Computation of Maximal Determinants of Binary Circulant Matrices

Richard P. Brent
Mathematical Sciences Institute
Australian National University
Canberra, ACT 2601, Australia
circulants@rpbrent.com

Adam B. Yedidia
Electrical Engineering and Computer Science
Massachusetts Institute of Technology
Cambridge, Massachusetts, USA
adamyedidia@gmail.com

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 \leq 52. 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 \((k - j) \mod n\). Thus, an \(n \times n\) circulant is a matrix of
the form $A = (a_{(k-j) \mod n})_{0 \leq j, k < n}$. 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.

We write $\text{circ}(a_0, a_1, \ldots, a_{n-1})$ for the circulant $(a_{(k-j) \mod n})_{0 \leq j, k < n}$ 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 correspondence between the integers $\{0, 1, \ldots, 2^n - 1\}$ and the binary circulant matrices of order $n$. 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 [20] states that, in the case of binary matrices $A$ over $\{\pm 1\}$, we have

$$|\det A| \leq n^{n/2}. \quad (1)$$

Moreover, Hadamard’s inequality is sharp for infinitely many $n$, for example, powers of two (Sylvester [35]), or $n$ of the form $q + 1$ where $q \equiv 3 \pmod 4$ and $q$ is a prime power (Paley [32]).

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 Neubauer and Radcliffe [28] 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 $\det A = 2^n \det B$.

$$B = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} \quad \text{double} \quad \begin{pmatrix} 2 & 0 & 2 \\ 2 & 2 & 0 \\ 0 & 2 & 2 \end{pmatrix}$$
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
\[
|\det B| = 2^{-n} |\det A| \leq 2^{-n} (n + 1)^{(n+1)/2},
\]
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.

The mapping from $\{0,1\}$-matrices to $\{\pm 1\}$-matrices is reversible if we are allowed to normalize 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 (Paley [32]) uses a circulant matrix of order $p$, where $p$ is a prime, $p \equiv 3 \pmod{4}$, 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 [16] use two circulants and a border of width two to construct Hadamard matrices. The Williamson construction (Williamson [40]) requires four matrices $A, \ldots, D$ which satisfy certain conditions, and for computational reasons these matrices are usually taken to be circulants.

Circulant matrices also play an important role in noisy convolutional Gaussian channels. Given a channel in which the output vector is given by the convolution of the input vector with a chosen mask vector, in the

---

1In fact, Hadamard in [20] 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 [9].
presence of additive Gaussian noise, the choice of mask that maximizes the
mutual information of the channel in high-SNR regimes is the first row of a
\{0, 1\}-circulant with near-flat Fourier spectrum, and this circulant is often
one with maximal or close to maximal determinant. This has important
applications in X-ray and gamma ray astronomy, optics, and computational
imaging [11, 2, 11, 15, 25, 42].

It is well-known that the (unnormalized) eigenvectors of \( \text{circ}(a_0, \ldots, a_{n-1}) \)
are given by \( v_j = (1, \omega^j, \omega^{2j}, \ldots, \omega^{(n-1)j})^T, \) \( 0 \leq j < n, \) where \( \omega \) 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

\[
\lambda_j = a_0 + a_1 \omega^j + \cdots + a_{n-1} \omega^{(n-1)j}, \quad 0 \leq j < n,
\]
and the determinant is

\[
\prod_{j=0}^{n-1} \lambda_j = \prod_{j=0}^{n-1} f(\omega^j),
\]
where

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

The polynomial \( f(z) \) is called the associated polynomial of the circulant.
Also, \( f(z) \) is called a Littlewood polynomial if the coefficients \( a_k \in \{ \pm 1 \} \), and
a Newman polynomial if the \( a_k \in \{0, 1\} \) and \( a_0 = 1 \).

If \( A = \text{circ}(a_0, \ldots, a_{n-1}) \) is nonsingular, then (4) gives

\[
\frac{\log |\det A|}{n} = \frac{1}{n} \sum_{j=0}^{n-1} \log |f(e^{2\pi ij/n})|.
\]

This may be regarded as a discrete analogue of the Mahler measure [36]

\[
m(f) := \int_0^1 \log |f(e^{2\pi it})| \, dt.
\]

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 that we
may 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 \( p \equiv 1 \pmod{n} \), and \( \rho \) is a primitive root \( \pmod{p} \), then

\[
\omega := \rho^{(p-1)/n} \pmod{p}
\]

is a primitive \( n \)-th root of unity in the finite field \( F_p \), and we can use (4) to compute \( \det A \pmod{p} \). If \( U \) is an upper bound on \( |\det A| \), and \( p \geq 2U + 1 \), then the result 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.

