Determinants of binary matrices achieve every integral value up to $\Omega(2^n/n)$

Rikhav Shah

December 2018

Abstract

This work shows that the smallest natural number d_n that is not the determinant of some $n \times n$ binary matrix is at least $c\,2^n/n$ for $c = 1/201$. That same quantity naturally lower bounds the number of distinct integers D_n which can be written as the determinant of some $n \times n$ binary matrix. This asymptotically improves the previous result of $d_n = \Omega(1.618^n)$ and slightly improves the previous result of $D_n \geq 2^n/g(n)$ for a particular $g(n) = \omega(n^2)$ function.

1 Introduction

We take a binary matrix M to mean a matrix with all entries in $\{0, 1\}$. We investigate the range of the determinant, i.e. $\mathcal{D}_n = \{\det(M) : M \in \{0,1\}^{n\times n}\}$ [1]. Much work has sought to characterize $\mathcal{D}_n$. An old conjecture stated that $\mathcal{D}_n$ is a set of consecutive integers. A proof that $n = 7$ is a counter-example to this conjecture was published in 1969 by Metropolis [2], and an apparently independent proof was published by Carigen [1] in 1990. Carigen [1] also provides exact values of $\mathcal{D}_n$ for $n \leq 7$, and large subsets of $\mathcal{D}_n$ for $8 \leq n \leq 10$. In 2004, Orrick [3] finds exact values for $n = 8, 10$ and a larger subset for $n = 9$. Despite the aforementioned conjecture being false, it seems empirically that $\mathcal{D}_n$ does contain a large set of consecutive integers centered at 0, so one may ask what the smallest natural number d_n *not* in $\mathcal{D}_n$ is. For large n, the best lower bound on d_n known prior to this work is $\Omega(\phi^n)$ for $\phi = (1 + \sqrt{5})/2$ given by a construction due to Paseman [4]. For $n \leq 19$, the best known lower bounds are given by Zivkovic [6] and are optimal for $n \leq 9$.

Note that one has $|\mathcal{D}_n| \geq 2d_n - 1$ by observing $\mathcal{D}_n \supset \{1 - d_n, \cdots, d_n - 1\}$. The construction of Paseman thus guarantees $|\mathcal{D}_n| = \Omega(\phi^n)$. However, a stronger result on $|\mathcal{D}_n|$ is known. In particular, Tikhomirov [5] recently determined the related quantity

$$|\{M \in \{0,1\}^{n\times n} \mid \det(M) = 0\}| = 2^{n^2}\left(\frac{1}{2} + o(1)\right)^n.$$

His technique involved showing that for a uniformly randomly selected M, there is strong anti-concentration of $\langle \mathbf{h}, \mathbf{r}_n \rangle$, where $\mathbf{h}$ is a unit vector perpendicular to the first $n - 1$ rows of M with

[1] Many papers take entries of binary matrices to be ± 1. There exists a one-to-one correspondence between matrices with entries in {-1,1} of size $n + 1$ and matrices with entries in {0,1} of size n, such that the determinants of corresponding matrices are off by a constant factor of $(-2)^n$. In this way, results pertaining to one type of matrix easily carry over to results about the other.

nth row $\mathbf{r}_n$. In particular, one has for any t that $P(\det(M) = t) \leq \left(\frac{1}{2} + o(1)\right)^n$. This gives a lower bound of $(2 - o(1))^n$ on the size of the support of $\det M$, i.e.

$$|\mathcal{D}_n| \geq (2 - o(1))^n.$$

The probabilistic approach is non-constructive, however, and it is unclear if it can help determine any particular members of $\mathcal{D}_n$. This work provides a construction that guarantees $d_n \geq (2-o(1))^n$, which asymptotically improves the best known lower bound on d_n and slightly improves the best known lower bound on $|\mathcal{D}_n|$ by shrinking the $o(1)$ term so that the overall new bound is $d_n = \Omega(2^n/n)$ versus the old bound of $d_n \geq 2^n/g(n)$ for a particular $g(n) = \omega(n^2)$.

Let $\mathcal{M}(\mathbf{r}_2, \cdots, \mathbf{r}_n) \subset \{0,1\}^{n \times n}$ be the family of binary matrices whose ith row is given by $\mathbf{r}_i$ for each $i \in \{2, \cdots, n\}$. Note that there are 2^n matrices in such a family. Our task will be to select suitable rows $\mathbf{r}_i$ such that taking the determinant of each matrix in the family will result in few collisions. It will be easier to first construct rows $\mathbf{s}_i \in \{-1, 0, 1\}^n$, and from those construct $\mathbf{r}_i \in \{0,1\}^n$.

