Invertibility Probability of Binary Matrices

Team Members:

Angela DAI, Dos Pueblos High School, Goleta, California, USA

Caroline KIM, Dos Pueblos High School, Goleta, California, USA

John KIM, Dos Pueblos High School, Goleta, California, USA

Coach:

Dr. Guofang Wei

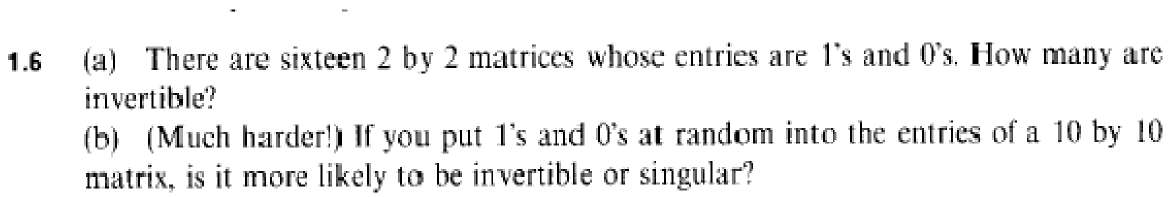
University of California Santa Barbara, Santa Barbara, California, USA

Abstract

Motivated by an extra credit problem from our Linear Algebra class, we study the invertibility probability of binary matrices (the number of invertible binary matrices divided by the total number of binary matrices). Binary matrices are of interest in combinatorics, information theory, cryptology, and graph theory. It is known that the invertibility probability of $n \times n$ binary matrices goes to 1 as $n \to \infty$. We conjecture that this probability monotonically increases as the size of the binary matrix increases, and we investigate this by exploring how $n \times n$ binary matrices of rank n and rank $(n-1)$ can be enlarged to $(n+1) \times (n+1)$ invertible binary matrices. Calculating this explicitly for the identity matrix, we obtain a probable bound that would show that, in a sense, our conjecture is asymptotically true. With the use of a computer, we also computed how many $(n+1) \times (n+1)$ invertible binary matrices can be enlarged from $n \times n$ matrices of rank n and rank $(n-1)$ for small n. In addition, we study the invertibility probability of matrices with entries in $\mathbb{Z}_q$.

1 Introduction

In this paper, we explore the invertibility probability of binary matrices ((0, 1)-matrices). We had come across a question in our Linear Algebra class, which our teacher assigned for extra credit, regarding whether there were more singular or non-singular binary 10×10 matrices:



1.6 (a) There are sixteen 2 by 2 matrices whose entries are 1's and 0's. How many are invertible?
(b) (Much harder!) If you put 1's and 0's at random into the entries of a 10 by 10 matrix, is it more likely to be invertible or singular?

Figure 1: The extra credit problem, from [3].

Part (a) was quite easy; one can just list them out. However, part (b) turned out to be a surprisingly difficult question. As we looked into it, it became more and more fascinating.

Binary matrices are of interest in combinatorics, information theory, cryptology, and graph theory. Their invertiblity is especially important in encoding (see Section 2 for more detail). There are many important works on the invertibility of binary matrices. Note that there are 2^{n^2} $n \times n$ binary matrices. Let $F(n,k)$ be the number of $n \times n$ matrices of rank k, and $P(n) = \frac{F(n,n)}{2^{n^2}}$, the invertibility probability. In 1967, J. Komlos [2] showed that $\lim_{n\to\infty} P(n) = 1$, unlike the mod 2 case (see Section 3 for more detail). Recently T. Tao and V. Vu [4, 5] studied the rate of convergence and made great progress. However, it is very difficult to explicitly compute $F(n,n)$, and thus $P(n)$ as well. For $n \leq 8$, M. Živković explicitly calculated $F(n,k)$ with the use of a computer [7], see Table 1 in the Appendix.

We conjecture that the invertibility probability monotonically increases as the size of the matrix increases.

Conjecture 1.1. [1] *$P(n+1) \geq P(n)$ for all $n \geq 3$.*

This is true for $3 \leq n \leq 8$ from M. Živković's work [7]. We have tested it with random computer sampling, with sample sizes of 100,000 for $n \leq 30$, which suggested that it is true in that range. Later, we found that T. Voigt and G. Ziegler had used computer sampling of sizes 250,000 for $n \leq 30$ [6], which also indicated that it is true.