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 words were introduced by Shirshov [34] (who called them “regular words”) and Lyndon [26] (who called them “standard lexicographic sequences”).

Since we consider words of a fixed length \( n \), it is convenient to use the concept of a (binary) necklace. We say that \( w = w_0 \ldots w_{n-1} \) 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 \( n \)” [12, (3) on p. 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 be modified to apply to the other.

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

\[ ^3 \text{Tests indicate that, at least for } n \leq 50, \text{ it is faster to use a single prime. One reason for this is that the value } \det A \text{ needs to be reconstructed for each circulant } A, \text{ so the cost of the reconstruction steps is not negligible.} \]
The number \( K(n) \) of necklaces of length \( n \) over a binary alphabet is

\[
K(n) = \frac{1}{n} \sum_{d|n} 2^{n/d} \phi(d) = \frac{2^n}{n} + O \left( \frac{2^{n/2}}{n} \right),
\]

(5)

where \( \phi \) is Euler’s phi function. \( K(n) \) is tabulated in OEIS \[A000031\].

If \( A \) is a circulant, then \(|\det A|\) is invariant under rotations of the first row \((a_0, \ldots, a_{n-1})\). 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 \( w = w_0 \ldots w_{n-1} \) is in fact a necklace. Booth’s algorithm is closely related to the initial phase of the Knuth, Morris and Pratt fast pattern-matching algorithm [22].

The other algorithm that we use is Duval’s algorithm [12] which, given a necklace of length \( n \), returns the next necklace (of length \( n \)) in lexicographic order\(^4\) in amortized (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 [33] gives an algorithm that reduces the number of comparisons used by Booth’s algorithm. 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.

\section{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

---

\(^4\)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 [12] considers Lyndon words but, using [12, comment (3) on p. 258], we easily get a similar algorithm for necklaces.
changed as we go from one necklace to the next is $O(1)$ on average. Thus, each $\lambda_j$ 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 $\approx 2^n/n$ 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 $\omega^{jk}$ ($0 \leq j, k < n$) 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, $n$ is never 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.

### 4 Parallel algorithms

Suppose we wish to use $P \geq 1$ processors in parallel. If the $K = K(n) \approx 2^{n}/n$ necklaces of length $n$ are $W_0 = 0 \ldots 0, W_1, W_2, \ldots, W_{K-1} = 1 \ldots 1$, we would like processor $q$ ($0 \leq q < P$) to compute the determinants corresponding (approximately) to necklaces $W_{[qK/P]}, \ldots, W_{[(q+1)K/P]-1}$. The problem is how to determine the starting point for processor $q$, without enumerating $W_1, W_2, \ldots, W_{[qK/P]}$. Kociumaka et al. [23] sketch a deterministic polynomial-time algorithm for this problem, but it is very complicated. We used a simpler, randomized algorithm.

The idea is to take a random sample of $T$ necklaces, each of length $n$. Sort the sample, and then divide it into $P$ equal-sized segments. Modify the initial segment to start with $W_0 = 0 \ldots 0$ and the final segment to end with $W_{K-1} = 1 \ldots 1$. Thus, each processor has approximately $\mu = K/P$ words to process. Also, we know the necklace starting each segment, so we can use

---

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.

7 A similar algorithm, although not specifically intended for parallel computation, is described by Briggs and Ying [7]. For related references, see Ghosh and Pasupathy [17].
Duval’s algorithm to enumerate all necklaces in a segment.

How large does the sample size $T$ need to be? Suppose the procedure just described gives the $q$-th processor $S_q$ necklaces to process, where $0 \leq q < P$ and $S_0 + \cdots + S_{P-1} = K = P\mu$. Define $\varepsilon_q$ by $S_q = (1 + \varepsilon_q)\mu$, so $\varepsilon_q$ measures the relative difference between $S_q$ and the mean $\mu$. Using extreme-value theory it can be shown that, as $\min(P, T/(P\ln P), 2^n/T) \to \infty$, we have

$$E[\max\{\varepsilon_0, \ldots, \varepsilon_{P-1}\}] \sim \sqrt{\frac{2P\ln P}{T}}. \quad (6)$$