2 Lemmas

Lemma 2.1. *Let $\mathbf{r}_1, \cdots, \mathbf{r}_n$ be the rows of invertible square matrix M. If $\mathbf{v} \in \mathbb{R}^n$ is orthogonal to $\mathbf{r}_2, \cdots, \mathbf{r}_n$ with $\mathbf{v}(k) \neq 0$ for some k, then $\det(M) = c \sum_j \mathbf{v}(j)\mathbf{r}_1(j)$ where*

$$c = \mathbf{v}(k)^{-1} \det \left(\begin{bmatrix} - & e_k & - \\ - & \mathbf{r}_2 & - \\ & \vdots & \\ - & \mathbf{r}_n & - \end{bmatrix} \right) \tag{1}$$

where e_k is the kth row of the identity. In particular, c does not depend on $\mathbf{r}_1$.

Proof. Both $\mathbf{v}$ and the first column of M^{-1} are orthogonal to $\mathbf{r}_2, \cdots, \mathbf{r}_n$. Since $\mathbf{r}_2, \cdots, \mathbf{r}_n$ are linearly independent, the orthogonal complement of their span has dimension 1. Therefore, $\mathbf{v}$ and the first column of M^{-1} must be proportional. Recall that we can write M^{-1} in terms of the cofactor matrix C of M. Specifically, $M^{-1} = \frac{1}{\det(M)} C^T$. Thus the first column of M^{-1} is proportional to the first row of C. This allows us to claim that there is some c such that $C_{1j} = c\mathbf{v}(j)$ for all $j \in [n]$. By definition, C_{1j} does not depend on $\mathbf{r}_1$, so c does not depend on $\mathbf{r}_1$ either. The Laplace expansion of the determinant gives $\det(M) = \sum_j C_{1j}\mathbf{r}_1(j) = c\sum_j \mathbf{v}(j)\mathbf{r}_1(j)$. The formula for c follows immediately by setting $\mathbf{r}_1 = e_k$. □

Lemma 2.2. *Let $1 = b_1, \cdots, b_n$ be an integer sequence such that $b_{i+1} \leq b_1 + \cdots + b_i$ for $i \in [n-1]$. Then for every nonnegative integer $a \leq b_1 + \cdots + b_n$, there exists $S \subset [n]$ such that $a = \sum_{i \in S} b_i$.*

Proof. This is proved using induction. Assume it is true for $n-1$. Then, if $a \leq b_1 + \cdots + b_{n-1}$ we are already done. We thus restrict our attention to $a > b_1 + \cdots + b_{n-1} \geq b_n$. In this case, note that $a - b_n \leq b_1 + \cdots + b_{n-1}$, so applying the lemma for $n-1$ on $a - b_n$ again gives the result. □

Lemma 2.3. *Let* $\mathbf{r}_2, \cdots, \mathbf{r}_n \in \{0,1\}^n$ *be linearly independent such that*

$$D := \det\left(\begin{bmatrix} 1 & & \\ - & \mathbf{r}_2 & - \\ & \vdots & \\ - & \mathbf{r}_n & - \end{bmatrix}\right) = \pm 1.$$

If $\mathbf{v} \in \mathbb{R}^n$ *is orthogonal to* $\mathbf{r}_2, \cdots, \mathbf{r}_n$*, and* $\mathbf{v}(1), \cdots, \mathbf{v}(m)$ *satisfy* $0 \le \mathbf{v}(i+1) \le \mathbf{v}(1) + \cdots + \mathbf{v}(i)$ *for* $i \in [m-1]$ *and* $\mathbf{v}(1) = 1$*, then* $d_n > \mathbf{v}(1) + \cdots + \mathbf{v}(m)$ *where* d_n *is the smallest natural number not in* $\mathcal{D}_n$*.*

Proof. If $D = -1$, then swap $\mathbf{r}_2$ and $\mathbf{r}_3$ so that $D = 1$ and $\mathbf{v}$ is still orthogonal to all the rows. Let $\mathcal{M} := \mathcal{M}(\mathbf{r}_2, \cdots, \mathbf{r}_n)$. For any invertible $M \in \mathcal{M}$, let $\mathbf{r}_1$ be its top row. Then by Lemma 2.1, we can write for the same c that

$$\det(M) = c \sum_{j=1}^{n} \mathbf{v}(j)\mathbf{r}_1(j) = c \sum_{j \in S} \mathbf{v}(j) \quad \text{where } S = \{j \mid \mathbf{r}_1(j) = 1\}$$

