Computation of Maximal Determinants of Binary Circulant Matrices

Richard P. Brent* Adam B. Yedidia†

Abstract

We describe algorithms for computing maximal determinants of binary circulant matrices of small orders. Here "binary matrix" means a matrix whose elements are drawn from $\{0,1\}$ or $\{-1,1\}$. We describe efficient parallel algorithms for the search, using Duval's algorithm for generation of necklaces and the well-known representation of the determinant of a circulant in terms of roots of unity. Tables of maximal determinants are given for orders ≤ 48. Our computations extend earlier results and disprove two plausible conjectures.

1 Introduction

A *circulant* matrix $A = (a_{j,k})$ of order n is an $n \times n$ matrix whose elements $a_{j,k}$ depend only on $(k-j) \bmod n$. Thus, an $n \times n$ circulant is a matrix of the form $A = (a_{(k-j) \bmod n})_{0 \le j,k < n}$. Circulants arise in various applications in signal processing and combinatorics, and have a close connection with Fourier transforms. The set of all circulants of order n (with elements in some fixed ring R) form a commutative algebra, since the sum and product of two circulants is a circulant, and it is easy to see that multiplication of circulants is commutative.

*Mathematical Sciences Institute, Australian National University, Canberra, ACT 2600, Australia, and CARMA, University of Newcastle, Callaghan, NSW 2308, Australia. circulants@rpbrent.com

†Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology, Cambridge, Massachusetts, USA. adamyedidia@gmail.com

We write $\text{circ}(a_0, a_1, \ldots, a_{n-1})$ for the circulant $(a_{(k-j) \bmod n})_{0 \le j,k < n}$ whose first row is $(a_0, a_1, \ldots, a_{n-1})$.

By a *binary* matrix we mean a matrix whose elements are in one of the sets $S_{01} := \{0, 1\}$ or $S_{\pm 1} := \{-1, 1\}$. It will be clear from the context which of these two cases is being considered. A *binary circulant* is a circulant matrix whose elements are in S_{01} or $S_{\pm 1}$.

There is a natural one-to-one correspondence between the integers $\{0, 1, \ldots 2^n - 1\}$ and the binary circulant matrices of order n. More precisely, if $N \in \{0, 1, \ldots, 2^n - 1\}$ has the representation

$$N = \sum_{j=0}^{n-1} 2^{n-1-j}\, b_j,$$

so may be written in binary as $b_0 \ldots b_{n-1}$, we associate N with $\text{circ}(a_0, \ldots, a_{n-1})$, where $a_j = b_j$ in the case of S_{01}, and $a_j = 2b_j - 1$ in the case of $S_{\pm 1}$.

The *maximal determinant problem* is concerned with the maximal value of $|\det(A)|$ for an $n \times n$ binary matrix A. The *Hadamard bound* [14] states that, in the case of binary matrices A over $\{\pm 1\}$, we have

$$|\det(A)| \le n^{n/2}. \tag{1}$$

Moreover, Hadamard's inequality is sharp for infinitely many n, for example powers of two (Sylvester [26]) or n of the form $q+1$ where q is a prime power and $q \equiv 3 \bmod 4$ (Paley [22]).

There is a well-known connection between the determinants of $\{0, 1\}$-matrices of order n and $\{\pm 1\}$-matrices of order $n+1$. This implies that an $(n+1) \times (n+1)$ $\{\pm 1\}$-matrix always has determinant divisible by 2^n. See [18] or [21, Lemma 3.1] for details. We give an example with $n = 3$, starting with an $n \times n$ binary matrix B and ending with an $(n+1) \times (n+1)$ $\{\pm 1\}$-matrix A, with $\det(A) = 2^n \det(B)$.

$$B = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} \xrightarrow{\text{double}} \begin{pmatrix} 2 & 0 & 2 \\ 2 & 2 & 0 \\ 0 & 2 & 2 \end{pmatrix}$$

$$\xrightarrow{\text{border}} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 2 & 0 & 2 \\ 0 & 2 & 2 & 0 \\ 0 & 0 & 2 & 2 \end{pmatrix} \underset{\text{first row}}{\xrightarrow{\text{subtract}}} \begin{pmatrix} 1 & 1 & 1 & 1 \\ -1 & 1 & -1 & 1 \\ -1 & 1 & 1 & -1 \\ -1 & -1 & 1 & 1 \end{pmatrix} = A.$$

The doubling step is the only step where the determinant changes, and there it is multiplied by 2^n.