Simulations show that (6) gives a reasonable approximation even for small $P$, provided $2^n \geq T \geq P > 1$. Thus, for a given (one-sided) tolerance $\varepsilon > 0$, we should take

$$T \approx \frac{2P\ln P}{\varepsilon^2}. \quad (7)$$

With this choice of $T$ we can expect that, on average, the slowest processor will take only about $1 + \varepsilon$ times as long as the average processor.\footnote{In fact, our program used simply $T = 4000P$, equivalent to taking $\varepsilon = \sqrt{\ln(P)/2000}$ in (7). We had $P \leq 416$, so $\varepsilon \leq \sqrt{\ln(416)/2000} < 0.06$.}

We now describe how to randomly and uniformly sample the set of all necklaces of length $n$. Generate a random binary string of length $n$, and test (using Booth’s algorithm) if it corresponds to a necklace. If so, accept the string. Otherwise, reject the string and try again.\footnote{This ignores any random variations in speed due to other users in a shared multiprocessor computer system. In practice such variations may be larger than the variations caused by random sampling.} This 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 of a random binary string of length $n$ being a necklace is $K/2^n$, the expected number of random binary strings that are needed is $T/(K/2^n) = nT(1 + O(2^{-n/2}))$. The algorithm that we have described is an example of Von Neumann’s rejection method.\footnote{It is not sufficient to rotate the string until we obtain a necklace. This would not give each necklace an equal probability of selection. Consider, for example, the case $n = 2$, where the three necklaces 00, 01, and 11 would be selected with probabilities 1/4, 1/2, and 1/4 respectively.} Other examples may be found in Devroye’s book.\footnote{In Devroye’s book.}

For $n \geq 2$ we can speed up the generation of random necklaces, if we exclude the special cases 0...0 and 1...1, and take advantage of the fact that all other necklaces have the form $0x\ldots y1$, where $x, \ldots, y \in \{0, 1\}$.
5 Computational results

Our computations extend some entries in the OEIS [30]. Tables 1–2 give computational results for the maximal determinants $D_{01}(n)$ of $\{0, 1\}$-circulants of orders $n \leq 52$. 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, Tables 3–4 give computational results for the maximal determinants $D_{\pm1}(n)$ of $\{\pm1\}$-circulants of orders $n \leq 52$. 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

$$
H_{BE}(n) := \begin{cases} 
\frac{n^{n/2}}{2}, & \text{if } n \equiv 0 \pmod{4}; \\
2(n-1)(n-2)^{(n-2)/2}, & \text{if } n \equiv 2 \pmod{4}; \\
(2n-1)^{1/2}(n-1)^{(n-1)/2}, & \text{otherwise}.
\end{cases}
$$

(8)

Then $H_{BE}(n)$ is an upper bound on $|\det A|$ for $\{\pm1\}$-matrices $A$ of order $n$. The case $n \equiv 0 \pmod{4}$ is due to Hadamard [20]; the case $n \equiv 2 \pmod{4}$ is due to Ehlich [13] and Wojtas [41]; and the remaining case ($n$ odd) is due to Barba [3], Ehlich [13], and Wojtas [41]. We do not use Ehlich’s slightly sharper, but more complicated, bound that applies when $n \equiv 3 \pmod{4}$. For this bound, see Ehlich [14] or Orrick [31].

In view of the discussion in [41], we take

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

(9)

and

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

(10)

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 $n \equiv 0 \pmod{4}$, this is the circulant Hadamard problem.) On the other hand, $D_{01}(p) = U_{01}(p)$ for all primes $p \equiv 3 \pmod{4}$. This follows from the first Paley construction [32], 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 $n \leq 37$ in OEIS A086432 and the associated b-file. Table 4 extends the list of $D_{\pm 1}(n)/2^{n-1}$ values given for $n \leq 28$ in OEIS A215897. This implies a corresponding extension for OEIS A215723, which lists the unscaled values $D_{\pm 1}(n)$.

As an indication of the time required to compute the tables, we note that the computation of $D_{01}(52)$ using our parallel program (implemented in C using GMP [19]) took 11 processor-years using 128 Intel Xeon3 (2.2GHz) and 224 Xeon4 (2.6GHz) processors. The computation time for order $n$ was roughly proportional to $2^n$.

For verification, all the values given in the tables for orders $n < 50$ were computed at least twice, using different programs and/or different prime moduli $p$. No discrepancies were found.