When the matrices are over a finite field, it is well known that the number of invertible ones can be explicitly computed. In fact, the invertibility probability for these matrices decreases as their size increases. We present it in Section 3 for comparison.

[1] We have checked with several experts that this is still open.

To investigate our conjecture, note that $P(n+1) \geq P(n)$ is equivalent to

$$F(n+1, n+1) \geq 2^{2n+1} F(n, n). \tag{1.1}$$

Thus, we look at the number of invertible $(n+1) \times (n+1)$ binary matrices that correlate to a single $n \times n$ binary matrix. A single $n \times n$ binary matrix can be enlarged by an $n \times 1$ column and a $1 \times (n+1)$ row to generate 2^{2n+1} $(n+1) \times (n+1)$ binary matrices (see (4.4) in Section 4). Therefore, given an $n \times n$ invertible matrix, if the matrices it generates are all invertible, we are done. However, this is never true as one can always append a row of zeros, making the matrix singular. We denote $S(A_n)$ as the number of singular $(n+1) \times (n+1)$ binary matrices generated by A_n, and $N(A_n)$ the number of nonsingular ones generated. $S(A_n) \geq (n+1)2^n$ for all invertible matrices A_n (see the explanation above (4.5) in Section 4). On the other hand, a singular $n \times n$ matrix can generate invertible $(n+1) \times (n+1)$ matrices. We try to compensate for the loss of the former with these ones.

First, in Section 4.1, we give the following rough estimate which holds for matrices with entries in $\mathbb{Z}_q$, with q prime.

Theorem 1.2. *For matrices with entries in $\mathbb{Z}_q$, with q prime, $F(n+1, n+1) \geq q^{2n}(q-1)F(n, n)$.*

Letting $q = 2$ gives

Corollary 1.3. *For binary matrices, $F(n+1, n+1) \geq 2^{2n}F(n, n)$, namely, at least half of the $(n+1) \times (n+1)$ binary matrices generated by an invertible $n \times n$ binary matrix are invertible.*

To obtain a better bound for binary matrices, we compute $S(I_n)$ explicitly, giving the estimate below.

Theorem 1.4. *The number of $(n+1) \times (n+1)$ invertible matrices that can be enlarged from the identity matrix I_n is bounded from below by*

$$N(I_n) > 2^{2n+1}\left(1 - \frac{n+1}{2}(\frac{3}{4})^n\right). \tag{1.2}$$

We had hoped that for any invertible matrix A_n, $N(A_n) \geq N(I_n)$ since the rows of I_n are able to produce many linear combinations that remain binary. However, it turns out that this is not true. While $N(I_3) = 74$, we found many invertible matrices A_3 with $N(A_3) = 72$ through a program we created to compute the number of invertible matrices generated by each 3×3 invertible one (see Table 2 in the appendix for more data). On the other hand, it is possible that the estimate (1.2) is true for all invertible $n \times n$ matrices (its right hand side is only 20 when $n = 3$).

In Section 4.2, we look at the number of invertible binary matrices that can be generated from a singular $n \times n$ binary matrix, especially the ones of rank $(n-1)$. As an example, we take I_{n-1} and expand it to an $n \times n$ matrix by adding zeros, which gives an $n \times n$ matrix of rank $(n-1)$, B_n (see (4.7)). Again we compute the number of singular $(n+1) \times (n+1)$ matrices B_n generates by looking at the linear combinations of its rows. As a result, we find

Theorem 1.5. *The number of $(n+1) \times (n+1)$ invertible matrices that can be enlarged from the matrix B_n is bounded from below by*

$$N(B_n) > 2^{2n} - (n+1)3^{n-1}. \tag{1.3}$$

We expect this to be true for all $n \times n$ matrices of rank $(n-1)$.