Thus, Hadamard's bound (1) gives the bound

$$|\det(B)| = |\det(A)|/2^n \le (n+1)^{(n+1)/2}/2^n, \tag{2}$$

which applies for all $\{0,1\}$-matrices B of order n. We shall refer to both (1) and (2) as *Hadamard's inequality*, since it will be clear from the context which inequality is intended.[1]

The mapping from $\{0,1\}$-matrices to $\{\pm 1\}$-matrices is reversible if we are allowed to normalise the first row and column of the $\{\pm 1\}$-matrix by changing the signs of rows/columns as necessary.

The transformation illustrated above (or its reverse) does *not* preserve any circulant structure.

Hadamard matrices are square matrices with entries in $S_{\pm 1}$ and mutually orthogonal rows. The order of a Hadamard matrix is 1, 2, or a multiple of 4. It is not known whether a Hadamard matrix of order $4k$ exists for every positive integer k (this is the *Hadamard conjecture*).

Various constructions for Hadamard matrices use circulant matrices. For example, the first Paley construction [22] uses a circulant matrix of order p, where p is a prime, $p \equiv 3 \bmod 4$, to construct a Hadamard matrix of order $p+1$. (The Paley construction also works for prime powers, e.g. $27 = 3^3$, but does not involve circulants in such cases.) Fletcher, Gysin and Seberry [12] use two circulants and a border of width two to construct Hadamard matrices. The Williamson construction [27] requires four matrices $A, \ldots, D$ which satisfy certain conditions, and for computational reasons these matrices are usually taken to be circulants.

It is well-known that the (unnormalised) eigenvectors of $\mathrm{circ}(a_0, \ldots, a_{n-1})$ are given by $v_j = (1, \omega^j, \omega^{2j}, \ldots, \omega^{(n-1)j})^T$, $0 \le j < n$, where ω is a primitive n-th root of unity. For example, in $\mathbb{C}$ we can take $\omega := \exp(2\pi i/n)$. It follows that the eigenvalues are

$$\lambda_j = a_0 + a_1\omega^j + \cdots + a_{n-1}\omega^{(n-1)j},\ 0 \le j < n, \tag{3}$$

and the determinant is

$$\prod_{j=0}^{n-1} \lambda_j = \prod_{j=0}^{n-1} f(\omega^j), \tag{4}$$

[1] In fact, Hadamard in [14] proved a more general inequality than (1), and as far as we are aware he never stated (2) explicitly. A simple proof of (1) is given by Cameron [7].

where

$$f(z) := \sum_{k=0}^{n-1} a_k z^k.$$

The polynomial $f(z)$ is called the *associated polynomial* of the circulant.

Using (4) to compute $\det(A)$ for a circulant matrix A takes $O(n^2)$ arithmetic operations, whereas Gaussian elimination does not take advantage of the circulant structure and takes of order n^3 operations. If we are considering binary matrices, whose determinants are integers, it is necessary to perform the operations in $\mathbb{C}$ to sufficient precision to obtain a result with absolute error less than 1/2, so that the correct result can be found by rounding to the nearest integer. From the Hadamard bounds (1)–(2), this means we have to work with of order $n \log n$ bits of precision.

To avoid the problem of rounding errors altogether, we can work over a finite field. If p is a prime such that $p \equiv 1 \bmod n$, and ρ is a primitive root (mod p), then[2]

$$\omega = \rho^{(p-1)/n} \bmod p$$

is a primitive n-th root of unity in the finite field F_p, and we can use (4) to compute $\det(A) \bmod p$. If U is an upper bound on $|\det(A)|$, and $p \geq 2U+1$, then the result mod p is sufficient to determine $\det(A)$. Thus, if we use a Hadamard bound for U, the prime p should have of order $n \log n$ bits. Alternatively, we could use several smaller primes with a sufficiently large product, and reconstruct the result using the Chinese Remainder Theorem.[3]

2 Lyndon words and necklaces

The usual definition of a *Lyndon word* is a nonempty string that is strictly smaller in lexicographic order than all of its proper rotations. Thus, the first six Lyndon words over S_{01} are 0, 1, 11, 101, 111, and 1111. Lyndon

[2]It is not necessary to know a primitive root (mod p). We can choose a random a, compute $\omega = a^{(p-1)/n}$, and check if $1, \omega, \omega^2, \ldots, \omega^{n-1}$ are distinct (mod p). If not, reject ω and repeat with another random a. In this way we work in a (small) group of order n, instead of a (large) group of order $p-1$, and there is no need to factor $p-1$. The expected number of iterations is $n/\phi(n) = O(\log \log n)$.

[3]Tests indicate that for $n \leq 50$ it is faster to use a single prime. One reason for this is that the value $\det(A)$ needs to be reconstructed for each circulant A, so the cost of the reconstruction steps is not negligible.

words were introduced by Shirshov [24] (who called them "regular words") and Lyndon [17] (who called the "standard lexicographic sequences").