In Sections 6–8 we discuss some plausible conjectures that motivated our computations.

6 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 $n \in \{1, 2, 3, 4, 7, 11, 15, 19, 23\}$. The Paley construction explains this for $n = 3, 7, 11, 19, 23$, and larger cases where $n$ is a prime and $n \equiv 3 \pmod{4}$. 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 $n \equiv 3 \pmod{4}$ is the product of at most two distinct primes. Support is provided by the computation for $n = 35 = 5 \times 7$, since $D_{01}(35) = U_{01}(35)$.

Our computation for $n = 39$ disproves this conjecture, since $39 = 3 \times 13$ is a product of two distinct primes, but $D_{01}(39) < U_{01}(39)$. Another counter-example is $n = 51 = 3 \times 17$. We find that $D_{01}(51) < U_{01}(51)/2$.

After our computations were completed, we found an explanation for the cases $n = 15$ and $n = 35$. In each case $n$ has the form $p(p + 2)$, where $p$ and $p+2$ are both prime. Such $n$ are covered by case (2) of the following theorem, which we quote (with a change in notation) from Kotsireas et al. [24]. Note that a “circulant core” of order $n$ refers to a $\{0, 1\}$-circulant matrix of order $n$ which can be used to construct a Hadamard matrix of order $n+1$ using the correspondence between $\{0, 1\}$-matrices and $\{\pm 1\}$-matrices described in §1.
Theorem 1 (Hadamard circulant core construction). A Hadamard matrix of order $n + 1$ with circulant core of order $n$ exists if

1. $n \equiv 3 \pmod{4}$ is a prime;
2. $n = p(p + 2)$, where $p$ and $p + 2$ are prime;
3. $n = 2^k - 1$, where $k$ is a positive integer; or
4. $n = 4k^2 + 27$, where $k$ is a positive integer and $n$ is a prime.

Proof. Case (1) is due to Paley [32]; case (2) is due to Stanton and Sprott [37] and also Whiteman [39]; case (3) is due to Singer [35]; and case (4) is due to Hall [21, Theorem 2.2].

Hall [21, p. 980] remarks that case (4) is subsumed by case (1), since $4k^2 + 27 \equiv 3 \pmod{4}$, but we mention case (4) since Hall’s construction is different from that of Paley.

We do not know if the list given by Theorem 1 is exhaustive. The computational results given in Tables 1–2 show that, for $1 \leq n \leq 52$, only those $n$ given by Theorem 1 can provide a Hadamard matrix of order $n + 1$ with a circulant core. Also, a circulant $\{0, 1\}$-matrix of order $n \leq 52$ can achieve the upper bound (10) if and only if $n \leq 4$ or $n$ satisfies condition (1), (2) or (3) of Theorem 1.

7 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\textsuperscript{11} 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 separately. For example, if $n = 2$ we have $\det A = a_0^2 - a_1^2$. Nevertheless,

\textsuperscript{11}This is already implicit in Hadamard [20].
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 \[12\]

The smallest examples occur for $n = 9$. Consider $A = \text{circ}(a_0, \ldots, a_8)$ with $(a_0, \ldots, a_8) = (0,0,0,1,1,1,0,1)$. We have $\det A = 95 = D_{01}(9)$, but $\partial \det A/\partial a_0 = 9$. If $a_0 = \varepsilon$ for some small $\varepsilon$, 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 $A = \text{circ}(0,0,1,0,0,1,1,1,0)$, $\det A = 275$. 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 $n$ up to the limit of Table 2. However, there is a different class of examples that occur when $n = 4k + 1 > 5$ is a prime, e.g., $n = 13,17,29,37,41$, etc. For this class we make a small modification to the Uniformly Redundant Arrays (URAs) of \[8,15\], which are equivalent to Abelian difference sets \[21\]. Define

$$A_n(x) := \text{circ}(x, \frac{1+\chi(1)}{2}, \frac{1+\chi(2)}{2}, \ldots, \frac{1+\chi(n-1)}{2}),$$

where $\chi$ is a quadratic character, defined by the Legendre symbol

$$\chi(j) = \left(\frac{j}{n}\right) := \begin{cases} +1, & \text{if } j \text{ is a quadratic residue modulo } n, j \not\equiv 0 \pmod{n}; \\ -1, & \text{if } j \text{ is a quadratic non-residue modulo } n; \\ 0, & \text{if } j \equiv 0 \pmod{n}. \end{cases}$$