If (1.2) holds for all $n \times n$ invertible matrices and (1.3) for all $n \times n$ rank $(n-1)$ matrices, then

$$F(n+1, n+1) \geq 2^{2n+1} \left(1 - \frac{n+1}{2} (\frac{3}{4})^n \right) F(n, n) + [2^{2n} - (n+1)3^{n-1}]F(n, n-1).$$

By (4.5), $F(n, n-1) \geq n2^{n-1}F(n-1, n-1)$. Hence dividing by $2^{(n+1)^2}$ gives a bound on the invertibility probability of $(n+1) \times (n+1)$ binary matrices:

$$P(n+1) \geq P(n) + P(n-1)\frac{n}{2^{n+1}} - P(n)\frac{3^n(n+1)}{2^{2n+1}} - P(n-1)\frac{3^{n-1}(n+1)n}{2^{3n+1}}.$$

This would show that $P(n)$ is, in a sense, asymptotically increasing with an error of $O((\frac{3}{4})^n)$, which is known from T. Tao and V. Vu [5]. We hope our method of estimating $F(n+1, n+1)$ by $N(A_n)$ would provide a much simpler approach. Furthermore, we conjecture that

Conjecture 1.6. *When A_n is invertible,* $\lim_{n\to\infty} \frac{N(A_n)}{2^{2n+1}} = 1$.

We provide evidence for this in Section 4.3, namely, that on average, Conjecture 1.6 is true. In fact, for most A_n, our conjecture is true. Note also that if (1.2) is true for all invertible binary matrices, then Conjecture 1.6 would be an immediate consequence. Thus one can view Conjecture 1.6 as a weakened version of Theorem 1.4 for all invertible binary matrices.

We are continuing to look into this.

2 Binary Matrices and Science

Binary matrices are widely used not only in mathematics but also in cryptography, telecommunications, combinatorics, and graph theory. Invertible matrices' unique nature of having a determinant and an inverse helps to encrypt messages and compress communication signals effectively. Several techniques of encryption have been developed using matrix inverses, such as the Hill Cipher, one of the first polygraphic substitution ciphers (multiple letters encrypted to ciphertext) [1].

To encrypt a plaintext message using the Hill Cipher, the message is divided into m blocks, each containing n letters. Then a number is assigned to each possible n letter combination (e.g. if $n = 2$, assign $aa = 0$, $ab = 1...$ $zz = 26^2 - 1$, or in any pattern). The plaintext message is made into an $m \times 1$ vector, each entry containing the assigned number. Then generate a word of $m^2 n$ letter length as a key and convert it to a matrix by coding n length letters of the word to assigned numbers (e.g. if $m = 3$ and $n = 2$, $abcdefghijklmnopqr \Rightarrow [1(ab)55(cd)109(ef)164(gh)...]$) to be placed into a matrix horizontally. Lastly, this key matrix is multiplied with the converted plaintext $m \times 1$ vector to create the final encrypted matrix. The Hill Cipher can be deciphered using matrix inverses, so the key matrix should be invertible. As shown above, the calculation process of Hill Cipher is simple and completely linear; thus the encrypted matrix is vulnerable to known plaintext attacks. Yet as the numbers get larger, combined with non-linear operations, its security grows rapidly.

The extension of this cipher technique is used in telecommunications with binary matrices. Bits of data are formed into binary matrices through heapsort, facilitating the application of more complicated and advanced techniques (such as multiplying the key matrix in the Hill Cipher). The goal in communications engineering is to transmit and receive data accurately and quickly (for this, smaller amounts of data, and thus compression as well, are good) and often in a secure environment, hence this technique.

In addition, the development of random matrix theory in combinatorics has cleared the path for modern physics theories, such as nuclear physics and quantum theory, to be represented in math.

3 Matrices over Finite Fields

Given a finite field $\mathbb{F}_q$ with q elements, the order of $GL(n,q)$ ($n \times n$ invertible matrices over $\mathbb{F}_q$) can be explicitly calculated. Note that $A \in GL(n,q)$ is equivalent to $\det A \neq 0$ in $\mathbb{F}_q$. Therefore, the number of $GL(n,q)$ gives a lower bound on the $F(n,n)$ when $q = 2$. An $n \times n$ matrix $A \in GL(n,q)$ is also the same as a set of n linearly independent vectors in $\mathbb{F}_q$. The first vector can be any nonzero vector, of which there are $q^n - 1$ choices. This first vector spans a one-dimensional subspace, which contains q^1 elements. We must choose a second vector that is not in this subspace, giving $q^n - q^1$ possibilities. Having already chosen k independent vectors, there are $q^n - q^k$ possible vectors that will create a linearly independent set. Hence, the number of ways to choose vectors that will form an $n \times n$ invertible matrix is

$$(q^n - q^0)(q^n - q^1)(q^n - q^2) \cdots (q^n - q^{n-1}) = \prod_{k=1}^{n} (q^n - q^{k-1}).$$