In particular, since $\mathbf{v}(1) \neq 0$, Lemma 2.1 gives $c = D/\mathbf{v}(1) = 1$. By Lemma 2.2, we can select $\mathbf{r}_1$ so that $\det(M) = a$ for any positive integer $a \le \mathbf{v}(1) + \cdots + \mathbf{v}(m)$. □

3 Construction

We will first construct a matrix M whose rows $\mathbf{s}_i$ have entries in $\{-1, 0, 1\}$. Then we will construct a transformation T such that the rows $\mathbf{r}_i$ of TM have entries in $\{0, 1\}$. Finally we will find $\mathbf{v}$ that will satisfy the hypothesis of Lemma 2.3 along with the rows $\mathbf{r}_i$ of TM.

Fix an integer $k \ge 2$. Let the top row of M be $[1, 0, \cdots, 0]$. We separate the rest of the rows of M into three categories

$$\text{'Base' rows:} \qquad \mathbf{s}_i(j) = \begin{cases} -1 & \text{if } j = i \\ 1 & \text{if } j = i-1 \\ 0 & \text{o.w.} \end{cases} \qquad \text{for } i \in \{2, \cdots, k\}.$$

$$\text{'Recursive' rows:} \qquad \mathbf{s}_i(j) = \begin{cases} -1 & \text{if } j = i \\ 1 & \text{if } i-k \le j < i \\ 0 & \text{o.w.} \end{cases} \qquad \text{for } i \in \{k+1, \cdots, n-k\}.$$

$$\text{'Finishing' rows:} \qquad \mathbf{s}_i(j) = \begin{cases} 1 & \text{if } j = i \\ 1 & \text{if } i-k \le j \le n-k \\ 0 & \text{o.w.} \end{cases} \qquad \text{for } i \in \{n-k+1, \cdots, n\}.$$

The transformation $T = [t_{ij}]$ is defined by

$$t_{ij} = \begin{cases} 1 & i = j = 1 \\ 1 & \text{if } j \ge i > 1 \text{ and } i \equiv j \mod k \\ 0 & \text{o.w.} \end{cases}.$$

For example, for $k = 3, n = 10$ we have

$$M = \begin{bmatrix} 1 & & & & & & & & \\ 1 & -1 & & & & & & & \\ & 1 & -1 & & & & & & \\ 1 & 1 & 1 & -1 & & & & & \\ & 1 & 1 & 1 & -1 & & & & \\ & & 1 & 1 & 1 & -1 & & & \\ & & & 1 & 1 & 1 & -1 & & \\ & & & & 1 & 1 & 1 & 1 & \\ & & & & & 1 & 1 & & 1 \\ & & & & & & 1 & & \end{bmatrix}, \quad T = \begin{bmatrix} 1 & & & & & & & & & \\ & 1 & & & 1 & & & 1 & & \\ & & 1 & & & 1 & & & 1 & \\ & & & 1 & & & 1 & & & 1 \\ & & & & 1 & & & 1 & & \\ & & & & & 1 & & & 1 & \\ & & & & & & 1 & & & 1 \\ & & & & & & & 1 & & \\ & & & & & & & & 1 & \\ & & & & & & & & & 1 \end{bmatrix}.$$

Note that the top row of T is $[1, 0, \cdots, 0]$, so the top row of TM is the same as the top row of M, which is also $[1, 0, \cdots, 0]$. It is worth remarking that the case of $k = 2$ is essentially equivalent to Paseman's construction.

Lemma 3.1. *The rows $\mathbf{r}_i$ of TM have entries in {0,1}.*

Proof. First we noted above that $\mathbf{r}_1 = [1, 0, \cdots 0]$. Then for $i \geq 2$, the definitions of T and M give

$$\mathbf{r}_i = \mathbf{s}_i + \mathbf{s}_{i+k} + \cdots + \mathbf{s}_{i+k\lfloor \frac{n-i}{k} \rfloor}.$$

We now show $\mathbf{r}_i(j) \in \{0, 1\}$ in each of several cases. For $i \geq n-k$ we just have $\mathbf{r}_i = \mathbf{s}_i \in \{0, 1\}^n$ so are already done in that case. For $j \geq n-k$, note that the last k columns of M match the last k columns of the identity, so the last k columns of TM exactly match those of TM, so all those entries are in $\{0, 1\}$.