Since we consider words of a fixed length n, it is convenient to use the concept of a (binary) necklace [29]. We say that $w = w_0 \dots w_{n-1}$ is a *necklace of length* n if w is not larger (in the lexicographic order) than any of its rotations. This corresponds to Duval's "representative of a class of words of length n" [9, (3) on pg. 258], where two words are said to be in the same class if one is a rotation of the other.

For example, according to our definition, the six necklaces of length 4 over S_{01} are 0000, 0001, 0011, 0101, 0111, and 1111. It can be seen that, if we strip off leading zeros, we obtain the first six Lyndon words. Thus, the concepts of "Lyndon word" and "necklace" are closely related, and algorithms for one may often by modified to apply to the other.

The number $K(n)$ of necklaces of length n over a binary alphabet is

$$K(n) = \frac{1}{n} \sum_{d|n} 2^{n/d} \phi(d) \simeq 2^n/n, \tag{5}$$

where ϕ is Euler's phi function. $K(n)$ is tabulated in OEIS A000031 [25].

If A is a circulant, then $|\det(A)|$ is invariant under rotations of the first row $(a_0, \dots, a_{n-1})$. Thus, when searching for circulants of order n with maximal determinants, it is sufficient to consider circulants whose first row is a necklace of length n. From (5), this saves a factor of approximately n.

In our computations we use two nontrivial algorithms related to Lyndon words/necklaces. One is the algorithm of Booth [5], which determines in linear time if a word $w = w_0 \dots w_{n-1}$ is in fact a necklace.[4] Booth's algorithm is closely related to the initial phase of the Knuth, Morris and Pratt fast pattern-matching algorithm [15].

The other algorithm that we use is Duval's algorithm [9] which, given a necklace of length n, returns the next necklace (of length n) in lexicographic order[5], in amortised (i.e. average) constant time, see [4]. Using Duval's algorithm we can cycle through all necklaces of length n in time $O(2^n/n)$.

Other algorithms could be used. For example, Shiloach [23] gives an algorithm that reduces the number of comparisons used by Booth's algorithm.

[4] We use a simplified version of Booth's algorithm since we do not need to know the rotation that would convert w into a necklace.

[5] Duval's paper [9] considers Lyndon words but, using [9, comment (3) on pg. 258], we easily get a similar algorithm for necklaces.

We used Booth's algorithm because it was sufficient for our purposes, and simpler to implement than Shiloach's algorithm. The overall complexity of our algorithms is dominated by the time required to evaluate determinants using (4), not by the time required to check or enumerate necklaces.

3 Fast evaluation of circulant determinants

Standard algorithms of linear algebra, such as Gaussian elimination, require of order n^3 operations to evaluate the determinant of an $n \times n$ matrix A. Using formula (4), this can be reduced to order n^2 if A is a circulant. In fact, using the fast Fourier transform (FFT), $O(n \log n)$ operations suffice.

However, in our application we can do even better. Because Duval's algorithm takes constant time (on average), the number of symbols that are changed as we go from one necklace to the next is $O(1)$ on average.[6] Thus, each λ_j value given by (3) can be updated in $O(1)$ operations (on average), and the determinant, given by (4), can be updated with $O(n)$ operations (on average). Since there are $\simeq 2^n/n$ necklaces of length n, the computation of all the relevant determinants can be done with $O(2^n)$ operations. The cost of precomputing a table of powers ω^{jk} $(0 \le j, k < n)$, is negligible.

Note that we used the term "operations" rather than "time", because the arithmetic operations need to be performed using of order $n \log n$ bits of precision, as noted above. Thus, the overall complexity is $O(2^n M(n \log n))$, where $M(N)$ is the time required to multiply N-bit numbers.

In theory, a slightly better complexity can be attained by using several small primes and reconstructing the result via the Chinese Remainder Theorem. However, the cost of $O(2^n/n)$ reconstructions must be taken into account. In practice, n can not be very large, because of the exponentially growing factor 2^n in the complexity, so the difference between the two approaches is essentially an implementation-dependent constant factor.

[6] We find experimentally that the mean number of symbols changed is $2 + O(n/2^n)$ as $n \to \infty$. The limiting value 2 is the same as the mean number of bits changed when counting up in binary.

4 Parallel algorithms

Suppose we wish to use $P \geq 1$ processors in parallel. If the $K \simeq 2^n/n$ necklaces of length n are $W_0 = 0\ldots0, W_1, W_2, \ldots, W_{K-1} = 1\ldots1$, we would like to ask processor q $(0 \leq q < P)$ to compute the determinants corresponding to necklaces $W_{\lfloor qK/P \rfloor}, \ldots, W_{\lfloor (q+1)K/P \rfloor - 1}$. The problem is how to determine the starting point $W_{\lfloor qK/P \rfloor}$ for processor q, without enumerating $W_1, W_2, \ldots, W_{\lfloor qK/P \rfloor}$. A polynomial-time algorithm for this problem is claimed in [16], but it is very complicated. We preferred to adopt a simpler approach which is much easier to implement and sufficient in practice.

