richard Isaac for suggesting format for statistical tests.

References

[BA80] R. R. Bitmead, B. D. O. Anderson, Asymptotically Fast Solution of Toeplitz and Related Systems of Linear Equations, *Linear Algebra and Its Applications*, **34**, 103–116, 1980.

[M80] M. Morf, Doubling Algorithms for Toeplitz and Related Equations, *Proceedings of IEEE International Conference on ASSP*, 954–959, IEEE Press, Piscataway, New Jersey, 1980.

[P01] V. Y. Pan, *Structured Matrices and Polynomials: Unified Superfast Algorithms*, Birkhäuser/Springer, Boston/NewYork, 2001.

[Pa] V. Y. Pan, Nearly Optimal Toeplitz/Hankel Computations, Technical Report, Ph.D. Program in Computer Science, The Graduate Center of City University of New York, New York, 2002.

[S69] V. Strassen, Gaussian Elimination Is Not Optimal, *Numerische Mathematik*, **13**, 354–356, 1969.

Appendix

Table 1: Number of times a random general matrix M is nonsingular over $\mathbb{Z}_q$ out of $100,000$ samples for $q = 2^{g+1}$

	$n = 5$	$n = 10$	$n = 50$	$n = 100$
$g = 0$	29,986	28,781	28,940	28,781
$g = 1$	58,637	57,679	57,884	57,782
$g = 2$	77,650	76,817	77,047	77,104
$g = 3$	88,399	87,916	88,000	88,080
$g = 4$	94,102	93,888	93,943	93,921
$g = 5$	97,046	96,911	96,963	96,937
$g = 6$	98,519	98,414	98,483	98,452
$g = 7$	99,245	99,180	99,212	99,235
$g = 8$	99,634	99,598	99,590	99,620
$g = 9$	99,820	99,791	99,783	99,806
$g = 10$	99,911	99,894	99,892	99,899
$g = 11$	99,956	99,957	99,950	99,953
$g = 12$	99,977	99,977	99,978	99,980
$g = 13$	99,985	99,992	99,991	99,992
$g = 14$	99,992	99,996	99,993	99,995
$g = 15$	99,993	99,997	99,996	99,998
$g = 16$	99,995	99,999	99,999	99,998
$g = 17$	99,998	99,999	99,999	99,998
$g = 18$	99,999	100,000	99,999	99,999
$g = 19$	99,999	100,000	100,000	100,000
$g = 20$	99,999	100,000	100,000	100,000

Table 2: Number of times a random general matrix M is strongly nonsingular over $\mathbb{Z}_q$ out of $100,000$ samples for $q = 2^{g+1}$

	$n = 5$	$n = 10$	$n = 50$	$n = 100$
$g = 0$	3,139	93	0	0
$g = 1$	18,018	3,001	0	0
$g = 2$	41,353	15,653	5	0
$g = 3$	63,254	37,406	566	1
$g = 4$	78,891	59,785	6,440	374
$g = 5$	88,518	76,762	23,843	5,681
$g = 6$	94,042	87,455	47,873	22,908
$g = 7$	96,948	93,386	68,784	46,996
$g = 8$	98,402	96,580	82,731	68,572
$g = 9$	99,164	98,253	90,944	82,738
$g = 10$	99,577	99,121	95,323	90,927
$g = 11$	99,789	99,553	97,669	95,353
$g = 12$	99,886	99,769	98,792	97,582
$g = 13$	99,934	99,877	99,403	98,779
$g = 14$	99,965	99,947	99,707	99,371
$g = 15$	99,978	99,967	99,854	99,662
$g = 16$	99,983	99,984	99,917	98,836
$g = 17$	99,986	99,990	99,963	99,914
$g = 18$	99,987	99,994	99,982	99,947
$g = 19$	99,987	99,994	99,988	99,970
$g = 20$	99,988	99,995	99,992	99,983

Table 3: Number of times a random Toeplitz matrix M is nonsingular over $\mathbb{Z}_q$ out of $100,000$ samples for $q = 2^{g+1}$

	$n = 5$	$n = 10$	$n = 50$	$n = 100$
$g = 0$	50,068	49,773	50,021	50,157
$g = 1$	68,707	68,502	68,969	68,717
$g = 2$	82,867	82,697	82,940	82,692
$g = 3$	90,399	90,421	90,478	90,432
$g = 4$	94,941	94,953	95,020	95,017
$g = 5$	97,258	97,315	97,293	97,265
$g = 6$	98,669	98,640	98,574	98,610
$g = 7$	99,329	99,311	99,257	99,243
$g = 8$	99,661	99,653	99,613	99,594
$g = 9$	99,834	99,837	99,801	99,814
$g = 10$	99,915	99,926	99,901	99,906
$g = 11$	99,958	99,963	99,951	99,960
$g = 12$	99,978	99,982	99,970	99,981
$g = 13$	99,992	99,993	99,986	99,991
$g = 14$	99,996	99,997	99,993	99,996
$g = 15$	99,999	99,999	99,996	99,996
$g = 16$	99,999	99,999	99,997	99,997
$g = 17$	100,000	100,000	99,998	99,998
$g = 18$	100,000	100,000	100,000	100,000
$g = 19$	100,000	100,000	100,000	100,000
$g = 20$	100,000	100,000	100,000	100,000

Table 4: Number of times a random Toeplitz matrix M is strongly nonsingular over $\mathbb{Z}_q$ out of $100,000$ samples for $q = 2^{g+1}$

	$n = 5$	$n = 10$	$n = 50$	$n = 100$
$g = 0$	15,944	3,809	0	0
$g = 1$	29,232	10,023	1	0
$g = 2$	51,344	27,054	162	0
$g = 3$	68,900	47,684	2,536	50
$g = 4$	82,183	67,021	13,449	1,820
$g = 5$	90,105	80,386	33,048	10,788
$g = 6$	94,730	89,071	55,604	30,396
$g = 7$	97,167	94,018	73,141	52,867
$g = 8$	98,558	96,829	85,008	71,673
$g = 9$	99,268	98,322	94,913	84,117
$g = 10$	99,631	99,180	95,720	91,556
$g = 11$	99,809	99,591	97,797	95,505
$g = 12$	99,904	99,787	98,884	97,613
$g = 13$	99,950	99,906	99,428	98,784
$g = 14$	99,968	99,952	99,719	99,391
$g = 15$	99,977	99,977	99,847	99,667
$g = 16$	99,983	99,987	99,940	99,832
$g = 17$	99,986	99,990	99,968	99,901
$g = 18$	99,986	99,995	99,968	99,941
$g = 19$	99,989	99,996	99,980	99,966
$g = 20$	99,268	98,996	99,987	99,978