

How fast can one compute the permanent of circulant matrices?

A. Bernasconi* B. Codenotti† V. Crespi‡ G. Resta†

Abstract

In this paper we address the problem of computing the permanent of $(0,1)$ -circulant matrices. We investigate structural properties of circulant matrices, showing that (i) if they are dense enough, then they contain large arbitrary submatrices, and, (ii) if they are very sparse, then they are not too “far” from convertible matrices. Building upon (ii), we then develop an efficient algorithm, which allows us to compute permanents of very sparse circulants of size up to 200.

1 Introduction

The computation of the permanent of a matrix seems to be a very hard task, even for $(0,1)$ matrices. Valiant proved that computing the permanent of a $(0,1)$ matrix is $\#P$ -complete (see [V179] and [V279]). The class $\#P$ contains those functions that can be computed in polynomial time by a counting (nondeterministic) Turing machine, and the $\#P$ -complete problems represent the hardest problems within the class. More recently, several authors have found even stronger negative results [DLMV88, FL92].

Thus it is extremely unlikely that there is a polynomial time algorithm for computing the permanent. Actually, the best known algorithm for computing the permanent is due to Ryser [R63] and takes $O(n 2^n)$ operations, where n is the matrix size.

In this paper, we continue the work started in [CCR96] and investigate structural and computational properties of permanents of circulant matrices.

We first deal with a *structural* issue. Namely we address the problem of computing the permanent of circulants vs the general case. The results obtained give indications that permanents of dense enough circulants cannot be computed significantly faster than those of arbitrary matrices. On the other hand, we also show that very sparse circulants are not too

*Institut für Informatik, Technische Universität München, 80290 München (Germany). e-mail: bernasco@informatik.tu-muenchen.de.

†Istituto di Matematica Computazionale del CNR, Via S. Maria 46, 56126-Pisa (Italy). e-mail: {codenotti,resta}@imc.pi.cnr.it.

‡Dipartimento di Informatica, Università degli Studi di Milano, Milano (Italy). e-mail: crespi@dsi.unimi.it. Part of this work has been done while visiting IMC-CNR in Pisa.

“far” from convertible matrices and we take advantage of this property to develop an efficient algorithm for the computation of the permanent of $(0, 1)$ -circulants with three nonzero entries per row. Using this algorithm we are able to compute permanents of matrices of size up to 200. The efficiency of the algorithm depends on two facts, i.e., (a) that these matrices contain large convertible submatrices, and (b) that for any matrix of prime size n and of the form $I + P^h + P^k$, we can find a matrix (with the same permanent) of the form $I + P^i + P^j$ such that the sum of the two least values among $\{i, j, n - i, n - j\}$ does not exceed $\sqrt{8n}$.

The rest of this paper is organized as follows. In Section 2 we introduce the main notation used throughout the paper. In Section 3 we investigate the relationship between general matrices on the one side, and circulant matrices and convertible matrices on the other one. Building upon our previous work on the same topic and on some new equivalences between permanents, in Section 4 we present an efficient algorithm for the computation of permanents of very sparse circulants, and we show the outcomes of the experiments. Concluding remarks are in Section 5.

2 Preliminaries

Let Σ be the set of all permutations of the first n integers. The permanent of an $n \times n$ matrix $A = (a_{i,j})$ is defined as $\sum_{\sigma \in \Sigma} \prod_{i=1}^n a_{i,\sigma_i}$, where $\sigma = (\sigma_1, \dots, \sigma_n)$. We will denote the permanent and the determinant of a square matrix A as $\text{per}(A)$ and $\det(A)$, respectively. A $(0, 1)$ -matrix A is said to be *convertible* if there exists a $(-1, 1)$ -matrix X such that $\text{per}(A) = \det(A \star X)$, where \star denotes the elementwise product, i.e., the (i, j) -th entry of the matrix $A \star X$ is $a_{i,j}x_{i,j}$.

The permanent of a $(0, 1)$ matrix has an interpretation in terms of both the digraph and the bipartite graph that can be associated with the matrix. More precisely, if A is an $n \times n$ $(0, 1)$ matrix, we denote by $D(A)$ the digraph whose adjacency matrix is A and by $G[A]$ the $2n$ -node bipartite graph associated with A in the natural way. Then the permanent of A is equal to the number of cycle covers of $D(A)$ as well as to the number of perfect matchings of $G[A]$. Recall that a cycle cover of $D(A)$ is a node disjoint covering of all the nodes of $D(A)$ in terms of its cycles, whereas a matching of $G[A]$ is a set of pairwise node disjoint edges, and a perfect matching (or 1-factor) of $G[A]$ is a matching such that each node of $G[A]$ is incident to exactly one of the edges forming the matching.

We will use the *Big-Oh* notation for orders of magnitudes, i.e., $O(m)$ will stand for “asymptotically not greater than cm ”, and $\theta(m)$ for “asymptotically of the same order as cm ”, where c is a constant with respect to m .

Let P_n denote the $(0, 1)$ $n \times n$ matrix with 1's only in positions $(i, i + 1)$, $i = 1, 2, \dots, n - 1$, and $(n, 1)$. Any $(0, 1)$ circulant matrix can be written in the form $P^{t_1} + P^{t_2} + \dots + P^{t_k}$, where $0 \leq t_1 < t_2 < \dots < t_k < n$.

3 Circulant, arbitrary, and convertible matrices

Although circulant matrices have a very nice special structure, the evaluation of their permanents is in general far from trivial. The results of Section 3.1 will provide an explanation for this fact. Indeed we will show that a graph whose adjacency matrix is circulant (which we will call circulant graph) contains a *large* arbitrary subgraph, provided it has enough edges. This property however leaves an open door to the existence of faster algorithms in the *sparse* case. In later sections we will actually show some progress to this respect.

3.1 Arbitrary subgraphs of circulant graphs

We need some preliminary results on properties of certain sequences of integers.

Theorem 1 ([BC62, HR66]) *If m is a power of a prime, there exist m integers a_1, \dots, a_m such that*

$$1 \leq a_1 < a_2 < \dots < a_m \leq m^2 - 1,$$

and all the sums $a_i + a_j$ are distinct, $1 \leq i \leq j \leq m$.

Corollary 2 *For any n , there exist at least $M(n) = \lfloor \sqrt{n}/2 \rfloor$ integers $1 \leq a_1 < \dots < a_m \leq n$, such that all the differences $a_j - a_i$ are distinct, $1 \leq i \leq j \leq m$.*

Proof. First note that if all the sums $a_i + a_j$, $1 \leq i \leq j \leq m$, are distinct, then also all the differences $a_j - a_i$, $1 \leq i \leq j \leq m$, are distinct. In fact, $a_j - a_i = a_h - a_k$ would imply $a_j + a_k = a_h + a_i$.

If $\lfloor \sqrt{n} \rfloor$ is a power of a prime, then there exist $m = \lfloor \sqrt{n} \rfloor \geq M(n)$ numbers $1 \leq a_1 < \dots < a_m \leq m^2 - 1 \leq n$ whose differences are distinct and we are done. If $\lfloor \sqrt{n} \rfloor$ is not a power of a prime, let us consider the two consecutive powers of 2 such that $2^h < \lfloor \sqrt{n} \rfloor < 2^{h+1}$. Letting $m = 2^h \geq \lfloor \sqrt{n}/2 \rfloor = M(n)$ we obtain the thesis. \square

We can now prove a structural property of circulant matrices, which sheds some light into the complexity of computing permanents of circulant matrices with enough nonzero entries.

Theorem 3 *Let A be an $n \times n$ circulant matrix with first row $[\alpha_1, \alpha_2, \dots, \alpha_n]$. A has a principal submatrix M of size $m = \theta(\sqrt{n})$ whose off-diagonal entries are distinct elements of the first row of A . More precisely, we have*

$$\lfloor \sqrt{n}/(2\sqrt{2}) \rfloor \leq m \leq \lceil \sqrt{n} + 1 \rceil.$$

Proof. The ij -th entry of the circulant matrix A can be defined as $a_{ij} = \alpha_{1+(n+j-i) \bmod n}$.

The upper bound on m is trivial, since there are $m^2 - m$ off-diagonal entries in M and $n - 1$ in A . Hence we must have $m^2 - m \leq n - 1$, from which we obtain $m \leq \frac{1}{2} + \sqrt{n - \frac{3}{4}} < \lceil \sqrt{n} + 1 \rceil$.

For the lower bound we want to determine a set of indexes $S = \{s_1 < s_2 < \dots < s_m\}$ such that the principal submatrix $M = A(S)$ does not contain repeated elements, except for the diagonal which is constant and equal to the diagonal of A by construction.

Let us assume, for simplicity, that $s_m < n/2$. This implies that the entries of the strictly upper triangular submatrix U of M must be chosen from $\alpha_2, \alpha_3, \dots, \alpha_{s_m}$, while those below the diagonal from $\alpha_{n+2-s_m}, \alpha_{n+3-s_m}, \dots, \alpha_n$. This guarantees that there is not any overlapping between entries above and below the main diagonal.