Then $A_n(0)$ corresponds to a 1-D URA, but $\det A_n(0)$ is not generally maximal in the class of circulant determinants. However, $\det A_n(\frac{1}{2})$ may be larger than the corresponding entry in Tables 1,2. It may be shown \[14\] that, for $n = 4k + 1$ an odd prime,

$$\det A_n(x) = (x + 2k)(x^2 - x - k)^{2k}. \quad (11)$$

\[12\] 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.

\[13\] Our construction is also close to the “modified” URAs (MURAs) of \[15\].

\[14\] The proof uses the identity $A_n(0)^2 + A_n(0) = k(I + J)$.
In particular, \( \det A_n(0) = 2k^{2k+1} \), \( \det A_n(1) = (2k + 1)k^{2k} \), and
\[
\det A_n\left(\frac{1}{2}\right) = 2^{-n} n^{(n+1)/2}.
\]

It may be verified numerically that \( \det A_n\left(\frac{1}{2}\right) \) exceeds the maximal determinant given in Tables 1–2 for \( n = 13, 17, 29, 37, \) and 41. The next possibility, \( n = 53 \), is beyond the range of Table 2.

We observe that the maximum of \( \det A_n(x) \) for \( x \in [0, 1] \) is not at \( x = \frac{1}{2} \). One can show, by logarithmic differentiation of (11), that a local maximum occurs at
\[
x = x_k := \frac{\sqrt{1 + 4k^2 + 1 - 2k}}{2} = \frac{1}{2} + \frac{1}{8k} + O(k^{-3}),
\]
and
\[
\max_{0 \leq x \leq 1} \det A_n(x) = \det A_n(x_k) = \det A_n\left(\frac{1}{2}\right) \left(1 + \frac{1}{8kn} + O(k^{-4})\right).
\]

For example, if \( k = 3, n = 13 \), we have \( x_3 = (\sqrt{37} - 5)/2 \approx 0.5414 \), and \( U_{01}(13) = 9477 > \det A_{13}(x_3) \approx 7684.16 > \det A_{13}\left(\frac{1}{2}\right) \approx 7659.73 > D_{01}(13) = 6561 > \det A_{13}(1) = 5103 > \det A_{13}(0) = 4374.8 \)

8 Conjecture B, case \([-1, 1]\)

Replacing \([0, 1]\) by \([-1, 1]\), we find analogous behaviour to that described in [7] for \( n = 2, 9, 10, 11, 18, 22 \), and no other \( n \) up to the limit of Table 4.

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
\[
A(\varepsilon) := \text{circ}(1 - \varepsilon, 1, -1, 1, 1, -1, -1, 1, 1, 1, 1).
\]

We find that
\[
\det A(\varepsilon) = 6912 + 4608\varepsilon + O(\varepsilon^2),
\]
so sufficiently small \( \varepsilon > 0 \) gives \( \det A(\varepsilon) > 6912 = D_{\pm 1}(9) \). Indeed, we can take \( \varepsilon = 1 \), as \( \det A(1) = 8582 > 6912 \).

If \( n = 10 \), we find that
\[
\det \text{circ}(1 - \varepsilon, -1, 1, 1, -1, -1, -1, -1, -1, -1, 1) = -(22528 + 2560\varepsilon + O(\varepsilon^2)),
\]

13
and
\[
det \ circ(-1 + \varepsilon, -1, -1, 1, -1, 1, -1, -1, 1) = 22528 + 7680\varepsilon + O(\varepsilon^2),
\]
so in both cases a sufficiently small \( \varepsilon > 0 \) disproves the conjecture. A different type of exceptional case is illustrated by
\[
A(x) := \ circ(x, -1, 1, -1, 1, -1, -1, 1, -1),
\]
where we find that \( \det A(x) \) is an even polynomial in \( x \), and
\[
-\det A(0) = 33489 > -\det A(\pm 1) = 22528 = D_{\pm 1}(10).
\]
Similarly, for order 22, consider
\[
A(x) := \ circ(x, -1, 1, -1, -1, -1, -1, 1, 1, -1, 1, 1, -1, 1, 1, 1, 1, -1, 1, 1, 1, 1, -1, 1).
\]
Then
\[
-\det A(0) = 216409254831025 > -\det A(\pm 1) = 215055782117376.
\]
Since 215055782117376 = \( D_{\pm 1}(22) = 2^{21} \times 102546588 \) (see Table 3), we have \( |\det A(0)| > D_{\pm 1}(22) \).