Now fix any $i, j \leq n-k-1$. Note that the support of $\mathbf{s}_{i+lk}$ is a subset of $\{i+(l-1)k, \cdots, i+lk\}$. We consider the case of $j = i + lk$ for some l and $j \in \{i + (l-1)k + 1, \cdots, i + lk - 1\}$ for some l separately. For $j = i + lk$ we have

$$\mathbf{r}_i(j) = \mathbf{s}_i(j) + \mathbf{s}_{i+k}(j) + \cdots + \mathbf{s}_{i+k\lfloor \frac{n-i}{k} \rfloor}(j) = \mathbf{s}_{i+lk}(j) + \mathbf{s}_{i+(l+1)k}(j) = -1 + 1 = 0.$$

For $j \in \{i + (l-1)k + 1, \cdots, i + lk - 1\}$, we note that j lies in the support of $\mathbf{s}_{i+lk}$ and no other rows. So $\mathbf{r}_i(j) = 1$.

□

Lemma 3.2. *If $\mathbf{v}$ is orthogonal to $\mathbf{s}_2, \cdots, \mathbf{s}_n$, then it is orthogonal to $\mathbf{r}_2, \cdots, \mathbf{r}_n$.*

Proof. By hypothesis, $M\mathbf{v} = [\mathbf{s}_1 \cdot \mathbf{v}, 0, \cdots, 0]^T$. Since T is upper triangular, $T[\mathbf{s}_1 \cdot \mathbf{v}, 0, \cdots, 0]^T = [\mathbf{s}_1 \cdot \mathbf{v}, 0, \cdots, 0]^T$ so $TM\mathbf{v} = [\mathbf{s}_1 \cdot \mathbf{v}, 0, \cdots, 0]^T$ as required. □

Before we proceed, we define the k-step Fibonacci sequence.

Definition 3.1. *Let $F_k(j)$ be the jth term of the k-step Fibonacci sequence. That is, let $F_k(j) = 1$ for $j \leq k$ and $F_k(j) = \sum_{j'=j-k}^{j-1} F_k(j')$ for $j > k$.*

Theorem 3.3.

$$d_n > \sup_k F_k(1) + \cdots + F_k(n-k).$$

Proof. We start by constructing $\mathbf{v}$ that is orthogonal to $\mathbf{s}_2, \cdots, \mathbf{s}_n$. Let $\mathbf{v}(1) = 1$. Orthogonality with the 'base' rows requires

$$\mathbf{v}(i-1) = \mathbf{v}(i) \quad \text{for } i \in \{2, \cdots, k\}.$$

Orthogonality with the 'recursive' rows requires

$$\sum_{j=i-k}^{i-1} \mathbf{v}(j) = \mathbf{v}(i) \quad \text{for } i \in \{k+1, \cdots, n-k\}.$$

Finally orthogonality with the finishing rows requires

$$-\sum_{j=i-k}^{n-k} \mathbf{v}(j) = \mathbf{v}(i) \quad \text{for } i \in \{n-k+1, \cdots, n\}.$$

Note each entry in $\mathbf{v}$ is defined solely in terms of the entries before it. Further note that the definitions of $\mathbf{v}(j)$ and $F_k(j)$ match for $j \leq n-k$, so we actually have

$$\mathbf{v}(j) = F_k(j) \text{ for } j \leq n-k.$$

Then since all the terms are positive, $\mathbf{v}$ satisfies $\mathbf{v}(i) \leq \mathbf{v}(1) + \cdots + \mathbf{v}(i-1)$ for $i \leq n-k$. By Lemma 3.2, we have that $\mathbf{v}$ is orthogonal to $\mathbf{r}_2, \cdots, \mathbf{r}_n$. Since M and T are triangular with ± 1 on the diagonals, we have $\det(TM) = \pm 1$. The hypotheses of Lemma 2.3 are thus satisfied for $m = n-k$, so we have

$$d_n > \mathbf{v}(1) + \cdots + \mathbf{v}(n-k) = F_k(1) + \cdots + F_k(n-k).$$

Taking the supremum over possible values of k gives the desired result. □

We finish with an approximation of $F_k(j)$.

Lemma 3.4. *$F_k(n) > \frac{1}{5}\alpha_k^n$ for all $k \geq 2, n \geq 8$ where α_k is the unique zero of $z - 2 + z^{-k}$ with norm greater than 1. Furthermore, $\alpha_k \in [2 - 2^{1-k}, 2)$.*

Proof. If we modify the definition of the base case of $F_k(n)$ such that $F_k(n) = 0$ for $k \leq 0$ and $F_k(1) = F_k(2) = 1$, and one starts recursing at $n = 3$, then the exact formula is known to be

$$\left\lfloor \alpha_k^{n-1} \frac{\alpha_k - 1}{k(\alpha_k - 2) + \alpha_k} \right\rfloor. \tag{2}$$

Since our base case is larger, (2) is a lower bound on our definition of $F_k(n)$.