Two entries of U , say u_{ij} and u_{hk} , with $(i, j) \neq (h, k)$, take the same values if and only if $\alpha_{s_j-s_i+1} = \alpha_{s_k-s_h+1}$. This implies that $u_{ij} \neq u_{hk}$ if and only if

$$s_j - s_i \neq s_k - s_h. \tag{1}$$

The same condition holds for the entries below the diagonal of M .

By Corollary 2 there exists a sequence of $M(n/2) = \lfloor \sqrt{n/2}/2 \rfloor$ indexes that satisfies condition 1 such that $s_m < n/2$, and we obtain the thesis. \square

The above result shows that a circulant graph contains an arbitrary subgraph of size $\theta(\sqrt{n})$. Thus it would be rather surprising to come up with algorithms for computing permanents of arbitrary circulants with running time less than $T(\sqrt{n})$, where $T(n)$ is the worst case running time of the best available algorithm for the general case.

3.2 Circulant vs convertible matrices

In this section we explore the relationship between circulant matrices of the form $I + P + P^j$ and the class of convertible matrices. More precisely, we take advantage of a recent characterization of convertibility [MRST97] in order to analyze “how far” matrices of the form $I + P + P^j$ are from convertible matrices.

3.2.1 Characterization of convertible matrices

Let A be a $(0-1)$ square matrix, and let G be its associated bipartite graph. The complexity of the problem of saying whether or not A is convertible has been shown to be polynomial. Indeed, in [MRST97], the authors give a structural characterization of convertible matrices, and use it to design a polynomial-time algorithm which, given an input matrix A , outputs the $(-1, 1)$ -matrix X such that $\text{per}(A) = \det(A \star X)$, or a certain forbidden submatrix which implies that A is not convertible.

We first recall some results and definitions from [MRST97]. We start with the definitions of the 0-sum and 4-sum graph operations, which are the basic ingredients involved in the characterization of convertible matrices, while we refer to [MRST97] for the definition of the 2-sum operation, which is more complicated and not used in our analysis.

Definition 1 Let $G = (V, E)$ be a bipartite graph with a perfect matching, (A, B) be a bipartition of G , and X be a nonempty proper subset of A such that $|N(X)| = |X|$, where $N(X)$ is the set of vertices adjacent to a vertex in X . Let $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ be the following graphs:

- $V_1 = X \cup N(X)$, $E_1 = \{(a, b) \in E \mid a \in X \wedge b \in N(X)\}$;
- $V_2 = V \setminus V_1$, $E_2 = \{(a, b) \in E \mid a \in A \setminus X \wedge b \in B \setminus N(X)\}$.

Then, we say that G is a 0-sum of G_1 and G_2 .

Definition 2 Let G_0 be a graph, let C be a circuit of G_0 of length four, and let G_1, G_2 be two subgraphs of G_0 such that $G_1 \cup G_2 = G_0$, $G_1 \cap G_2 = C$, $V(G_1) - V(G_2) \neq \emptyset$ and $V(G_2) - V(G_1) \neq \emptyset$. (The intersection and union of two subgraphs are defined in the natural way.) Let G be obtained from G_0 by deleting some (possibly none) of the edges of C . We say that G is a 4-sum of G_1 and G_2 along C .

The characterization of convertible matrices also involves the *Heawood graph*, which is the bipartite graph associated with the incidence matrix of the Fano plane. Note that the Heawood graph is a circulant graph on 14 vertices, whose associated matrix is $I_7 + P + P^3$.

We are now ready to state the main result from [MRST97].

Theorem 4 *The matrix A is convertible if and only if its associated bipartite graph either has no perfect matching, or it can be obtained by repeatedly applying the 0-sum, 2-sum, 4-sum operations starting from connected planar bipartite graphs with perfect matchings and the Heawood graph.*

Roughly speaking, convertible matrices can all be obtained by piecing together planar bipartite graphs and one sporadic non-planar bipartite graph.

3.2.2 Constructions for some special cases

We now use the above characterization in order to analyze the distance from convertibility for some special matrices of the form $I + P + P^j$. We will show that these special matrices are very “close” to convertible matrices, i.e., they become convertible after deleting just a constant number of their entries.

Notice that any circulant matrix of the class under investigation can be obviously transformed into a convertible one, by deleting three entries on the same row (or column). Indeed, in this way we obtain a matrix whose associated graph has no perfect matching. However, in the following analysis we will not consider this trivial transformation, since we are interested in reductions from circulant to convertible matrices that preserve, as far as possible, the structural properties of the associated graphs.

Given an $n \times n$ matrix $A_n = I_n + P_n + P_n^j$, the associated bipartite graph is a cycle of length $2n$, with n additional chords of length $2j - 1$. We will use the following labelling for the vertices: we choose one vertex and label it with $1'$, then we proceed clockwise and label the second vertex with 1 , the third with $2'$, etc. The i -th vertex will thus be labelled with $\lceil i/2 \rceil'$, if i is odd, and with $i/2$, if i is even. Given this labelling, any vertex i , $i = 1, \dots, n$, will be adjacent to i' and $(i + 1)'$ along the cycle, and to the vertex $(i + j)'$ through one of the chords (where the sum is taken mod n).

Matrices of the form $I_n + P_n + P_n^2$. For n even, we can use the characterization of [MRST97] to verify the convertibility of the matrix $A_n = I_n + P_n + P_n^2$. Indeed the bipartite graph $G[A_n]$ can be obtained as the 4-sum of the graphs $G[A_4]$ and $G[A_{n-2}]$, where $A_4 = I_4 + P_4 + P_4^2$ and $A_{n-2} = I_{n-2} + P_{n-2} + P_{n-2}^2$. The convertibility of A_n then follows by induction, since A_4 is connected and planar. In order to obtain this decomposition for $G[A_n]$, the 4-sum operation must be performed along, e.g., the circuit $C \equiv \{(1, 2'), (2', 4), (4, 5'), (5', 1)\}$ of $G[A_4]$ and $G[A_{n-2}]$, from which $G[A_n]$ can be derived by deleting the edges $(5', 1)$ and $(2', 4)$ of C (see Figure 1).

On the contrary, when n is odd, A_n is known to be non-convertible (see [CCR96]). However, it is possible to turn it onto a convertible matrix, just by deleting one of its entries. In fact, $G[A_n]$ can be obtained by a 4-sum of the graphs $G[A_{n-1}]$ and $K_{3,3}$, where $A_{n-1} = I_{n-1} + P_{n-1} + P_{n-1}^2$. Since $n - 1$ is even, we know that A_{n-1} is convertible and $G[A_{n-1}]$ can be obtained as in Theorem 4. Finally, since $K_{3,3}$ can be turned into a planar graph by deleting just one of its edges, then A_n becomes convertible by deleting one of its entries. In this case, the 4-sum operation is performed along, e.g., the circuit $C \equiv \{(1, 2'), (2', 3), (3, 4'), (4', 1)\}$, and then $G[A_n]$ is derived by deleting the edges $(4', 1)$ and $(2', 3)$ of C (see Figure 1).

Matrices of the form $I_n + P_n + P_n^{\frac{n+1}{2}}$. Let $A_n = I_n + P_n + P_n^{\frac{n+1}{2}}$, n odd. In this case it is possible to verify that $G[A_n]$ can be obtained by piecing together, using the 4-sum operation, the connected planar bipartite graphs $G[B_4]$ on 8 vertices, corresponding to the matrix $B_4 = I_4 + P_4 + P_4^2$, and the graph $G[A_{n-2}]$, where $A_{n-2} = I_{n-2} + P_{n-2} + P_{n-2}^{\frac{n-1}{2}}$ (see Figure 2). By repeated applications of the same procedure, we finally obtain a decomposition of $G[A_n]$ into $\frac{n-3}{2}$ graphs (all isomorphic to $G[B_4]$) and the graph $K_{3,3}$. This shows how A_n can be made convertible by deleting only one of its entries.