The idea is to take a random sample of (say) $T := 4000P^2$ necklaces (each of length n). Sort the sample, and then divide it into P equal-sized segments. Modify the initial segment to start with $W_0 = 0\ldots0$ and the final segment to end with $W_{K-1} = 1\ldots1$. Thus, each processor has the same number $\lfloor K/P \rfloor$ words to process, apart from a small sampling error which is negligible in practice. Also, we know the necklace starting each segment, so we can use Duval's algorithm to enumerate all necklaces in a segment.

We describe how to randomly sample the set of all necklaces of length n in such a manner that each necklace occurs in the sample with equal probability. Generate a random binary string of length n, and test (using Booth's algorithm) if it corresponds to a necklace. If so, the string is accepted. Otherwise, the string is rejected and we try again. The process is repeated until we have the desired number T of necklaces (not necessarily distinct). Clearly each necklace is equally likely to appear in the final list. Since the probability that a random binary string is a necklace is close to $1/n$, the number of random binary strings that are needed is of order nT. What we have described is, in fact, a simple example of Von Neumann's *rejection method*, first described by Forsythe in [19]. Other examples may be found in Devroye's book [8].

5 Computational results

In Tables 1–2 we give computational results for the maximal determinants $D_{01}(n)$ of $\{0,1\}$-circulants of order $n \leq 49$. The third column of each table gives the ratio $D_{01}(n)/U_{01}(n)$, where $D_{01}(n)$ is the maximum of $|\det(B)|$ for $\{0,1\}$-circulants B of order n, and $U_{01}(n)$ is an upper bound on $D_{01}(n)$.

Similarly, in Tables 3–4 we give computational results for the maximal determinants $D_{\pm1}(n)$ of $\{\pm1\}$-circulants of order $n \le 48$. Here the third column is the ratio $D_{\pm1}(n)/U_{\pm1}(n)$, where $U_{\pm1}(n)$ is an upper bound on $D_{\pm1}(n)$. In Tables 3–4 we scale the determinants of $\{\pm1\}$-circulants by dividing by the known factor 2^{n-1}. In the last column of Table 3, "−" and "+" are used as abbreviations for -1 and $+1$ respectively.

The bounds $U_{01}(n)$ and $U_{\pm1}(n)$ are defined as follows. Let

$$\mathrm{HBE}(n) := \begin{cases} n^{n/2} \text{ if } n \equiv 0 \bmod 4, \\ 2(n-1)\,(n-2)^{(n-2)/2} \text{ if } n \equiv 2 \bmod 4, \\ (2n-1)^{1/2}\,(n-1)^{(n-1)/2} \text{ otherwise.} \end{cases} \tag{6}$$

Then $\mathrm{HBE}(n)$ is an upper bound on $|\det(A)|$ for $\{\pm1\}$-matrices A of order n. The case $n \equiv 0 \bmod 4$ is due to Hadamard [14]; the case $n \equiv 2 \bmod 4$ is due to Ehlich [10] and Wojtas [28]; and the remaining case (n odd) is due to Barba [3], Ehlich [10], and Wojtas [28]. We do not use Ehlich's slightly sharper, but more complicated, bound that applies when $n \equiv 3 \bmod 4$. For this bound, see Ehlich [11] or Orrick [20].

In view of the discussion in §1, we take

$$U_{\pm1}(n) := 2^{n-1}\lfloor HBE(n)/2^{n-1}\rfloor$$

and

$$U_{01}(n) := \lfloor HBE(n+1)/2^n\rfloor.$$

It is an open question whether $D_{\pm1}(n)$ attains the bound $U_{\pm1}(n)$ for any $n > 13$. (If we restrict attention to the cases $n \equiv 0 \bmod 4$, this is the *circulant Hadamard* problem.) On the other hand, $D_{01}(p) = U_{01}(p)$ for all primes $p \equiv 3 \bmod 4$. This follows from the first *Paley construction* [22], which constructs a Hadamard matrix of order $p+1$ with a circulant submatrix of order p. Inspection of Tables 1–2 reveals that $D_{01}(n) = U_{01}(n)$ in some other cases, specifically $n \in \{1, 2, 4, 15, 35\}$.

Table 2 extends the list of $D_{01}(n)$ values given for $n \le 37$ in OEIS A086432 and the associated b-file [1]. Table 4 extends the list of $D_{\pm1}(n)/2^{n-1}$ values given for $n \le 28$ in OEIS A215897 [2]. This implies a corresponding extension for OEIS A215723, which lists the unscaled values $D_{\pm1}(n)$.