So the invertibility probability of an $n \times n$ matrix over field $\mathbb{F}_q$ is

$$\frac{\prod_{k=1}^{n}(q^n - q^{k-1})}{q^{n^2}} = \prod_{k=1}^{n}(1 - q^{k-1-n}) < 1 - \frac{1}{q}.$$

It is interesting to note that as n grows, this probability decreases. Also, for any fixed n, when $q \to \infty$, the invertibility probability goes to 1. This case corresponds to binary matrices when $\mathbb{F}_q = \mathbb{Z}_2$. However, it is very different from the case with invertible matrices over $\mathbb{R}$, as that invertibility probability has been shown to approach 1 as $n \to \infty$. Hence, there are much fewer invertible matrices in $\mathbb{Z}_2$. (This is the case because in $\mathbb{Z}_2$, k linearly independent vectors span a much larger set.) This does not give a good lower bound on $P(n)$ at all.

4 From Size n to Size $n+1$ Binary Matrices

In order to compare the invertibility probability of a $n \times n$ binary matrix to a $(n+1) \times (n+1)$ binary matrix, we look at how many distinct invertible $(n+1) \times (n+1)$ binary matrices can be generated from one invertible $n \times n$ binary matrix and one singular $n \times n$ binary matrix, respectively.

Given an $n \times n$ binary matrix A_n, we can enlarge it by an $n \times 1$ column vector (on the right), and to this new matrix append a $1 \times (n+1)$ row vector (to the bottom) as follows:

$$\begin{pmatrix} & & * \\ & A_n & \vdots \\ * & \cdots & * \end{pmatrix}, \tag{4.4}$$

where the asterisks signify the appended column and row of components 0 or 1.

Thus we produce 2^{2n+1} different possible $(n+1) \times (n+1)$ binary matrices from A_n. When A_n is invertible, at least $(n+1)2^n$ of these matrices generated are singular, since we can always append a last row of 0s or one of the original n rows. Hence, when A_n is invertible,

$$S(A_n) \geq (n+1)2^n. \tag{4.5}$$

4.1 $n \times n$ Invertible Matrices to $(n+1) \times (n+1)$ Invertible Matrices

First, we give a rough lower bound for $F(n+1, n+1)$ in terms of $F(n, n)$, proving Theorem 1.2. Given an invertible matrix A_n whose entries are in $\mathbb{Z}_q$, the $(n+1) \times (n+1)$ matrices it generates will be singular if and only if the last row (the appended row) is in the span of the above n rows. After enlarging A_n by an $n \times 1$ column, giving $q^n F(n, n)$ matrices, these matrices have n linearly independent columns. In adding a $1 \times (n+1)$ row to these matrices, the entries in this appended row that correspond to the n linearly independent columns completely determine the remaining entry in the row. Thus the probability that this appended row is in the span of the first n is at most $\frac{1}{q}$. This gives at most $q^n F(n,n)\frac{1}{q}(q^{n+1}) = q^{2n}F(n,n)$ singular matrices (with entries in $\mathbb{Z}_q$) produced by an $n \times n$ invertible matrix (with entries in $\mathbb{Z}_q$).

With these estimates, we have

$$F(n+1,n+1) \geq (q^{2n+1} - q^{2n})F(n,n) = q^{2n}(q-1)F(n,n).$$

Dividing this by $q^{(n+1)^2}$ gives

$$P(n+1) \geq \frac{q-1}{q}P(n).$$

Here, as $q \to \infty$, $P(n+1) \geq P(n)$.

This applies to binary matrices when $q = 2$. In this case,

$$F(n+1,n+1) \geq (2^{2n+1} - 2^{2n})F(n,n) = 2^{2n}F(n,n).$$

Dividing this by $2^{(n+1)^2}$ gives

$$P(n+1) \geq \frac{1}{2}P(n).$$

However, this only gives half of the invertible binary matrices we need.