Matrices of the form $I_n + P_n + P_n^{\frac{n}{2}}$. Let $A_n = I_n + P_n + P_n^{\frac{n}{2}}$, n even. We prove that A_n can be made convertible by deleting two of its entries. We use the following strategy: we first delete two edges from $G[A_n]$, and then verify that the resulting graph $\tilde{G}[A_n]$ can be obtained as a 0-sum of a cycle of length four and a graph G_1 , which is a bipartite graph on $2(n - 2)$ vertices, with the same structure as $\tilde{G}[A_n]$. The result then follows by induction. The basis

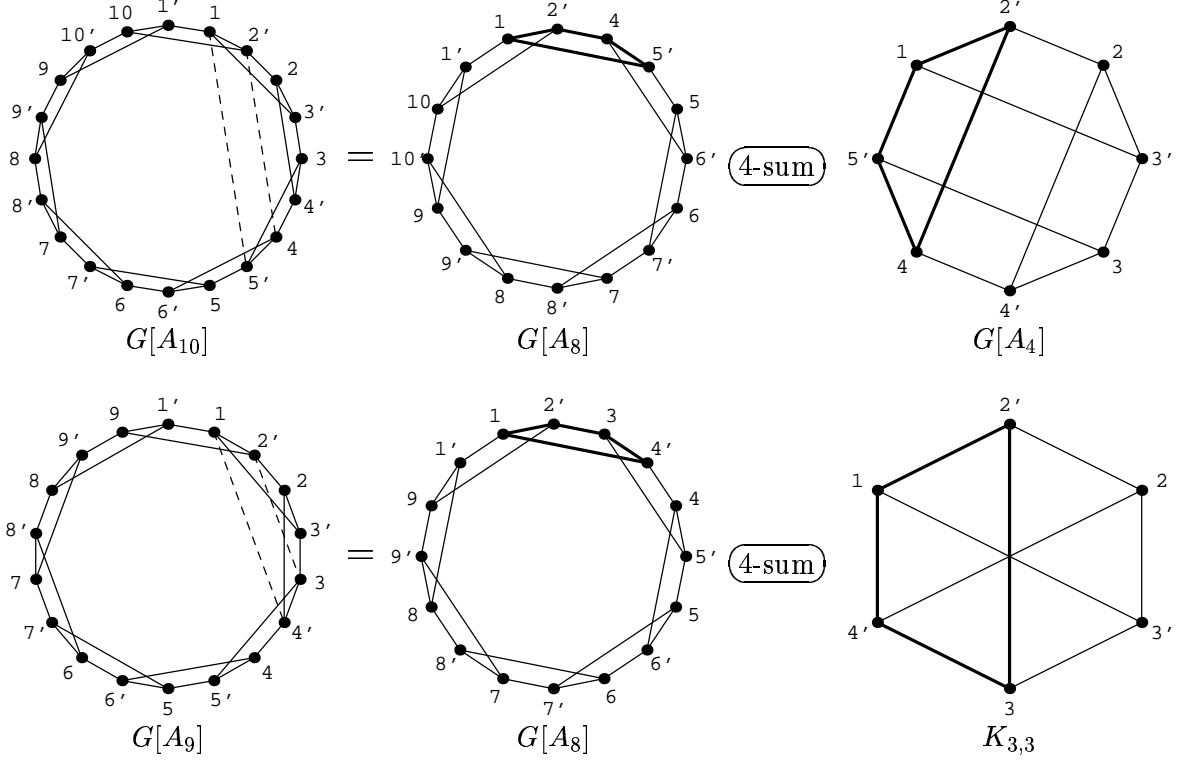


Figure 1: Construction of $G[A_n]$, $A_n = I_n + P_n + P_n^2$, for $n = 10$ and $n = 9$, respectively. $G[A_{10}]$ is obtained as the 4-sum of $G[A_8]$ and $G[A_4]$ along the cycle $\{(1, 2'), (2', 4), (4, 5'), (5', 1)\}$ (bold-faced in $G[A_8]$ and $G[A_4]$), by deleting the edges $(5', 1)$ and $(2', 4)$ (dotted in $G[A_{10}]$). $G[A_9]$ is obtained as the 4-sum of $G[A_8]$ and $K_{3,3}$ along the cycle $\{(1, 2'), (2', 3), (3, 4'), (4', 1)\}$ (bold-faced in $G[A_8]$ and $K_{3,3}$), by deleting the edges $(4', 1)$ and $(2', 3)$ (dotted in $G[A_9]$).

of the induction is provided by the graph $G[A_8]$, whose associated matrix $I + P + P^4$ can be made invertible by deleting at most two entries.

We thus delete from $G[A_n]$ the two edges $(1, 2')$ and $(\frac{n}{2} + 1, (\frac{n}{2} + 2)')$, and obtain the graph $\tilde{G}[A_n]$. Note that these two edges are located in opposite sides, with respect to the center of the cycle representing $G[A_n]$. The set of vertices $X = \{1, 2, \dots, n\} \setminus \{2, \frac{n}{2} + 2\}$ is such that $|X| = |N(X)|$, where $N(X)$ is the set of vertices adjacent to a vertex in X . This implies that $\tilde{G}[A_n]$ can be obtained as a 0-sum of the two graphs $G_2 = \tilde{G}[A_n] \setminus (X \cup N(X))$ and $G_1 = \tilde{G}[A_n] \setminus V(G_2)$, where G_2 is simply given by the cycle $\{(2, (\frac{n}{2} + 2)'), ((\frac{n}{2} + 2)', \frac{n}{2} + 2), (\frac{n}{2} + 2, 2'), (2', 2)\}$.

Let us now examine the structure of G_1 . G_1 is a bipartite graph, whose $2(n - 2)$ vertices can be arranged over a cycle lacking two opposite edges. Moreover, the length ℓ_1 of the chords of G_1 is less (by a factor of two) than the length ℓ of the chords of $\tilde{G}[A_n]$, because of the “subtraction” of the graph G_2 (see Figure 3). Since the length of the chords of $\tilde{G}[A_n]$ is $\ell = 2(\frac{n}{2}) - 1$, we get $\ell_1 = 2(\frac{n-2}{2}) - 1$.

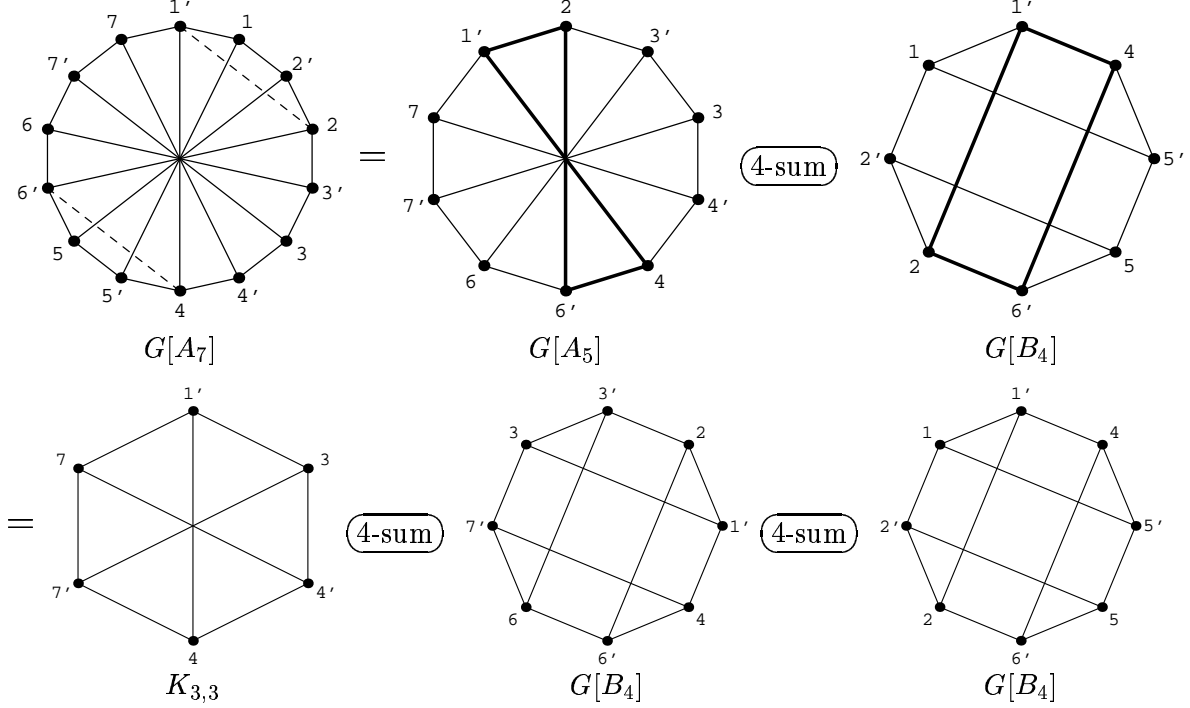


Figure 2: Construction of $G[A_n]$, $A_n = I_n + P_n + P_n^{\frac{n+1}{2}}$, for $n = 7$. $G[A_7]$ is first obtained as the 4-sum of $G[A_5]$ and $G[B_4]$ (where $B_4 = I_4 + P_4 + P_4^2$) along the cycle $\{(1', 2), (2, 6'), (6', 4), (4, 1')\}$ (bold-faced in $G[A_5]$ and $G[B_4]$), by deleting the edges $(1', 2)$ and $(6', 4)$ (dotted in $G[A_7]$). By applying the same procedure to $G[A_5]$, we then obtain a decomposition of $G[A_7]$ into two graphs isomorphic to $G[B_4]$ and $K_{3,3}$.

From these observations, it follows that G_1 has exactly the same structure as $\tilde{G}[A_n]$. In fact, G_1 is the graph obtained from $G[A_{n-2}]$, where $A_{n-2} = I_{n-2} + P_{n-2} + P_{n-2}^{\frac{n-2}{2}}$, by deleting two edges located in opposite sides, with respect to the center of the cycle.

Matrices of the form $I_n + P_n + P_n^{\frac{n}{k}}$. More in general, it is possible to prove, by taking advantage of the 0-sum operation, that any matrix of the form $I_n + P_n + P_n^{\frac{n}{k}}$ can be made convertible by deleting at most k of its entries.