As an indication of the time required to compute the tables, we note that the computation of $D_{01}(46)$ using our parallel program (implemented in C using GMP [13]) took 1394 processor-hours (87.1 hours × 16 processors) using a 2.6 GHz Intel Xeon E5-2697A. The computation times for other orders n may be estimated as they are roughly proportional to 2^n. For verification, all the values given in the tables for orders $n \le 46$ were computed at least twice, using different programs and/or different prime moduli p.

6 Some conjectures

In this section we discuss, and disprove, some plausible conjectures.

Conjecture A

From the third column of Table 1, the determinant of a $\{0, 1\}$-circulant can attain the upper bound $U_{01}(n)$ in the cases $n \in \{1, 2, 3, 4, 7, 11, 15, 19\}$. The Paley construction explains this for $n = 3, 7, 11, 19$, and larger cases where n is a prime and $n \equiv 3 \bmod 4$. However, it does not explain the case $n = 15 = 3 \times 5$. Also, the upper bound is not attained for $n = 27 = 3^3$. Thus, a plausible conjecture is that the upper bound can be attained whenever $n \equiv 3 \bmod 4$ is square-free. A weaker conjecture would replace "square-free" by "product of at most two distinct primes". Some support is provided by the computation for $n = 35 = 5 \times 7$, where we find that $D_{01}(35) = U_{01}(35)$.

Our computation for $n = 39$ disproves these conjectures, since $39 = 3 \times 13$ is a product of two distinct primes, but $D_{01}(39) < U_{01}(39)$.

Conjecture B, case $[0, 1]$

When considering maximal determinants of matrices with real elements in the interval $[0, 1]$, we can see that the maximum occurs at extreme points of the polytope.[7] To prove this, we need only note that the determinant $\det(A)$ of a square matrix $A = (a_{j,k})$ is a linear function of each variable $a_{j,k}$ considered separately. Thus, if a local maximum of $\det(A)$ occurs for some $a_{j,k} \in (0, 1)$, we can replace $a_{j,k}$ by (at least one of) 0 or 1 without decreasing $\det(A)$.

This argument does not apply if A is restricted to be a circulant of order $n > 1$, because then the free parameters are just the elements $a_0, \ldots, a_{n-1}$ of the first row of A, and $\det(A)$ is *not* a linear function of each a_j considered

[7] This is already implicit in Hadamard [14].

separately. For example, if $n = 2$ we have $\det(A) = a_0^2 - a_1^2$. Nevertheless, inspection of small cases suggests the conjecture that the maximum of $|\det(A)|$ occurs at extreme points of the n-dimensional polytope.

We were unable to prove the conjecture, so wrote a program to check it numerically, and found that, in general, the conjecture is false.

The idea is as follows. Consider all possible circulants A of order n with entries in $\{0, 1\}$. If $\det(A) = \pm D_{01}(n)$, check if a small perturbation of a_0 towards the interior of the polytope would increase $|\det(A)|$. Although such behaviour is rare, it does occur.[8]

The smallest examples occur for $n = 9$. Consider $A = \mathrm{circ}(a_0, \ldots, a_8)$ with $(a_0, \ldots, a_8) = (0, 0, 0, 1, 1, 1, 1, 0, 1)$. We have $\det(A) = 95 = D_{01}(9)$, but $\partial \det(A)/\partial a_0 = 9$. If $a_0 = \varepsilon$ for some small ε, then $|\det(A(\varepsilon))| = 95 + 9\varepsilon + O(\varepsilon^2)$, so $|\det(A(\varepsilon))| > 95$ for sufficiently small $\varepsilon > 0$. In fact, $|\det(A(0.241))| > 96.757$.

For $n = 10$, an example is $A = \mathrm{circ}(0, 0, 1, 0, 0, 1, 1, 1, 1, 0)$, $\det(A) = 275$. Replacing a_0 by $\varepsilon = 0.112$, we obtain $\det(A(\varepsilon)) > 279.4$.

We found examples of such behaviour for $n = 9, 10$ and no other $n < 48$. However, our search for interior extrema was not exhaustive, so there may be other $n < 48$ for which the maximum determinant does not occur at an extreme point of $[0, 1]^n$.

Conjecture B, case $[-1, 1]$

Replacing $[0, 1]$ by $[-1, 1]$, we find similar behaviour for $n = 2, 9, 10, 11, 18, 22$ and no other $n < 48$. The case $n = 2$ is trivial because, for circulants of order 2 over $S_{\pm 1}$, we necessarily have $\det(A) = 0$ at the extreme points $(a_0, a_1) = (\pm 1, \pm 1)$.