Our search was not exhaustive, so there may be other \( n \) within the range of Tables 3–4 for which the maximum determinant does not occur at an extreme point of \([-1, 1]^n\).

9 Remarks on periodic autocorrelations

It is hard to discern a pattern in the lex-least words given in Tables 1–4. It seems more fruitful to consider the periodic autocorrelations of the first rows of the corresponding circulants. Equivalently, we can consider the first rows of the Gram matrices \( G = A^T A \), where \( A \) is the relevant circulant.

In the case of (0, 1)-circulants, it can be useful to map \( (0, 1) \to (-1, 1) \), and consider the first row of \( G' = (2A - J)^T (2A - J) \). Provided \( n > 4 \), the upper bound is achieved in Tables 1–2 if and only if the first row of \( G' \) is \( (n, -1, -1, \ldots, -1) \). See, for example, MacWilliams and Sloane [27].

In some cases the maximal determinants given in Tables 1–4 have only small prime factors. For example, the entry for \( n = 52 \) in Table 4 factors as \( 2^{49} \times 3^{24} \times 5^4 \), and this can be explained if we observe that the first row of \( G \) is \( (52, 0, 0, 0, 4, 0, 0, 0, 0, 0, 0, 0) \). Thus, we can write \( G = 52I + 4E^4 + 4E^8 + \cdots + 4E^{48} \), where \( E \) is the “circular shift” matrix. Similarly, the entry for \( n = 48 \) in Table 4 is \( 2^{49} \times 3^6 \times 5^{12} \), and here \( G = 48I + 4E^{12} + 8E^{24} + 4E^{36} \).
10 Acknowledgements

We thank Jörg Arndt for correcting our terminology, Alex Arkhipov for his helpful comments about Hadamard matrices with circulant cores and related group theory, and the authors of Magma [6] and GMP [19] for their invaluable software. An anonymous referee helped us to clarify several points in §2 and §4. 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. G. Ables, Fourier transform photography: a new method for X-ray astronomy, Proc. Astron. Soc. Austral. 1 (1968), 172–173.

[2] M. S. Asif, A. Ayremlou, A. Sankaranarayanan, A. Veeraraghavan, and R. Baraniuk, Flatcam: Thin, bare-sensor cameras using coded aperture and computation, IEEE Trans. Comput. Imaging, to appear. Preprint, 2015, http://arxiv.org/abs/1509.00116.

[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, Theoret. Comput. Sci. 132 (1994), 415–425.

[5] K. S. Booth, Lexicographically least circular substrings, Inform. Process. Lett. 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] K. Briggs and F. Ying, How to estimate quantiles easily and reliably, Math. Today (Southend-on-Sea) 54, 1 (Feb. 2018), 26–29.

[8] A. Busboom, H. Elders-Boll, and H. D. Schotten, Uniformly redundant arrays, Experimental Astronomy 8 (1998), 97–123.

[9] P. J. Cameron, Hadamard Matrices, in Encyclopaedia of Design Theory, Queen Mary, University of London, 2006. http://www.maths.qmul.ac.uk/~lsoicher/designtheory.org/library/encyc/topics/.
[10] L. Devroye, *Non-Uniform Random Variate Generation*, Springer-Verlag, New York, 1986, §II.3 Available from http://luc.devroye.org/rnbookindex.html.

[11] R. H. Dicke, Scatter-hole cameras for X-rays and gamma rays, *Astrophys. J.* 153 (1968), L101–L106.

[12] J.-P. Duval, Génération d’une section des classes de conjugaison et arbre des mots de Lyndon de longueur bornée, *Theoret. Comput. Sci.* 60 (1988), 255–383.

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

[14] H. Ehlich, Determinantenabschätzungen für binäre Matrizen mit \( n \equiv 3 \pmod{4} \), *Math. Z.* 84 (1964), 438–447.

[15] E. E. Fenimore and T. M. Cannon, Coded aperture imaging with uniformly redundant arrays, *Applied Optics* 17 (1978), 337–347.

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

[17] S. Ghosh and R. Pasupathy, Low-storage online estimators for quantiles and densities, *Proc. 2013 Winter Simulation Conference*, IEEE, New York, 2013, 778–789.

[18] S. R. Gottesman and E. E. Fenimore, New family of binary arrays for coded aperture imaging, *Applied Optics* 28 (1989), 4344–4352.