We basically proceed as in the previous case: we first delete k edges from $G[A_n]$, and then verify that the resulting graph $\tilde{G}[A_n]$ can be obtained as a 0-sum of a cycle of length $2k$ and a graph G_1 on $2(n - k)$ vertices, with the same structure of $\tilde{G}[A_n]$.

Let us delete from $G[A_n]$ the set of k edges $\{(\frac{in}{k} + 1, (\frac{in}{k} + 2)') \mid i = 0, 1, \dots, k - 1\}$, and obtain the graph $\tilde{G}[A_n]$. Note that these edges are uniformly distributed along the cycle representing $G[A_n]$. The set of vertices $X = \{1, 2, \dots, n\} \setminus \{\frac{in}{k} + 2 \mid i = 0, 1, \dots, k - 1\}$ is such that $|X| = |N(X)|$. This implies that $\tilde{G}[A_n]$ can be obtained as a 0-sum of $G_2 = \tilde{G}[A_n] \setminus (X \cup N(X))$ and $G_1 = \tilde{G}[A_n] \setminus V(G_2)$.

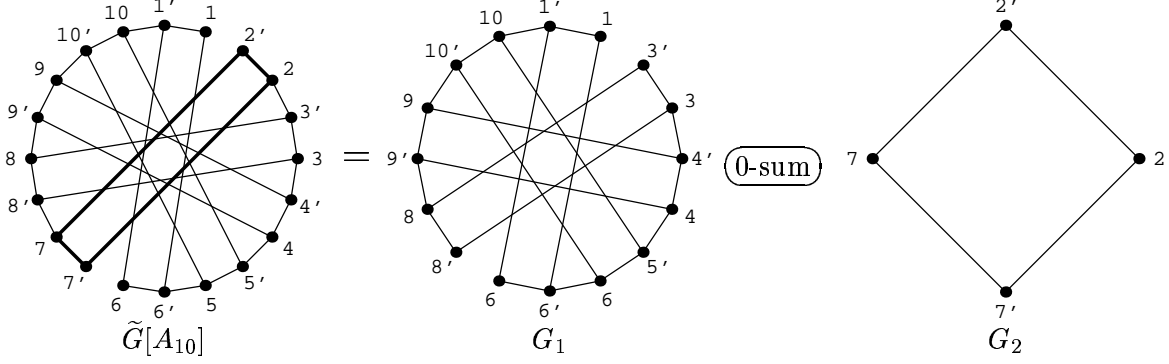


Figure 3: Construction of $\tilde{G}[A_n]$, $A_n = I_n + P_n + P_n^{\frac{n}{2}}$, for $n = 10$. $\tilde{G}[A_{10}]$, which is derived from $G[A_{10}]$ by deleting the edges $(1, 2')$ and $(6, 7')$, is obtained as the 0-sum of G_1 and of the cycle G_2 (bold-faced in $\tilde{G}[A_{10}]$). Note that G_1 has exactly the same structure as $\tilde{G}[A_{10}]$.

G_2 is simply given by the cycle of length $2k$ consisting of the edges $\{((\frac{in}{k} + 2)')', (\frac{in}{k} + 2), (\frac{(i+1)n}{k} + 2)'\} \mid i = 0, 1, \dots, k - 1\}$, where the sums are taken mod n .

G_1 turns out to be a bipartite graph, whose $2(n - k)$ vertices can be arranged over a cycle lacking k edges, uniformly distributed along it. Moreover, the length ℓ_1 of the chords of G_1 is less (by a factor of two) than the length ℓ of the chords of $\tilde{G}[A_n]$, because of the “subtraction” of the graph G_2 (see Figure 4). Since the length of the chords of $\tilde{G}[A_n]$ is $\ell = 2(\frac{n}{k}) - 1$, we get $\ell_1 = 2(\frac{n-k}{k}) - 1$.

From these observations, it follows that G_1 is the graph obtained from $G[A_{n-k}]$, where $A_{n-k} = I_{n-k} + P_{n-k} + P_{n-k}^{\frac{n-k}{k}}$, by deleting k edges uniformly distributed along the cycle. Thus, G_1 has exactly the same structure as $\tilde{G}[A_n]$.

Finally, the fact that the matrix $I_n + P_n + P_n^{\frac{n}{k}}$ can be made convertible by deleting at most k entries, follows by induction, and the basis of the induction is provided by graphs with a constant number of vertices, which can be analyzed by direct inspection.

4 An efficient algorithm

We present an algorithm for computing the permanent of $(0, 1)$ -circulants with three nonzero entries per row which takes advantage of the convertibility of some of their submatrices. This algorithm was already outlined in [CCR96]. Here we are able to add a proof of its worst case running time, we present its implementation, and the experimental results obtained.

Before stating the result we need some simple Lemmas and Definitions from [CCR96] which are reported in Section 4.1, and some equivalences between permanents of different circulant matrices, which are proved in Section 4.2.

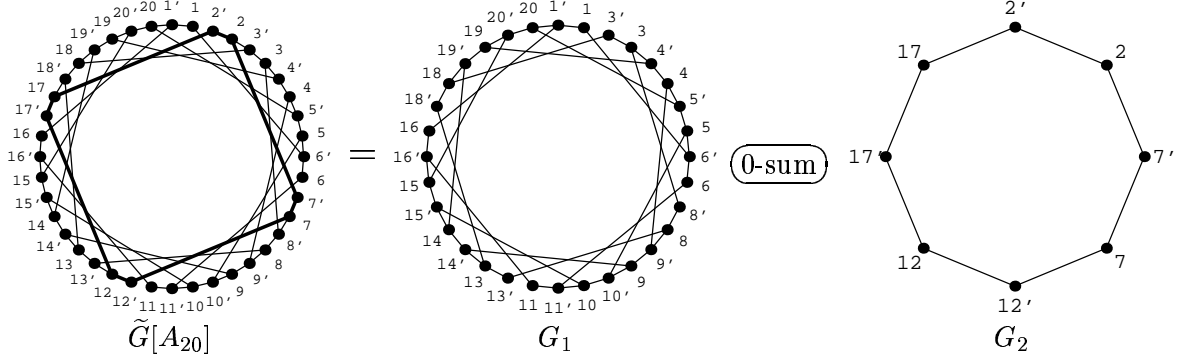


Figure 4: Construction of $\tilde{G}[A_n]$, $A_n = I_n + P_n + P_n^{\frac{n}{k}}$, for $n = 20$ and $k = 4$. $\tilde{G}[A_{20}]$, which is derived from $G[A_{20}]$ by deleting the four edges $(1, 2')$, $(6, 7')$, $(11, 12')$, $(16, 17')$, is obtained as the 0-sum of G_1 and of the cycle G_2 of length eight (bold-faced in $\tilde{G}[A_{20}]$). Note that G_1 has exactly the same structure as $\tilde{G}[A_{20}]$.

4.1 Background

Lemma 5 *Let A be a square $(0, 1)$ matrix such that $G[A]$ is planar. Then the bipartite graph associated with any square submatrix of A is planar.*

Lemma 6 *Let A be a square $(0, 1)$ matrix such that $a_{ij} = 1$. Then*

$$\text{per}(A) = \text{per}(A - E_{ij}) + \text{per}(A(i|j)),$$

where E_{ij} denotes the matrix whose only nonzero entry is in position (i, j) , and $A(i|j)$ denotes the matrix obtained by deleting the i -th row and j -th column of A .

Definition 1 *Let us denote with $\mathcal{P}_{k,n}$ the collection of all k -subsets of the n -set $\{1, 2, \dots, n\}$. Let A be a $(0, 1)$ $n \times n$ matrix. Then, for $\alpha, \beta \in \mathcal{P}_{k,n}$, we denote with $A[\alpha, \beta]$ the $k \times k$ submatrix of A determined by rows $i \in \alpha$ and columns $j \in \beta$. Then $\text{per}(A[\alpha, \beta])$ is called a permanental k -minor of A and we define $p_k(A)$ as the sum of all the permanental k -minors of A , i.e.,*

$$p_k(A) = \sum_{\alpha \in \mathcal{P}_{k,n}} \sum_{\beta \in \mathcal{P}_{k,n}} \text{per}(A[\alpha, \beta]). \quad (2)$$

$p_k(A)$ counts the number of different selections of k ones in A , such that each row and column has at most a nonzero entry.

Lemma 7 *Let A be a $(0, 1)$ $n \times n$ matrix, and let $a_{ij} = 1$. Then $p_k(A) = p_k(A - E_{ij}) + p_{k-1}(A(i|j))$, for $k \geq 2$, and $p_1(A) = p_1(A - E_{ij}) + 1$.*

Lemma 8 Let $A = (a_{ij})$ be an $n \times n$ $(0, 1)$ matrix, and let $z(A)$ denote the number of different $(0, 1)$ matrices $M = (m_{ij})$ with at most one nonzero entry in each row and column, satisfying $M \leq A$, i.e., $m_{ij} \leq a_{ij}$, for all pairs (i, j) . Then, for each nonzero entry a_{ij} , we have

$$z(A) = \sum_{k=1}^n p_k(A) \quad (3)$$

$$z(A) = z(A - E_{ij}) + z(A(i|j)), \quad (4)$$

and, in general, if the matrix A has k nonzero entries, then $k + 1 \leq z(A) \leq 2^k$.