The other cases are non-trivial. For example, if $n = 9$, consider

$$A(\varepsilon) := \mathrm{circ}(1 - \varepsilon, 1, -1, 1, -1, -1, 1, 1, 1).$$

We find that

$$\det(A(\varepsilon)) = 6912 + 4608\varepsilon + O(\varepsilon^2),$$

so sufficiently small $\varepsilon > 0$ gives $\det(A(\varepsilon)) > 6912 = U_{\pm 1}(9)$. Indeed, we can take $\varepsilon = 1$, as $\det(A(1)) = 8582 > 6912$.

[8]For reasons of efficiency, our program takes as input a list (generated during the computation of Tables 1–2) of necklaces that define circulants A with maximal $|\det(A)|$, then considers all possible rotations of these circulants.

If $n = 10$, we find that

$$\det(\mathrm{circ}(1-\varepsilon, -1, 1, 1, -1, -1, -1, -1, -1, -1)) = -(22528 + 2560\varepsilon + O(\varepsilon^2)),$$

and

$$\det(\mathrm{circ}(-1+\varepsilon, -1, -1, 1, -1, 1, 1, -1, -1, -1)) = 22528 + 7680\varepsilon + O(\varepsilon^2),$$

so in both cases a sufficiently small $\varepsilon > 0$ disproves the conjecture. A different type of exceptional case is illustrated by

$$A(x) := \mathrm{circ}(x, -1, 1, -1, 1, 1, -1, -1, -1, -1),$$

where we find that $\det(A(x))$ is an even polynomial in x, and

$$-\det(A(0)) = 33489 > -\det(A(\pm 1)) = 22528 = U_{\pm 1}(10).$$

Similarly, for order 22, consider

$$A(x) := \mathrm{circ}(x,-1,1,1,-1,-1,-1,-1,-1,-1,-1,1,1,-1,1,-1,1,-1,1,1,-1,-1).$$

Then

$$-\det(A(0)) = 216409254831025 > -\det(A(\pm 1)) = 215055782117376.$$

Since $215055782117376 = U_{\pm 1}(22) = 2^{21} \times 102546588$ (see Table 4), we have $|\det(A(0))| > U_{\pm 1}(22)$.

As before, our search was not exhaustive, so there may be other $n < 48$ for which the maximum determinant does not occur at an extreme point of $[-1, 1]^n$.

7 Acknowledgements

We thank Jörg Arndt for his comments on a draft of this document, and the authors of Magma [6] and GMP [13] for their excellent software. Computing resources were provided by the Australian National University and the University of Newcastle (Australia). The first author was supported in part by Australian Research Council grant DP140101417.

References

[1] J. Arndt, Y. Dekel, H. Havermann, V. Jovivic and H. Yamanouchi, The On-Line Encyclopedia of Integer Sequences, A086432: *Maximum of* $|\det(A)|$ *where* A *is an* $n \times n$ *circulant* $(0, 1)$ *matrix over the integers*, `https://oeis.org/A086432/`, Dec. 16, 2016.

[2] J. Arndt, W. Smith *et al*, The On-Line Encyclopedia of Integer Sequences, A215897: $a(n) = \mathrm{A215723}(n)/2^{(n-1)}$, `https://oeis.org/A215897`, Aug. 26, 2012.

[3] G. Barba, Intorno al teorema di Hadamard sui determinanti a valore massimo, *Giorn. Mat. Battaglini* **71** (1933), 70–86.

[4] J. Berstel and M. Pocchiola, Average cost of Duval's algorithm for generating Lyndon words, *Theoretical Computer Science* **132** (1994), 415–425.

[5] K. S. Booth, Lexicographically least circular substrings, *Information Processing Letters* **10** (1980), 240–242.

[6] W. Bosma, J. Cannon and C. Playoust, The Magma algebra system. I. The user language, *J. Symbolic Comput.* **24** (1997), 235–265.

[7] P. J. Cameron, Hadamard Matrices, chapter in *Encyclopedia of Design Theory*, `http://www.maths.qmul.ac.uk/~lsoicher/designtheory.org/\library/encyc/topics/`.

[8] L. Devroye, *Non-Uniform Random Variate Generation*, Springer-Verlag, New York, 1986, §II.3 Available from `http://luc.devroye.org/rnbookindex.html`.

[9] J-P. Duval, Génération d'une section des classes de conjugaison et arbre des mots de Lyndon de longueur bornée, *Theoretical Computer Science* **60** (1988), 255–383.

[10] H. Ehlich, Determinantenabschätzungen für binäre Matrizen, *Math. Z.* **83** (1964), 123–132.

[11] H. Ehlich, Determinantenabschätzungen für binäre Matrizen mit $n \equiv 3 \bmod 4$, *Math. Z.* **84** (1964), 438–447.