Among the nonsingular $n \times n$ binary matrices, it seems that the identity matrix could produce the most binary linear combinations (at least, in terms of additive combinations). So we compute the number of singular $(n+1) \times (n+1)$ binary matrices that can be generated from the identity matrix I_n:

$$\begin{pmatrix} & & * \\ & I_n & \vdots \\ * & \cdots & * \end{pmatrix}$$

Let k be the number of 1s in the appended column, so $0 \leq k \leq n$. There are $\binom{n}{k}$ distinct ways to arrange these k 1s. In order for the last row to be in the span of the first n rows, we can only add together combinations of the first n rows (as subtracting would produce a non-binary matrix). However, we cannot add two rows which have the appended 1s as their $n+1$th entry, as this would produce a non-binary matrix as well. Thus there are $n-k$ rows that do not have the appended ones to choose to create combinations, giving $\sum_{i=0}^{n-k}\binom{n-k}{i} = 2^{n-k}$ different combinations. To these, we can also add one of the k rows with appended ones (or not add any), producing $(k+1)2^{n-k}$ possibilities. Hence, $S(I_n)$, the total number of singular $(n+1) \times (n+1)$ matrices we can create from an n by n identity matrix, is

$$S(I_n) = \sum_{k=0}^{n}\binom{n}{k}[(k+1)2^{n-k}] < (n+1)\sum_{k=0}^{n}\binom{n}{k}2^{n-k} = (n+1)3^n. \qquad (4.6)$$

Therefore, the probability of a singular matrix here is at most $\frac{3^n(n+1)}{2^{2n+1}} = \frac{3^n(n+1)}{2(4^n)}$, about $(\frac{3}{4})^n$.

This applies to permutation matrices as well, as they contain the same rows as the identity matrix.

Although the identity matrix can produce many linear combinations, it does not produce the most, as we had wished. We created a computer program to compare $S(I_n)$ to the number generated by other $n \times n$ invertible matrices, and found that the identity matrix did not generate the least amount of invertible $(n+1) \times (n+1)$ matrices. Some 3×3 invertible matrices, like

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

produce 72 4×4 invertible matrices, compared with $N(I_3) = 74$.

4.2 $n \times n$ Singular Matrix to $(n+1) \times (n+1)$ Invertible Matrix

We want $F(n+1, n+1) \geq 2^{2n+1} F(n, n)$, which is impossible through expanding only invertible $n \times n$ matrices to invertible $(n+1) \times (n+1)$ matrices, as there are only 2^{2n+1} total possible $(n+1) \times (n+1)$ matrices that can be generated from the original $n \times n$ matrix, and they are not all nonsingular (e.g. appending a row of 0s to the matrix creates a singular matrix). On the other hand, $n \times n$ singular binary matrices can be enlarged to $(n+1) \times (n+1)$ invertible ones. Thus we look at the number of invertible binary matrices that can be generated from a singular $n \times n$ binary matrix. This will cancel out some of the singular matrices generated by invertible $n \times n$ binary matrices.

We take the matrix

$$B_n = \begin{pmatrix} 0 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & I_{n-1} & \\ 0 & & & \end{pmatrix} \tag{4.7}$$

as an example of $n \times n$ matrices of rank $n-1$, as it gives the most additive linear combinations of its rows. Given this matrix, if we enlarge it by adding a 0 as $(n+1)$th entry of the top row, it then has a row of 0s, which gives 2^{2n} singular matrices in the below form:

$$\begin{pmatrix} 0 & 0 & \cdots & 0 & 0 \\ 0 & & & & * \\ \vdots & & I_{n-1} & & \vdots \\ 0 & & & & * \\ * & * & \cdots & * & * \end{pmatrix}$$

If we enlarge it by adding a 1 as $(n+1)$th entry of the top row, we have a situation similar to that with the identity matrix:

$$\begin{pmatrix} 0 & 0 & \cdots & 0 & 1 \\ 0 & & & & * \\ \vdots & & I_{n-1} & & \vdots \\ 0 & & & & * \\ * & * & \cdots & * & * \end{pmatrix}$$

Here, let m be the number of the rest of the 1s that we add in the extra column. Thus there are $\binom{n-1}{m}$ different ways to arrange these m 1s. From the $n-m-1$ rows without an appended 1, we can choose any combination, giving $\sum_{i=0}^{n-m-1} \binom{n-m-1}{i} = 2^{n-m-1}$ combinations. To these we can add any of the $m+1$ rows with appended 1s, or none of them, producing $(m+2)2^{n-m-1}$ possibilities. Hence,

$$\begin{aligned} S(B_n) &= 2^{2n} + \sum_{m=0}^{n-1} \binom{n-1}{m} [(m+2)2^{n-m-1}] \\ &\leq 2^{2n} + (n+1) \sum_{m=0}^{n-1} \binom{n-1}{m} 2^{n-m-1} = 2^{2n} + (n+1)3^{n-1}. \end{aligned}$$

Thus, $N(B_n) \geq 2^{2n+1} - 2^{2n} - (n+1)3^{n-1} = 2^{2n} - (n+1)3^{n-1}$. This finishes the proof of Theorem 1.5.