Lemma 9 ([VV89]) The permanent of an $n \times n$ convertible matrix A for which $G[A]$ is planar can be computed in $O(n^\gamma)$ time, $\gamma < 3$.

Theorem 10 Let A , B , and C be $n \times n$ $(0, 1)$ matrices such that $A = B + C$, and let $G[B]$ be planar. Then $\text{per}(A)$ can be computed in $O(z(C)n^\gamma)$ time, $\gamma < 3$.

Lemma 11 The bipartite graphs $G[I + Q^i + Q^j]$ and $G[I + Q^i + (Q^T)^j]$ are planar.

We are now ready to state a theorem proved in [CCR96] that will be the basis to develop an efficient algorithm (see Section 4.3).

Theorem 12 Let $A = I_n + P_n^{i'} + P_n^{j'}$. Then $\text{per}(A)$ can be computed in time $O(2^{i'+j'}n^{O(1)})$, where i' and j' are the two smallest numbers among $\{i, j, n - i, n - j\}$.

4.2 Equivalences

In this section we analyze the relationship between the permanents of different circulants $A = A(i, j) = I + P^i + P^j$ of size n . In particular, given n , we are interested in the number of different values that $\text{per}(A)$ can take, and we want to determine all the matrices B in the same *equivalence class*, i.e., which have the same permanent as A , and such that $\text{per}(B) = \text{per}(I + P^h + P^k)$, for given h and k . Our implementation of the algorithm derived from the results of Section 4.1 strongly relies on these equivalences, especially when n is prime.

In [ET70] are presented two criteria under which two graphs with circulant adjacency matrices are isomorphic. However the analysis we need differs since: (i) we are interested only in matrices of type $A = I + P^i + P^j$, and (ii) $B = P^{-i}A$ has the same permanent of A but the associated graphs are not necessarily isomorphic.

Given an $n \times n$ matrix $A = I + P^i + P^j$, where n is a prime number greater than 2, the bipartite graph $G[A]$ is a cycle of length $2n$ with n additional chords of length d [CCR96]. It is clear that if two different circulant matrices A and B of size n lead to the same chord lengths, then their associated graphs $G[A]$ and $G[B]$ are isomorphic and thus $\text{per}(A) = \text{per}(B)$.

Depending on n , i and j , the chord lengths will take one of the $(n - 1)/2$ odd values between 3 and n then there can be at most $(n - 1)/2$ different permanents.

In general, this “cycle+chords” representation is not unique. For example, in Figure 5, two different graphs, both corresponding to $A = I + P^4 + P^6$ are shown. In the first graph the edges of the cycle arise from I and P^4 , while the chords correspond to P^6 . The second graph is obtained using P^4 and P^6 for the cycle and I for the chords.

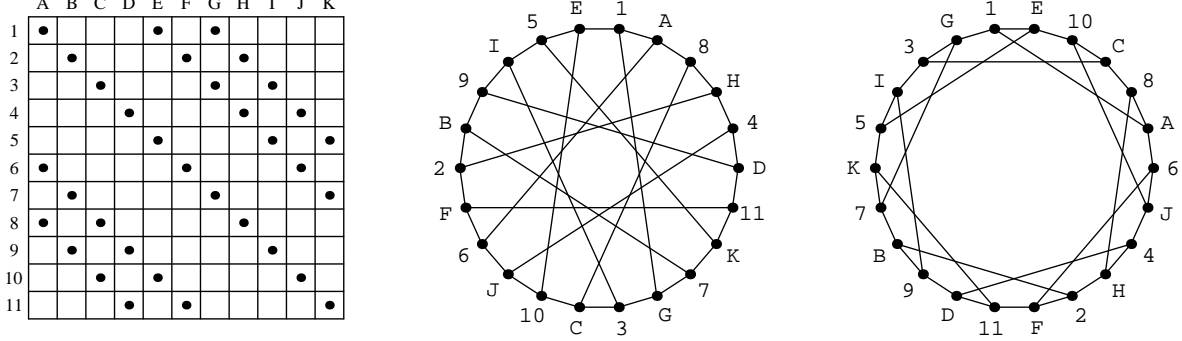


Figure 5: The matrix $A = I + P^4 + P^6$, for $n = 11$, and two equivalent descriptions of $G[A]$, with $d = 9$ and $d = 5$.

The above example can be easily generalized. Given an $n \times n$ matrix $A = I + P^i + P^j$, with n prime, we can obtain three “cycle+chords” representations of $G[A]$. When the chords correspond to I , their length can be computed as

$$D(n, i, j) = n - \left| n - 2 \left[i (j - i)^{-1} \right]_{\mathbf{Z}_n} - 1 \right|, \quad (5)$$

where the absolute value takes care of the fact that the chords with lengths d and $2n - d$ coincide. The notation $[E]_{\mathbf{Z}_n}$ indicates that the expression E is computed within the field \mathbf{Z}_n . The length of the chords of the other two representations of $G[A]$, can be obtained considering the two matrices $P^{n-i}A = I + P^{n-i} + P^{j-i}$ and $P^{n-j}A = I + P^{n-j} + P^{n+i-j}$. In other words, we look at the bipartite graphs $G[P^{n-i}A]$ and $G[P^{n-j}A]$. Assuming $j > i$, their chord lengths $D'(n, i, j)$ and $D''(n, i, j)$ satisfy

$$D'(n, i, j) = D(n, n - i, j - i) = n - \left| n - 2 \left[(j - i) (n - j)^{-1} \right]_{\mathbf{Z}_n} - 1 \right| \quad (6)$$

$$D''(n, i, j) = D(n, n - j, n + i - j) = n - \left| n - 2 \left[(n - j) i^{-1} \right]_{\mathbf{Z}_n} - 1 \right|. \quad (7)$$

For a given prime n , let us consider the triples $T_{i,j} = (a_{i,j}, b_{i,j}, c_{i,j}) \in \mathbf{Z}_n^3$, for $1 \leq i < j \leq n - 1$, where $a_{i,j} = (j - i)^{-1}i$, $b_{i,j} = i^{-1}(n - j)$ and $c_{i,j} = (n - j)^{-1}(j - i)$. The values $a_{i,j}$, $b_{i,j}$, and $c_{i,j}$ correspond to the ‘inner’ parts of $D(n, i, j)$, $D'(n, i, j)$ and $D''(n, i, j)$, respectively. Thus, if two triples $T_{i,j}$, and $T_{h,k}$, share a value, then $\text{per}(I + P^i + P^j) = \text{per}(I + P^h + P^k)$. Theorem 14 below characterizes the set of triples associated with a prime number n . Before

stating the theorem, we need the following technical lemma.

Lemma 13 *If p is a prime, then the congruence $x^n \equiv 1 \pmod{p}$ has $\gcd(n, p-1)$ solutions.*

Proof. See Theorem 2.27 in [NZ80]. □

Theorem 14 *For a given prime n , the following facts hold*

1. $1 \leq a_{i,j}, b_{i,j}, c_{i,j} \leq n-2$, and, for each $1 \leq t \leq n-2$, there exist i, j, i', j', i'', j'' such that $a_{i,j} = b_{i',j'} = c_{i'',j''} = t$.
2. If two triples have one element in common, then all their elements coincide.
3. The triples contain either three distinct values or an element repeated three times. The latter case happens only when $n \equiv 1 \pmod{3}$, and the repeated values u and v satisfy $u \neq v$, $u, v \neq 1$ and $u^3 \equiv v^3 \equiv 1 \pmod{n}$.

Proof.

1. Since $a_{i,i+1} = i$, then $a_{i,i+1}$ takes all the values between 1 and $n-2$, as i varies. It never occurs that $a_{i,j} = n-1 \equiv -1$, because $a_{i,j} = (j-i)^{-1}i = n-1$ would imply $j-i \equiv -i \pmod{n}$, and thus $j=0$, which is excluded by hypothesis. The proofs for $b_{i,j}$ and $c_{i,j}$ are similar.
2. Let us suppose that $a_{i,j} = a_{h,k}$ (the other cases are similar). From $(j-i)^{-1}i = (k-h)^{-1}h$ we obtain $i(k-h) = h(j-i)$, $ik = hj$ and $i^{-1} = kh^{-1}j^{-1}$. Thus we have

$$b_{i,j} = i^{-1}(n-j) = kh^{-1}j^{-1}(-j) = -kh^{-1} = (n-k)h^{-1} = b_{h,k}.$$

Since $ik = hj$ implies $j^{-1} = hi^{-1}k^{-1}$ and $j = ikh^{-1}$, we have

$$c_{i,j} = (n-j)^{-1}(j-i) = -hi^{-1}k^{-1}(ikh^{-1} - i) = -1 + hk^{-1} = (n-k)^{-1}(k-h) = c_{h,k}.$$

3. Let us assume that $a_{i,j} = b_{i,j}$. We obtain $(j-i)^{-1}i = i^{-1}(n-j)$, and

$$i^2 + j^2 \equiv ij \pmod{n}. \tag{8}$$

From $a_{i,j} = c_{i,j}$ and $c_{i,j} = b_{i,j}$ we obtain exactly the same condition, thus if (8) holds, then $a_{i,j}$, $b_{i,j}$ and $c_{i,j}$ coincide, while if (8) does not hold, then they are all distinct. Since in general we have $a_{i,j}b_{i,j}c_{i,j} \equiv 1 \pmod{n}$, if $a_{i,j} = b_{i,j} = c_{i,j}$, they must be equal to one of the cubic roots of 1 in \mathbf{Z}_n , with the exception of the value 1 (in order to have $a_{ij} = 1$, we should have $i-j \equiv i$, that is $j=0$, which is impossible). By Lemma 13, the only cubic root of 1, in \mathbf{Z}_n , when $n \equiv 2 \pmod{3}$, is 1. Hence in this case no

triple has coincident values, while if $n \equiv 1 \pmod{3}$ there are two other cubic roots, say u and v , i.e., the two triples (u, u, u) and (v, v, v) .