[12] R.J. Fletcher, M. Gysin, and J. Seberry, Application of the discrete Fourier transform to the search for generalised Legendre pairs and Hadamard matrices, *Australasian J. Combinatorics* **23** (2001), 75–86.

[13] T. Granlund *et al*, *The GNU MP Bignum Library*, https://gmbplib.org/.

[14] J. Hadamard, Résolution d'une question relative aux déterminants, *Bull. des Sci. Math.* **17** (1893), 240–246. Reprinted in *Oeuvres de Jacques Hadamard*, Tome 1, CNRS, Paris, 1968, 239–245.

[15] D. E. Knuth, J. H. Morris and V. Pratt, Fast pattern matching in strings, *SIAM J. on Computing* **6** (1977), 323–350.

[16] T. Kociumaka, J. Radoszewski and W. Rytter, Computing k-th Lyndon word and decoding lexicographically minimal de Bruijn sequence, *CPM 2014, LNCS* **8486** (2014), 202–211.

[17] R. C. Lyndon, On Burnside's problem, *Trans. Amer. Math. Soc.* **77** (1954), 202–215.

[18] M. G. Neubauer and A. J. Radcliffe, The maximum determinant of $\{\pm 1\}$-matrices, *Linear Algebra Appl.* **257** (1997), 289–306. Also http://www.math.unl.edu/%7Earadcliffe1/Papers/maxdet.pdf

[19] J. von Neumann, Various techniques used in connection with random digits, in *Monte Carlo Method*, Appl. Math. Series **12**, US Nat. Bureau of Standards, 1951, 36–38 (summary written by G. E. Forsythe); reprinted in *John von Neumann Collected Works* (ed. A. H. Taub), **5**, Pergamon Press, New York, 1963, 768–770.

[20] W. Orrick, The Hadamard maximal determinant problem, http://www.indiana.edu/~maxdet/.

[21] J. H. Osborn, *The Hadamard Maximal Determinant Problem*, thesis, Univ. of Melbourne, 2003.

[22] R. E. A. C. Paley, On orthogonal matrices, *J. Mathematics and Physics* **12** (1933), 311–320.

[23] Y. Shiloach, Fast canonization of circular strings, *Journal of Algorithms* **2** (1981), 107–121.

[24] A. I. Shirshov, Subalgebras of free Lie algebras, *Mat. Sbornik N.S.* **33** (75), 441–452.

[25] N. J. A. Sloane, The On-Line Encyclopedia of Integer Sequences, A000031: *Number of n-bead necklaces with 2 colors when turning over is not allowed; also number of output sequences from a simple n-stage cycling shift register; also number of binary irreducible polynomials whose degree divides n*, `https://oeis.org/A000031/`, Dec. 27, 2017.

[26] J. J. Sylvester, Thoughts on inverse orthogonal matrices, simultaneous sign successions, and tesselated pavements in two or more colours, with applications to Newton's rule, ornamental tile-work, and the theory of numbers, *London Edinburgh and Dublin Philos. Mag. and J. Sci.* **34** (1867), 461–475.

[27] J. Williamson, Hadamard's determinant theorem and the sum of four squares, *Duke Math. J.* **11** (1944), 65–81.

[28] M. Wojtas, On Hadamard's inequality for the determinants of order non-divisible by 4, *Colloq. Math.* **12** (1964), 73–83.

[29] Wolfram Mathworld, *Necklace*, `http://mathworld.wolfram.com/Necklace.html`.

2010 *Mathematics Subject Classification*: Primary 05A15; Secondary 05A19, 65T50.
Keywords: binary matrix, Booth's algorithm, circulant, Duval's algorithm, Hadamard bound, Lyndon word, maximal determinant, modular computation, necklace, parallel algorithm, parallel computation

---

(Concerned with sequences A000031, A086432, A215723, A215897.)

Appendix – Tables of Maximal Determinants

order	maximal |determinant|	ratio to upper bound	lex-least word (decimal)	lex-least word (over $\{0,1\}$)
1	1	1.0000	1	1
2	1	1.0000	1	01
3	2	1.0000	3	011
4	3	1.0000	7	0111
5	4	0.8000	15	01111
6	9	0.7500	11	001011
7	32	1.0000	23	0010111
8	45	0.6923	47	00101111
9	95	0.6597	47	000101111
10	275	0.6152	55	0000110111
11	1458	1.0000	183	00010110111
12	2240	0.6145	439	000110110111
13	6561	0.6923	1527	0010111110111
14	19952	0.5759	751	00001011101111
15	131072	1.0000	2479	000100110101111
16	214245	0.5691	2935	0000101101110111
17	755829	0.6784	2935	00000101101110111
18	2994003	0.6505	9903	000010011010101111
19	19531250	1.0000	22427	0000101011110011011
20	37579575	0.6010	28023	00000110110101110111
21	134534444	0.6560	45999	000001011001110101111
22	577397064	0.6178	117623	0000011100101101110111
23	4353564672	1.0000	340831	00001010011001101011111
24	10757577600	0.7060	843119	000011001101110101101111
25	31495183733	0.5787	638287	0000010011011110101001111