4.3 Remarks on Conjecture 1.6

From an $n \times n$ singular binary matrix, there are at most 2^n different columns to append, and 2^{n+1} rows. Thus there are at most 2^{2n+1} $(n+1) \times (n+1)$ invertible binary matrices that can be generated from an $n \times n$ singular binary matrix, hence at most $2^{2n+1} \sum_{k=1}^{n-1} F(n,k)$. We compare this to the total number of $(n+1) \times (n+1)$ binary matrices, $2^{(n+1)^2}$, giving $\frac{\sum_{k=1}^{n-1} F(n,k)}{2^{n^2}}$. As $n \to \infty$, Komlos has shown this to approach 0 [2]. So when A_n is singular, $\lim_{n\to\infty} \frac{\sum_{rank A_n < n} N(A_n)}{2^{(n+1)^2}} = 0$.

On the other hand,

$$\begin{aligned} F(n+1, n+1) &= \sum_{rank A_n = n} N(A_n) + \sum_{rank A_n < n} N(A_n) \\ &\leq \sum_{rank A_n = n} N(A_n) + 2^{2n+1} \sum_{k=1}^{n-1} F(n,k). \end{aligned}$$

Dividing by $2^{(n+1)^2}$ gives

$$P(n+1) \leq \frac{\sum_{rank A_n = n} \frac{N(A_n)}{2^{2n+1}}}{2^{n^2}} + \frac{\sum_{k=1}^{n-1} F(n,k)}{2^{n^2}}.$$

As $n \to \infty$, $\lim_{n\to\infty} P(n+1) = 1$ and $\lim_{n\to\infty} \frac{\sum_{k=1}^{n-1} F(n,k)}{2^{n^2}} = 0$. Thus, $\overline{\lim}_{n\to\infty} \frac{\sum_{rankA_n=n} \frac{N(A_n)}{2^{2n+1}}}{2^{n^2}} \geq 1$. However, $\frac{\sum_{rankA_n=n} \frac{N(A_n)}{2^{2n+1}}}{2^{n^2}} \leq 1$, so $\underline{\lim}_{n\to\infty} \frac{\sum_{rankA_n=n} \frac{N(A_n)}{2^{2n+1}}}{2^{n^2}} \leq 1$. Therefore, the limit exists and $\lim_{n\to\infty} \frac{\sum_{rankA_n=n} \frac{N(A_n)}{2^{2n+1}}}{2^{n^2}} = 1$. That is to say, on average, Conjecture 1.6 is true.

In fact, since $\frac{N(A_n)}{2^{2n+1}} \leq 1$, the discussion above suggests that for most A_n, $\lim_{n\to\infty} \frac{N(A_n)}{2^{2n+1}} = 1$.

This is formulated in the following statement.

Proposition 4.1. *For any $\delta > 0$ and any $\varepsilon > 0$, there exists an N such that for any $n \geq N$, $\#\{A_n \mid A_n \text{ is invertible and } \frac{\mathrm{N(A_n)}}{2^{2n+1}} \leq 1-\delta\} < \varepsilon 2^{\mathrm{n}^2}$.*

We prove this by contradiction. Suppose that there exists a $\delta_0 > 0$ and an $\varepsilon_0 > 0$ such that for any N, there exists $n \geq N$ such that

$$\#\{A_n \mid A_n \text{ is invertible and } \frac{\mathrm{N(A_n)}}{2^{2\mathrm{n}+1}} \leq 1-\delta_0\} \geq \varepsilon_0 2^{\mathrm{n}^2}.$$

Let $S = \{A_n \mid A_n \text{ is invertible and } \frac{\mathrm{N(A_n)}}{2^{2\mathrm{n}+1}} \leq 1-\delta_0\}$ and S' be its complement.