□

We can now resume our investigation on the sets of chord lengths that guarantee that different matrices have the same permanent, i.e.,

$$\mathcal{T}(n) = \{\{D(n, i, j), D'(n, i, j), D''(n, i, j)\} : 1 \leq i < j < n\}.$$

It is clear from relations (5–7) that if $a_{i,j} = a_{h,k}$ or $a_{i,j} = n - 1 - a_{h,k}$ then $D(n, i, j) = D(n, h, k)$, and the same holds for $b_{i,j}$ and $c_{i,j}$, too. Taking into account the results of Theorem 14 we obtain the following characterization of $\mathcal{T}(n)$.

Theorem 15 *The set $\mathcal{T}(n)$ has the following structure:*

- If $n \equiv 2 \pmod{3}$, then $\mathcal{T}(n)$ consists of $(n - 5)/6$ triples and a couple equal to $\{3, n\}$.
- If $n \equiv 1 \pmod{3}$, then $\mathcal{T}(n)$ consists of $(n - 7)/6$ triples, a couple equal to $\{3, n\}$ and a singleton $\{w\}$, where $w = 2 \min\{u, v\} + 1$, and u, v are defined as in the proof of statement 3 of Theorem 14.

In both cases, the sets in $\mathcal{T}(n)$ are a partition of the set $\{3, 5, 7, \dots, n - 2, n\}$.

Proof. The proof easily follows from Theorem 14. In fact, given two triples $T_{i,j}$ and $T_{h,k}$ such that $a_{i,j} = (n - 1) - a_{h,k}$ (and thus $a_{i,j}$ and $a_{h,k}$ are mapped in the same $D(n, i, j)$ by $x \mapsto n - |n - 2x - 1|$), it is easy to check that $b_{i,j} = (n - 1) - c_{h,k}$ and $c_{i,j} = (n - 1) - b_{h,k}$. Hence $T_{i,j}$ and $T_{h,k}$ lead to the same element of $\mathcal{T}(n)$. The same is true for $a_{i,j} = (n - 1) - c_{h,k}$ or $a_{i,j} = (n - 1) - b_{h,k}$.

There are two special cases. The first is given by the triples $(1, (n - 1)/2, n - 2)$, $((n - 1)/2, n - 2, 1)$ and $(n - 2, 1, (n - 1)/2)$ which lead to the couple $\{3, n\}$ in $\mathcal{T}(n)$. The second is given by the triples $\{u, u, u\}$ and $\{v, v, v\}$, when $n \equiv 1 \pmod{3}$.

Since $u \neq 1$ and $v \neq 1$ are two cubic roots of unity, we have that $u + v = n - 1$, and thus the two triples (u, u, u) and (v, v, v) lead to the same singleton $\{w\}$, where $w = 2 \min\{u, v\} + 1$, in $\mathcal{T}(n)$.

Except for these two special cases, it is easy to prove that, when $a_{i,j}$, $b_{i,j}$ and $c_{i,j}$ are distinct, then $D(n, i, j)$, $D'(n, i, j)$, and $D''(n, i, j)$ are distinct, too. Thus $\mathcal{T}(n)$ is indeed a partition, since all values $\{3, 5, 7, \dots, n - 2, n\}$ are spanned by $n - |n - 2x - 1|$ as x varies between 1 and $n - 2$. □

Since all matrices $I_n + P^i + P^j$ whose $D(n, i, j)$, $D'(n, i, j)$ or $D''(n, i, j)$ belong to the same element of $\mathcal{T}(n)$ have the same permanent, we have the following corollary.

Corollary 16 For any prime n , $\text{per}(I_n + P^i + P^j)$, for $1 \leq i < j \leq n - 1$, can take at most $\lceil n/6 \rceil$ different values.

We now prove some Lemmas that will be used in Theorem 19 to evaluate the computational cost of our algorithm.

Lemma 17 For every prime n and every $d = 1, \dots, n - 2$, the congruence $x(d + 1) + y \equiv 0 \pmod{n}$ is satisfied by a couple of values x and y such that $0 < x \leq \frac{1}{2}\sqrt{2}\lceil\sqrt{n}\rceil$ and $0 < |y| \leq \sqrt{2}\lceil\sqrt{n}\rceil$.

Proof. Let us compute the expression $x(d+1)+y \pmod{n}$ for all the values $|x| \leq \frac{1}{4}\sqrt{2}\lceil\sqrt{n}\rceil$ and $|y| \leq \frac{1}{2}\sqrt{2}\lceil\sqrt{n}\rceil$. Since

$$(1 + 2\frac{1}{4}\sqrt{2}\lceil\sqrt{n}\rceil)(1 + 2\frac{1}{2}\sqrt{2}\lceil\sqrt{n}\rceil) > n,$$

by pidgeon-hole principle there will be two distinct couples x_1, y_1 and x_2, y_2 such that

$$x_1(d + 1) + y_1 \equiv x_2(d + 1) + y_2 \pmod{n}.$$

Let us assume, without loss of generality, that $x_1 \geq x_2$, and define $x = x_1 - x_2$ and $y = y_1 - y_2$. It is clear that $x(d + 1) + y \equiv 0 \pmod{n}$, as requested. Let us prove that $x, y \neq 0$. If $y = 0$ then the congruence reduces to $x(d + 1) \equiv 0 \pmod{n}$. Since n is prime this is possible only if $x = 0$, but this will imply that $x_1 = x_2$ and $y_1 = y_2$, which is a contradiction. The case for $x = 0$ is similar. \square

Lemma 18 For every prime n and every $d = 1 \dots n - 2$, there are two values, i and j with $0 < i + j \leq 2\sqrt{2}\lceil\sqrt{n}\rceil$ such that at least one of the two congruences $b_{i,j} = i^{-1}(n - j) \equiv d \pmod{n}$ and $b_{i,j} = i^{-1}(n - j) \equiv n - 1 - d \pmod{n}$ is satisfied.

Proof. Since n is prime we can rewrite the congruences as $id \equiv -j \pmod{n}$ and $(d+1)i \equiv j \pmod{n}$. Let $x > 0$ and $y \neq 0$ the two values provided by Lemma 17 so that $x(d + 1) + y \equiv 0 \pmod{n}$. We have two cases:

- $y < 0$. We have $x(d + 1) \equiv -y \pmod{n}$ and taking $i = x$ and $j = -y$ we see that $j \equiv (d + 1)i \pmod{n}$ is satisfied.
- $y > 0$. We have $xd + x + y \equiv 0 \pmod{n}$, and hence $xd \equiv -(x + y) \pmod{n}$. Letting $i = x$ and $j = x + y$ we obtain that $id \equiv -j \pmod{n}$ is verified.

\square

We can now evaluate the computational cost of our algorithm.

Theorem 19 *Let $A = I_n + P_n^i + P_n^j$, with n prime. Then $\text{per}(A)$ can be computed in time $O(2^{c\sqrt{n}}n^{O(1)})$, where $c \leq 2\sqrt{2}$.*

Proof. Given A , we want to prove the existence of a circulant $B = I_n + P_n^{i'} + P_n^{j'}$ with $\text{per}(B) = \text{per}(A)$ such that $i' + j' \leq 2\sqrt{2}\lceil\sqrt{n}\rceil$. The thesis will then easily follow from Theorem 12.

Let us consider the value $d = b_{i,j}$ associated to A . Any other pair of values i' and j' such that $b_{i',j'} = d$ or $b_{i',j'} = n - 1 - d$ will lead to the same permanent, as seen above. Since in Lemma 18 we indeed proved the existence of such a pair, with sum bounded by $2\sqrt{2}\lceil\sqrt{n}\rceil$, the thesis easily follows. \square

4.3 Implementation of the algorithm

Given as input an $n \times n$ circulant matrix $B = I + P^i + P^j$, our implementation of the algorithm deriving from the results of Sections 4.1 and 4.2 works as follows.