[19] T. Granlund, *The GNU MP Bignum Library*, http://gmplib.org/, 2016.

[20] 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.

[21] M. Hall, Jr., A survey of difference sets, *Proc. Amer. Math. Soc.* 7 (1956), 975–986.
[22] D. E. Knuth, J. H. Morris, and V. Pratt, Fast pattern matching in strings, *SIAM J. Comput.* **6** (1977), 323–350.

[23] T. Kociumaka, J. Radoszewski, and W. Rytter, Computing $k$-th Lyndon word and decoding lexicographically minimal de Bruijn sequence, *CPM 2014, Lect. Notes in Comp. Sci.*, Vol. 8486, Springer, 2014, pp. 202–211.

[24] I. S. Kotsireas, C. Koukouvinos, and J. Seberry, Hadamard ideals and Hadamard matrices with circulant core, *J. Combin. Math. Combin. Comput.* **57** (May 2006), 47–63.

[25] A. Levin, R. Fergus, F. Durand, and W. Freeman, Image and depth from a conventional camera with a coded aperture, *ACM Trans. Graph.* **26.3** (2007), 70.

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

[27] F. J. MacWilliams and N. J. A. Sloane, Pseudo-random sequences and arrays, *Proc. IEEE* **64** (1976), 1715–1729.

[28] M. G. Neubauer and A. J. Radcliffe, The maximum determinant of $\{\pm 1\}$-matrices, *Linear Algebra Appl.* **257** (1997), 289–306.

[29] 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*, Vol. 5, Pergamon Press, New York, 1963, pp. 768–770.

[30] OEIS Foundation Inc., *The On-Line Encyclopedia of Integer Sequences*, [http://oeis.org](http://oeis.org) 2018.

[31] W. Orrick, The Hadamard maximal determinant problem, [http://www.indiana.edu/~maxdet/](http://www.indiana.edu/~maxdet/) 2018.

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

[33] Y. Shiloach, Fast canonization of circular strings, *J. Algorithms* **2** (1981), 107–121.
[34] A. I. Shirshov, Subalgebras of free Lie algebras, *Mat. Sbornik N.S.* 33 (1953), 441–452.

[35] J. Singer, A theorem in finite projective geometry and some applications to number theory, *Trans. Amer. Math. Soc.* 43 (1938), 377–385.

[36] C. Smyth, The Mahler measure of algebraic numbers: a survey, in *Number Theory and Polynomials*, J. McKee and C. Smyth (eds.), Cambridge Univ. Press, New York, 2008, 322–349.

[37] R. G. Stanton and D. A. Sprott, A family of difference sets, *Can. J. Math.* 10 (1958), 73–77.

[38] J. J. Sylvester, Thoughts on inverse orthogonal matrices ..., *London Edinburgh and Dublin Philos. Mag. and J. Sci.* 34 (1867), 461–475.

[39] A. L. Whiteman, A family of difference sets, *Illinois J. Math.* 6 (1962), 107–121.

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

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

[42] A. Yedidia, C. Thrampoulidis, and G. Wornell, Analysis and optimization of aperture design in computational imaging, preprint, 2017, [http://arxiv.org/abs/1712.04541](http://arxiv.org/abs/1712.04541).

---

2010 Mathematics Subject Classification: Primary 05A15; Secondary 05A19, 65T50.

Keywords: binary matrix, Booth’s algorithm, circulant, circulant core, computational imaging, convolutional Gaussian channel, difference set, discrete Mahler measure, Duval’s algorithm, Hadamard bound, Hadamard matrix, Lyndon word, maximal determinant, modular computation, MURA, necklace, parallel algorithm, parallel computation, quantile estimation, URA.

(Concerned with sequences A000031, A086432, A215723, A215897)
## Appendix: tables of maximal determinants