Then

$$\sum_{rankA_n=n} \frac{N(A_n)}{2^{2n+1}} = \sum_S \frac{N(A_n)}{2^{2n+1}} + \sum_{S'} \frac{N(A_n)}{2^{2n+1}}.$$

Substituting in the bound gives

$$\begin{aligned} \sum_S \frac{N(A_n)}{2^{2n+1}} + \sum_{S'} \frac{N(A_n)}{2^{2n+1}} &\leq \#S(1-\delta_0) + \#S' = \#S + \#S' - \#S\delta_0 \\ &\leq 2^{n^2} - \delta_0\varepsilon_0 2^{n^2} = 2^{n^2}(1-\delta_0\varepsilon_0). \end{aligned}$$

This implies that

$$\lim_{n\to\infty} \frac{\sum_{rankA_n=n} \frac{N(A_n)}{2^{2n+1}}}{2^{n^2}} \leq 1-\delta_0\varepsilon_0 < 1,$$

which is a contradiction, as we have shown that $\lim_{n\to\infty} \frac{\sum_{rankA_n=n} \frac{N(A_n)}{2^{2n+1}}}{2^{n^2}} = 1$. This finishes the proof of the proposition.

5 Appendix: Tables and Data

Table 1. ($F(n,k)$ for $k = n$ and $k = n - 1$ and $P(n)$ data from [7])

$n \times n$ Matrices				
n	Total	$F(n,n)$	$F(n,n-1)$	$P(n)$
1	2^1	1	1	0.5
2	2^4	6	9	0.375
3	2^9	174	288	0.33984
4	2^{16}	22560	36000	0.34424
5	2^{25}	12514320	17760600	0.37296
6	2^{36}	28836612000	34395777360	0.41963
7	2^{49}	270345669985440	259286329895040	0.48023
8	2^{64}	10160459763342013440	7547198043595392000	0.55080

Table 2. ($N(A_n)$ for invertible A_n data from our computer program)

$n \times n$ Invertible Matrices to $(n+1) \times (n+1)$ Invertible Matrices						
n	$F(n,n)$	# of A_n	$N(A_n)$	Total $N(A_n)$	Average	$N(A_n) + S(A_n)$
2	6	6	17	102	17	32
3	174	72 96 6	72 74 80	12768	73.379	128

Table 3. ($N(A_n)$ for $n \times n$ rank $(n-1)$ A_n data from our computer program)

$n \times n$ rank $n-1$ Matrices to $(n+1) \times (n+1)$ Invertible Matrices						
n	$F(n,n-1)$	# of A_n	$N(A_n)$	Total $N(A_n)$	Average	$N(A_n) + S(A_n)$
2	9	9	8	72	8	32
3	288	216 72	32 40	9792	34	128

Acknowledgements: We would like to thank Prof. Zhenghan Wang for helpful email communications and bringing our attention to the references [4, 7], Prof. Terence Tao for answering our email question and pointing out the reference [6], and Prof. Gilbert Strang, author of our linear algebra textbook, and our teacher Mr. Kruidenier for introducing us to this problem.

References

[1] M.A. Khamsi, *Application of Invertible Matrices: Coding*, http://www.sosmath.com/matrix/coding/coding.html

[2] J. Komlos, *On the Determinant of (0,1) Matrices*, Studia Scientiarum Mathematicarum Hungarica 2 (1967), pp. 7-21.

[3] G. Strang, *Linear Algebra and Its Applications, 4th ed.*, Belmont: Brooks/Cole (2006), pp. 65.

[4] T. Tao, V. Vu, *On Random* ± 1 *Matrices: Singularity and Determinant*, Random Structures Algorithms 28 (2006), no. 1, 1–23.

[5] T. Tao, V. Vu, *On the Singularity Probability of Random Bernoulli Matrices*, J. Amer. Math. Soc. 20 (2007), no. 3, 603–628.

[6] T. Voigt, G. Ziegler, *Singular 0/1-Matrices, and the Hyperplanes Spanned by Random 0/1-Vectors*, Combinatorics, Probability and Computing 15 (2006), 463-471.

[7] M. Živković, *Classification of Small* $(0,1)$ *Matrices.*, Linear Algebra Appl. 414 (2006), no. 1, 310–346.