1. Among the $n \times n$ circulant matrices $A = I + P^h + P^k$, with $\text{per}(B) = \text{per}(A)$, find one that minimizes $h' + k'$ where h' and k' are the two smallest numbers among $\{h, k, n-h, n-k\}$.
2. Fill with 2's the two chosen diagonals (of length h' and k') of the matrix A .
3. Set $S = 0$.
4. Push A in the stack.
5. While the stack is not empty:
 - (a) Pop a matrix M from the stack.
 - (b) If M does not contain entries equal to 2, then find a conversion M' of M and compute $S \leftarrow S + \det(M')$.
 - (c) Else, if $M_{ij} = 2$, then push in the stack the matrix obtained from M by setting $M_{ij} = 0$ and the matrix obtained from M by deleting the i -th row and j -th column.
6. End of While.
7. S is equal to $\text{per}(B) = \text{per}(A)$.

Let us analyze in more details the crucial steps of the above algorithm. In Step 1, we find a circulant matrix A , with $\text{per}(B) = \text{per}(A)$, that minimizes the number $h' + k'$ of entries to be 'eliminated'. This step, which is accomplished exploiting the relations between the permanents of the circulants (see Section 4.2), needs only $O(n^2)$ operations, but it actually determines the computational cost of the rest of the algorithm, which is proportional to $2^{h'+k'}$.

When n is prime, by Theorem 19, we have $h' + k' \leq 2\sqrt{2}\sqrt{n}$. Experimentally we found that for feasible values of n the multiplicative constant is smaller than $2\sqrt{2}$ and approximately equal to 1.15. When n is not prime, experimental results show that $h' + k' \leq n/2$, and we are still investigating the behaviour of the algorithm.

Step 5b consists of two parts. We first find a conversion of M , that is a matrix M' such that $\det(M') = \text{per}(M)$. Then we compute $\det(M')$. The computation of M' is performed by a simplified version of the Brualdi & Shader convertibility-test algorithm [BS95]. The simplification is due to the fact that we know in advance that the input matrix is convertible. This warrants that the algorithm has a polynomial cost. The conversion routine can be sketched as follows (for simplicity we identify M with the digraph whose adjacency matrix is M):

1. Permute M in such a way that $M \geq I$ (element-wise). If this is not possible, then $\det(M) = \text{per}(M) = 0$ and we are done.
2. Set all the diagonal entries of M to -1 .
3. Find the strong connected components of M .
4. For each strong connected component C of M :
 - (a) Select a node x of C . Let $C = C - \{x\}$. Let G be equal to a graph consisting only of x .
 - (b) While C is not empty:
 - i. Find a path or a cycle w whose endpoints are in G and whose edges and mid-points are in C .
 - ii. If w is a cycle, set the sign of one edge to -1 , and all the others to 1.
 - iii. If w is not a cycle, but a path joining x and y , find any path from y to x in G . If this path is negative, set all the signs of the edges of w to 1; if it is positive, set the sign of one edge to -1 , and all the others to 1.
 - iv. Let $C = C - w$ and $G = G \cup w$.
 - (c) End While
 - (d) Substitute C with G , in M .
5. End For

The computation of the determinant of an integer matrix M of size n is performed by resorting to the Chinese Remainder Theorem. We choose k distinct primes p_1, \dots, p_k of magnitude around $2^{15} = 32768$, such that

$$\prod_{i=1}^k p_i > 2 \max_{h,k} \text{per}(I_n + P_n^h + P_n^k).$$

For example, for $n = 103$, we need $k = 6$ primes. Then we compute the determinant of M in \mathbf{Z}_{p_i} , for $i = 1, \dots, k$, and using the Chinese Remainder Theorem we obtain $\det(M)$. The determinants are computed via modular Gaussian elimination. To speed-up the inversion of pivotal elements, the tables of inverses in \mathbf{Z}_{p_i} , for $i = 1, \dots, k$, are precomputed and stored. The choice of $p_i \approx 2^{15}$ allows us to maintain tables of inverses of reasonable size, and to perform integer multiplication in common 32-bits arithmetic without overflow. An alternative to modular arithmetic would consist of using a package for multiple precision arithmetic. This latter approach would not speed-up the algorithm, since in this case Gaussian elimination would operate either on rationals or on floating point numbers of suitable precision.

4.4 Experimental results

The algorithm described in Section 4.3 has been implemented in the C language, the code compiled with the GNU GCC compiler, and the experiments carried out on a SUN Superspark 20 workstation. Table 1 reports the time elapsed by our algorithm for matrices of prime size less than 103. Table 2 contains the values of the permanent of $I_n + P_n + P_n^k$ for $n \leq 101$, n prime.

It is known that permanents of matrices with three ones in each row and column are exponential in the size of the matrix. A great deal of work has been made in estimating the value of the basis of the exponentials. In particular, Minc [Mi87] finds formulas to estimate the dominating term α in the expressions $\alpha^n + \sum \beta_i^n$ for circulant permanents. We have used our algorithm to get a table of estimates for α . More precisely, Table 3 contains the values of the n -th root of the permanent of $I_n + P_n + P_n^k$ for $n \leq 131$. For these values of n we see that $1.39 \leq \sqrt[n]{\text{per}(I + P + P^k)} \leq 1.618$.

4.5 Further observations

We developed an algorithm for the permanent of $A = I + P^i + P^j$ which exploits the convertibility of the matrix B obtained after deleting two of the five diagonals of ones in A . The key property which guarantees the correctness of the algorithm is the planarity of $G[B]$. Not only this implies the convertibility of B , but also the planarity of all the graphs corresponding to the submatrices of B generated during the execution of the algorithm.

Since the cost of our algorithm is proportional to 2^k , where k is the number of 1's marked for deletion, it would be desirable to determine if k can be decreased, still maintaining the overall structure of the algorithm. In general the above question has a positive answer. For example, our algorithm applied to $A = I_7 + P + P^5$ marks 3 ones, which gives rise to the computation of 8 determinants, although the matrix A is already convertible, and thus one determinant computation would be enough.

As a first step toward understanding how and when Theorem 10 can be generalized exploiting convertibility instead of planarity, we have showed, in Section 3.2, that some circulants of

n	#	$j' + h'$	Min T.	Max T.	Ryser T.
5	1	2	0.60	0.60	< 0.01
7	2	3	0.61	0.61	< 0.01
11	2	3	0.61	0.61	0.01
13	3	4	0.61	0.64	0.02
17	3	4	0.62	0.68	0.35
19	4	5	0.63	0.74	1.45
23	3	5	0.64	0.82	25
29	5	5	0.71	0.99	2075
31	6	6	0.72	1.38	8670
37	7	7	0.81	2.94	0.5×10^6
41	7	7	0.88	3.51	8.8×10^6
43	8	7	0.92	3.95	.
47	8	7	1.02	4.64	.
53	9	7	1.20	6.08	.
59	10	8	1.44	13.6	.
61	11	9	1.54	30.6	.
67	12	9	1.86	41.2	.
71	12	9	2.07	43.6	.
73	13	9	2.22	49.7	.
79	14	10	2.65	103.6	.
83	14	9	3.00	58.9	.
89	15	10	3.59	145.0	.
97	17	11	4.52	338.2	.
101	17	11	5.02	390.4	1.0×10^{25}

n	#	$j' + h'$
6	3	3
8	3	4
9	3	3
10	3	5
12	8	6
14	6	7
15	7	5
16	8	8
18	11	9
20	10	10
21	10	7
22	7	11
24	21	12
25	6	5
26	10	13
27	9	9

Table 1: Times (in seconds) spent by our algorithm for various values of the size n . Column marked # reports the number of different values of the permanent; column labeled $j' + h'$ reports the maximum number of elements marked for elimination; columns Min T. and Max T. contain the minimum and maximal time elapsed for a problem of size n , respectively. For comparison we also report the actual or estimated times spent by a carefully implemented version of Ryser’s algorithm.

the form $I + P + P^k$ are “structurally” close to nontrivial convertible matrices. Unfortunately a submatrix of a convertible matrix is not necessarily convertible, and thus the generalization is not straightforward.