We can approximately locate α_k using Rouche's theorem. Let $K = \{z \in \mathbb{C}\,;\, |z-2| \leq 2^{1-k}\}$. Then on ∂K we have $|z^{-k}| \leq (2 - 2^{1-k})^{-k} < 2^{1-k} = |z-2|$. The number of zeros of $z-2$ inside K is one (it is $z = 2$), so $z - 2 + z^{-k}$ has exactly zero inside K as well. It is the unique zero of norm more than one. This implies $|\alpha_k - 2| \leq 2^{1-k}$. Finally $z - 2 + z^{-k}$ is negative at $z = 1.5$ and positive at $z = 2$, so α_k is real and less than 2.

The coefficient on α_k^{n-1} in (2) is decreasing in α_k, so we can bound it by

$$\frac{\alpha_k - 1}{k(\alpha_k - 2) + \alpha_k} > \frac{2-1}{k(2-2)+2} = \frac{1}{2}.$$

Thus

$$F_k(n) > \frac{1}{2}\alpha_k^{n-1} - 1 > \frac{1}{4}\alpha_k^n - 1.$$

For $k \geq 2, n \geq 8$ we have $\alpha_k^n > 20$, i.e. $\frac{1}{4}\alpha_k^n - 1 > \frac{1}{5}\alpha_k^n$.

□

Corollary 3.5.

$$d_n > c\,2^n/n$$

for $c = 1/201$, $n \geq 8$.

Proof. We take the logarithm of d_n and apply Lemma 3.4.

$$\begin{aligned}
\log(d_n) &\geq \log\left(F_k(1) + \cdots + F_k(n-k)\right) \\
&\geq \log F_k(n-k+1) \\
&\geq (n-k+1)\log\alpha_k - \log 5 \\
&= n\left(\left(1 - \frac{k+1}{n}\right)\log\alpha_k - \frac{1}{n}\log 5\right) \\
&\geq n\left(\left(1 - \frac{k+1}{n}\right)\log\left(2 - 2^{1-k}\right) - \frac{1}{n}\log 5\right) \\
&= n\left(\log\left(2 - 2^{1-k}\right) - \frac{(k+1)\log\left(2 - 2^{1-k}\right) + \log 5}{n}\right)
\end{aligned}$$

Set $k = \lfloor \log_2 n \rfloor$. Then one has

$$\log\left(2 - 2^{1-\lfloor \log_2 n \rfloor}\right) \geq \log 2 - \frac{3}{n}$$

and for $\epsilon = \log(10e^3)/\log n$, one has

$$\frac{3 + (k+1)\log\left(3 - 2^{1-k}\right) + \log 5}{n} \leq \frac{3 + (k+1)\log 2 + \log 5}{n} \leq \frac{\log n + \log(10e^3)}{n} = (1+\epsilon)\frac{\log n}{n}.$$

Thus $\log(d_n) \geq n\log 2 - (1+\epsilon)\log n$. Exponentiating gives $d_n \geq 2^n/n^{1+\epsilon}$, and using the numerical approximation $n^\epsilon = 10e^3 < 201$ yields the final result. □

4 Acknowledgements

The author thanks Asaf Ferber for his suggestion of this topic, funding, advisement, and guidance.

References

[1] Rob Craigen. The range of the determinant function on the set of $n \times n$ $(0, 1)$-matrices. *JCMCC. The Journal of Combinatorial Mathematics and Combinatorial Computing*, 8, Jan 1990.

[2] N. Metropolis. Spectra of determinant values in (0,1) matrices. *Computers in Number Theory: Proceedings of the Science Research Atlas Symposium No. 2 held at Oxford, 18-23 August, 1969, Academic Press, London*, pages 271–276, 1969.

[3] William P. Orrick. The maximal {-1,1}-determinant of order 15. *Metrika*, 62(2):195–219, Nov 2005. `https://arxiv.org/abs/math/0401179`.

[4] Gerhard Paseman. A different approach to hadamard's maximum determinant problem. In *ICM*, Aug 1998. NB: the relevant portion can be found at `https://web.archive.org/web/20070216021103/http://grpmath.prado.com/Lemmas.html`.

[5] Konstantin Tikhomirov. Singularity of random bernoulli matrices. *Annals of Mathematics*, 191(2):593–634, 2020. `https://arxiv.org/abs/1812.09016`.

[6] Miodrag Živković. Classification of small (0,1) matrices. *Linear Algebra and its Applications*, 414(1):310 – 346, 2006. `https://arxiv.org/abs/math/0511636`.