Table 1: Maximal determinants of $\{0,1\}$-circulants of order $n \leq 25$.

order n	maximal |determinant|	ratio to upper bound	lex-least word (decimal)
26	154611524732	0.5744	957175
27	738139162166	0.5442	1796839
28	3124126889325	0.6101	5469423
29	11937232425585	0.6069	6774063
30	65455857159975	0.6271	37463883
31	562949953421312	1.0000	77446231
32	1395230053365015	0.6148	47828907
33	5687258414265018	0.6123	196303815
34	30551195956571643	0.5827	95151003
35	300189270593998242	1.0000	1324935477
36	809028975189744400	0.6309	1822895095
37	3198686446402685263	0.5760	430812063
38	19288701806345611347	0.5825	2846677239
39	103227456252120723684	0.5161	10313700815
40	529663503370085366373	0.5885	6269629671
41	2311393009109010944326	0.5638	26764629467
42	15469925980869995489631	0.6023	22992859983
43	162805498773679522226642	1.0000	92035379515
44	402826140168935435652453	0.5245	162368181483
45	2268175963362305735661143	0.6192	226394696439
46	12738408112895861486972391	0.5307	631304341299
47	158993694406781688266883072	1.0000	4626135339999
48	483776963047101724429782080	0.6179	924925407055
49	2226275734022433928055705600	0.5715	1588449170843

Table 2: Maximal determinants of $\{0,1\}$-circulants, $25 < n \leq 49$.

order n	maximal $\lvert\det\rvert/2^{n-1}$	ratio to upper bound	lex-least word (decimal)	lex-least word (over {-,+})
1	1	1.0000	0	-
2	0	0.0000	0	--
3	1	1.0000	1	--+
4	2	1.0000	1	---+
5	3	1.0000	1	----+
6	4	0.8000	1	-----+
7	8	0.6667	11	---+-++
8	18	0.5625	11	----+-++
9	27	0.4154	11	-----+-++
10	44	0.3056	11	------+-++
11	267	0.5973	39	-----+--+++
12	1024	0.7023	83	-----+-+--++
13	3645	1.0000	83	------+-+--++
14	6144	0.6483	83	-------+-+--++
15	23859	0.6886	359	------+-++--+++
16	50176	0.3828	691	------+-+-++--++
17	187377	0.4977	1643	------++--++-+-++
18	531468	0.4770	2215	------+---+-+--+++
19	3302697	0.7176	9895	-----+--++-+-+--+++
20	1061683	0.5436	6483	-------++--+-+-+--++
21	39337984	0.6291	67863	----+----+--+---+-+++
22	102546588	0.5000	21095	-------+-+--+--++--+++
23	568833245	0.6087	72519	------+---++-++-+---+++
24	3073593600	0.7060	144791	------+---++-+-++--+-+++
25	8721488875	0.5724	108199	--------++-+--++-+-+--+++

Table 3: Scaled maximal determinants of $\{\pm 1\}$-circulants of order $n \leq 25$.

order n	maximal $\|\text{determinant}\|/2^{n-1}$	ratio to upper bound	lex-least word (decimal)
26	32998447572	0.6064	355463
27	164855413835	0.6125	604381
28	572108938470	0.4218	1289739
29	2490252810073	0.4863	1611219
30	10831449635712	0.5507	1680711
31	68045615234375	0.6520	6870231
32	282773291271138	0.5023	12817083
33	1592413932070703	0.7017	18635419
34	5234078743146888	0.5635	55100887
35	33374247484277975	0.6366	149009085
36	198124573871046186	0.6600	160340631
37	787413957917252603	0.6140	415804239
38	3195257068570067448	0.5754	829121815
39	22999238901574021485	0.6946	4737823097
40	117140061677844350646	0.5857	1446278811
41	536469708946538168543	0.5961	3001209959
42	2417648227367853639168	0.5897	19153917469
43	14611334654738350617599	0.5689	52222437727
44	65738632907943707712320	0.4038	20159598251
45	438910341492340511320163	0.5715	166482220965
46	2010768410464246499566152	0.5489	90422521191
47	12779930756727248097293989	0.5324	115099593371
48	100192997081088000000000000	0.6302	242235026743

Table 4: Scaled maximal determinants of $\{\pm 1\}$-circulants, $25 < n \leq 48$.