Given a circulant matrix $A = I + P^i + P^j$ we want to find a minimal subset $\mathcal{S}_{i,j}$ of the nonzero entries of A such that all the $2^{|\mathcal{S}_{i,j}|}$ submatrices obtained by zeroing some elements in $\mathcal{S}_{i,j}$ and deleting the rows and the columns containing the others, are convertible. In Table 4 we show some experimental results comparing for various n the maximum number M_n of 1’s marked for elimination by our algorithm with $S_n = \max_{i,j} |\mathcal{S}_{i,j}|$. The values of S_n have been determined by an exhaustive enumeration of all the possible subsets $\mathcal{S}_{i,j}$. These preliminary results seem to suggest that this approach can be convenient when n , the matrix size, is a composite number; however a more precise investigation of the properties of the pattern of

k	17
2	3573
3	785
4	581

k	19
2	9351
3	1637
4	1105
8	1143

k	23
2	64081
3	7225
4	4097
5	4097

k	29
2	1149853
3	68675
4	29525
5	28249
9	29757

k	31
2	3010351
3	146137
4	57167
5	54625
6	53571
12	57632

k	37
2	54018523
3	1420581
4	416327
5	396939
6	373037
8	426613
11	376071

k	41
2	370248453
3	6503177
4	1568499
5	1511673
6	1372437
12	1358333
13	1629589

k	43
2	969323031
3	13928219
4	3046123
5	2955651
6	2638225
7	2547495
9	3190001
10	2606921

k	47
2	6643838881
3	63983829
4	11500057
5	11366953
6	9767731
7	9413727
10	12261269
11	9526809

k	53
2	119218851373
3	631558391
4	84528961
5	86571899
6	70097485
7	64856845
8	67149837
11	92894163
12	66484793

k	59
2	2139295485801
3	6244908457
4	622595497
5	665382061
6	505021949
7	453652065
8	450616279
9	477247581
19	707680577
25	471616621

k	61
2	5600748293803
3	13407127661
4	1211861627
5	1315110105
6	976787147
7	863270905
8	862370179
9	908983817
14	867387795
17	917795389
22	1393937233

k	67
2	100501350283431
3	132727996427
4	8947448271
5	10190642249
6	7074918335
7	6055353205
8	6030910265
9	6024618295
10	6542432485
13	6517549489
14	10681787089
30	5931135339

k	71
2	688846502588401
3	612103287547
4	33957153531
5	39998871977
6	26540088263
7	22169473529
10	21923812393
16	21899281183
17	24289855301
21	24311987137
22	22071111975
23	41602991165

k	73
2	1803423556807923
3	1314551907889
4	66170258119
5	79289090017
6	51428337797
7	42456169575
8	41942454413
9	41680894464
11	46820047817
14	42159327339
15	82148571995
16	47021399629
17	41872768613

k	79
2	32361122672259151
3	13022543350313
4	490120158721
5	618688966103
6	374841497481
7	298235966941
9	289197065653
10	293979684257
12	341033311759
15	293199570317
19	335948035781
24	290253939819
28	633674437077
29	295855748291

k	83
2	221806434537978681
3	60072300386417
4	1863889859393
5	2436758511409
6	1410976216021
7	1095259679917
8	1083125196781
9	1060319697963
10	1046520278153
11	1085182066427
17	2477432460715
18	1280975924545
19	1072923467581
20	1251279477883

k	89
2	3980154972736918053
3	595210894056733
4	13839128604605
5	19070671004881
6	10322681530685
7	7717016548793
8	7634726841031
9	7349177621409
13	9357335794629
14	7330168349929
17	7526872339483
24	9008833568301
25	7335653104869
28	7643991831455
29	19187093799869

k	97
2	186982561199565069123
3	12667660180079657
4	200877989540023
5	296810077457753
6	147037002274969
7	104430193868633
8	104032722638089
9	98678638779713
10	97690229972273
11	97445494747147
18	97194604354623
19	133288159653127
20	294858794172343
21	103340544397733
22	101241405666173
26	125581432734649
36	96048233476839

k	101
2	1281597540372340914253
3	58440797725311553
4	765969157839923
5	1171504743943733
6	555557395068609
7	384382573015057
8	384553737065627
9	360680369008463
10	350967636680449
12	356424208391333
13	380243327921165
14	357266201596117
15	469339822694977
16	355371773799257
22	371758351715967
33	1157094722290417
40	503981220951531

k	5	7	11	13
2	13	31	201	523
3		24	91	185
4				159

Table 2: Permanents of $I_n + P_n + P_n^k$ for $n \leq 101$ prime.

k	73	k	79	k	83	k	89	k	97	k	101	k	131
2	1.6180	2	1.6180	2	1.6180	2	1.6180	2	1.6180	2	1.6180	2	1.618034
3	1.4656	3	1.4656	3	1.4656	3	1.4656	3	1.4656	3	1.4656	3	1.465571
15	1.4110	28	1.4106	17	1.4103	29	1.4101	5	1.4099	5	1.4099	5	1.409878
5	1.4103	5	1.4101	5	1.4101	5	1.4100	20	1.4098	33	1.4098	43	1.409387
4	1.4068	4	1.4060	4	1.4055	4	1.4049	4	1.4043	4	1.4040	4	1.402656
6	1.4019	6	1.4012	6	1.4008	6	1.4003	6	1.3998	6	1.3995	6	1.398521
16	1.4002	12	1.3995	18	1.3992	13	1.3988	19	1.3984	40	1.3982	19	1.397614
11	1.4001	19	1.3993	20	1.3988	24	1.3982	26	1.3975	15	1.3972	32	1.395832
7	1.3983	7	1.3972	7	1.3965	7	1.3957	7	1.3948	7	1.3945	8	1.393020
14	1.3981	29	1.3970	8	1.3964	8	1.3956	8	1.3948	8	1.3945	7	1.392411
8	1.3980	10	1.3969	11	1.3964	28	1.3956	21	1.3947	13	1.3943	17	1.392305
17	1.3980	15	1.3969	19	1.3962	17	1.3953	22	1.3944	22	1.3940	15	1.391956
9	1.3979	24	1.3967	9	1.3960	9	1.3950	9	1.3940	9	1.3936	9	1.391385
		9	1.3966	10	1.3958	14	1.3949	10	1.3939	12	1.3934	37	1.391121
						25	1.3949	11	1.3938	14	1.3934	20	1.391073
								18	1.3938	16	1.3934	31	1.390916
								36	1.3936	10	1.3932	21	1.390766
												24	1.390677
												10	1.390593
												18	1.390572
												16	1.390567
												11	1.390562

Table 3: The entries of the table are the values $\alpha = \sqrt[n]{\text{per}(I_n + P_n + P_n^k)}$, for different values of n and k .

the subsets $\mathcal{S}_{i,j}$ is needed.

n	7	8	9	10	11	12	13	14	15	16	17	18
M_n	3	4	3	5	3	6	4	7	5	8	4	9
S_n	1	2	3	2	3	3	4	4	4	4	4	4

Table 4: The maximum number M_n of 1's marked for elimination by our algorithm compared with $S_n = \max_{i,j} |\mathcal{S}_{i,j}|$.

5 Conclusions

In this paper we have provided an investigation on permanents of $(0, 1)$ -circulant matrices. We have shown that, for dense enough circulant matrices, these permanents do not seem to be significantly easier than in the general case. On the other hand we have developed and implemented a very efficient algorithm for the permanent of very sparse circulants, thus showing that they are more tractable. Notice that this contrasts with what happens for general matrices, where the restriction to matrices with three nonzeros per row does not make the problem easier.

Acknowledgment. We acknowledge the help of P. L. Montgomery, who suggested us a scheme for the proof of Lemma 17.

References

- [BC62] R.C. Bose, and S. Chowla. Theorems in the Additive Theory of Numbers. *Comment. Math. Helv.* 37:141-147 (1962-63).
- [BS95] R.A. Brualdi, and B.L. Shader. Matrices of sign-solvable linear systems. *Cambridge University Press (1995)*.
- [CCR96] B. Codenotti, V. Crespi, and G. Resta. On the Permanent of Certain (0,1) Toeplitz Matrices. *Linear Algebra and its Applications*, accepted for publication.
- [DLMV88] P. Dagum, M. Luby, M. Mihail, and U. Vazirani. Polytopes, Permanents, and Graphs with Large Factors. *Proc. 27th IEEE Symp. on Found. of Comput. Sc. (1988)*.
- [ET70] B. Elspas and J. Turner. Graphs with Circulant Adjacency Matrices. *J. Combinatorial Theory*, 9:297-307 (1970).
- [FL92] U. Feige, and C. Lund. On the Hardness of Computing the Permanent of Random Matrices. *Proc. 24th ACM Symp. on the Theory of Comput.* 643-654 (1992).
- [HR66] H. Halberstam, and K.F. Roth. Sequences. *Oxford University Press (1966)*.
- [MRST97] W. McCuaig, N. Robertson, P.D. Seymour and R. Thomas. Permanents, Pfaffian orientations, and even directed circuits (extended abstract). *Proc. 29th ACM Symp. on the Theory of Comput.* 402-405 (1997).
- [Mi87] H. Minc. Permenental Compounds and Permanents of (0, 1) Circulants. *Linear Algebra and its Appl.* 86:11-42 (1987).
- [NZ80] I. Niven and H.S. Zuckerman. An Introduction to the Theory of Numbers, *Jonh Wiley & Sons*, (1980).
- [R63] H.J. Ryser. Combinatorial Mathematics. *Carus Mathematical Monograph No. 14 (1963)*.
- [V179] L.G. Valiant. The complexity of computing the permanent. *Theoretical Computer Science* 8:189-201 (1979).
- [V279] L.G. Valiant. Completeness classes in algebra. *ACM Symp. on the Theory of Comput.* 249-261 (1979).
- [VV89] V.V. Vazirani. NC Algorithms for Computing the Number of Perfect Matchings in $K_{3,3}$ -Free Graphs and Related Problems. *Information and Comput.* 80 152-164 (1989).