| order $n$ | maximal determinant $D_{[01]}(n)$ | ratio $D_{[01]}(n)/U_{[01]}(n)$ | 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                     | 00101111110111                   |
| 14        | 19952                            | 0.5759                          | 751                      | 00001011101111                   |
| 15        | 131072                           | 1.0000                          | 2479                     | 000100110101111                  |
| 16        | 214245                           | 0.5691                          | 2935                     | 000010111101111                  |
| 17        | 755829                           | 0.6784                          | 2935                     | 0000101110111111                 |
| 18        | 2994003                          | 0.6505                          | 9903                     | 00001001101011111                |
| 19        | 19531250                         | 1.0000                          | 22427                    | 000010111101110111               |
| 20        | 37579575                         | 0.6010                          | 28023                    | 0000011011010111101111           |
| 21        | 134534444                        | 0.6560                          | 45999                    | 00000101110011101101111          |
| 22        | 577397064                        | 0.6178                          | 117623                   | 00000111010011011011101111      |
| 23        | 435364672                        | 1.0000                          | 340831                   | 0000010100110011010111011111    |
| 24        | 1075777600                       | 0.7060                          | 843119                   | 000011001101111010110111111     |
| 25        | 31495183733                      | 0.5787                          | 638287                   | 0000010011101111010100111111    |

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        | 312412689325        | 0.6101               | 5469423                 |
| 29        | 11937232425585      | 0.6069               | 6774063                 |
| 30        | 65455857159975      | 0.6271               | 37463883                |
| 31        | 56294995421312      | 1.0000               | 77446231                |
| 32        | 1395230053365015     | 0.6184               | 47828907                |
| 33        | 5687258414265018     | 0.6123               | 196303815               |
| 34        | 30551195956571643    | 0.5827               | 95151003                |
| 35        | 300189270593998242   | 1.0000               | 1324935477              |
| 36        | 80902897518974400    | 0.6309               | 1822895095              |
| 37        | 3198686446402685263  | 0.5760               | 430812063              |
| 38        | 19288701806345611347 | 0.5825               | 2846677239              |
| 39        | 10322745625120723684 | 0.5161               | 10313700815               |
| 40        | 529663503370085366373 | 0.5885              | 626962671                |
| 41        | 2311393009109010944326 | 0.5638              | 26764629467               |
| 42        | 15469925980869995489631 | 0.6023             | 22992859983               |
| 43        | 162805498773679522262642 | 1.0000            | 9203579515                |
| 44        | 402826140168935435652453 | 0.5245         | 162368181483               |
| 45        | 2268175963632305735661143 | 0.6192          | 22639469643                |
| 46        | 12738408112895861486972391 | 0.5307           | 631304341299               |
| 47        | 158993694406781688266883072 | 1.0000          | 4626135339999               |
| 48        | 483776963047101724429782080 | 0.6179           | 924925407055               |
| 49        | 2226275734022439328055705600 | 0.5715      | 1588449170843               |
| 50        | 15940963431893593997118039375 | 0.5992      | 5455102172067               |
| 51        | 8634390234665136953496818019 | 0.4706       | 12463552538547                |
| 52        | 471252255596620483490068604560 | 0.5013       | 23418838481755               |

Table 2: Maximal determinants of $\{0,1\}$-circulants, $25 < n \leq 52$. 
| order $n$ | maximal scaled $|\det| \cdot D_{\pm 1}(n)/2^{n-1}$ | ratio $D_{\pm}(n)/U_{\pm}(n)$ (decimal) | lex-least word (over $\{\pm 1\}$) |
|-----------|-----------------------------------------------|------------------------------------------|----------------------------------|
| 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        | 10616832                                      | 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: Maximal scaled determinants of $\{\pm 1\}$-circulants of order $n \leq 25$. 
| order | maximal scaled $|\text{det}|$ $D_{\pm 1}(n)/2^{n-1}$ | 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    | 11714006167784350646 | 0.5857     | 1446278811       |
| 41    | 536469708946538168543 | 0.5961     | 3001209959       |
| 42    | 2417648227367853639168 | 0.5897     | 1915391749       |
| 43    | 14611334654738350617599 | 0.5689    | 5222243727       |
| 44    | 65738632907943707712320 | 0.4038    | 20159598251      |
| 45    | 438910341492340511320163 | 0.5715    | 16648220965      |
| 46    | 2010768410464246499566152 | 0.5489    | 90422521191      |
| 47    | 12779930756727248097293989 | 0.5324    | 115099593371     |
| 48    | 1001929970810880000000000000 | 0.6302    | 242235026743     |
| 49    | 408375323859124630659059549 | 0.5216    | 1416138805685    |
| 50    | 2152519997519833685106486024 | 0.5526    | 2380679727935    |
| 51    | 14098690136202107270366810369 | 0.5300    | 2716242515341    |
| 52    | 99371059004238555166801920000 | 0.5416    | 1758408815375    |

Table 4: Maximal scaled determinants of $\{\pm 1\}$-circulants, $25 < n \leq 52$. 