MASSIVE COMPUTATION AS A PROBLEM SOLVING TOOL

MIODRAG ŽIVKOVIĆ

Abstract. We consider some problems, the solution of which requires a massive computation. One of them is the question: are there infinitely many primes of the form $\sum_{i=1}^{n}(-1)^{n-i}i!$? Another interesting problem is to determine the set of absolute values of $(0,1)$ determinants of order n, for n as large as possible. The question is answered for $n \leq 8$.

There are many simply formulated questions, that can be answered only by a very hard computation. Here we consider the two such problems. The first group of questions concerns testing hypotheses about factorial sums, among which is the Kurepa hypothesis on left factorials. We are also interested in finding the set of determinant absolute values of $(0,1)$ matrices of order n — for n as large, as possible. There is some difference between these two problems. The first of them requires a small memory, but the computation is time consuming. The solving process of the second problem requires both the large memory, and the long computation time; one is forced to make some trade-off while advancing towards its (partial) solution.

1. Left factorial hypotheses

1.1. **Problem formulation.** Let N and P denote the set of positive integers and the set of prime numbers, respectively. For integers m, n let (m,n) denote their greatest common divisor, and let $m \bmod n$ denote the remainder from division of m by n. The fact that m divides (does not divide) n is written as $m \mid n$ ($m \nmid n$). For $n \geq 1$ let

$$A_{n+1} = \sum_{i=1}^{n}(-1)^{n-i}i!$$

and let

$$!n = \sum_{i=1}^{n-1} i!$$

(left factorial function defined by Kurepa [17]). The following table lists a few first members of these sequences.

n	1	2	3	4	5	6	7	8	9	10
$n!$	1	2	6	24	120	720	5040	40320	362880	3628800
$!n$	1	2	4	10	34	154	874	5914	46234	409114
A_n		1	1	5	19	101	619	4421	35899	326981

Here we consider (see [25]) the following three questions from [11]: is it true that

(1) $$a_p := A_p \bmod p \neq 0 \text{ for all } p \in P?$$

(this question is raised in connection to [11, Problem B43]: is it true that there are infinitely many prime numbers among A_n, $n \in N$?),

$$r_p := !p \bmod p \neq 0 \text{ for all } p \in P, \quad p > 2? \tag{2}$$

([11, Problem B44]; an equivalent of the Kurepa hypothesis [17]), and is it true that

$$\text{for all } n \in N, \quad n > 3, \qquad !n \text{ is squarefree} \tag{3}$$

(also in [11, Problem B44]; the second Kurepa hypothesis [17, 19]).

Wagstaff verified that (1) and (2) are true for $n < 46340$ and $n < 50000$, respectively. The calculations were extended by Mijajlović [19] ((2) for $p \leq 311009$), Gogić [10] ((1) and (2) for $p < 1000000$) and Malešević [18] ((2) for $p < 3000000$). Mijajlović [19] proved that if $n \in N$, $p \in P$ and $2 < p \leq 1223$, then $!n$ is not divisible by p^2. An overview of these questions is given in [15]. We now shortly present main results from [25] concerning these problems.

1.2. **Probabilistic model.** Using the assumptions about a_p and r_p, we see that (1) and (2) are related to the event

$$R_\infty = \bigcap_{p \in P} \{R_p \neq 0\}.$$

But according to Mertens's theorem (see [21, Theorem 3.1] for example)

$$\prod_{p \in P(2,x)} \left(1 - \frac{1}{p}\right) \simeq \frac{e^{-\gamma}}{\ln x} \quad \text{as } x \longrightarrow \infty,$$

where $P(a,b) = P \cap (a,b)$ and γ is Euler's constant, so $e^{-\gamma} \simeq 0.5615$. Therefore, $Pr(R_\infty) = 0$. More precisely, we have the following asymptotic relation

$$Pr\left(\bigcap_{p \in P(x,x^\alpha)} \{R_p \neq 0\}\right) \simeq \frac{1}{\alpha}, \quad \text{as } x \longrightarrow \infty.$$

This heuristic argument suggests that (1) and (2) are not true, and even more, that the number of counterexamples is infinite. The "probability" that there is a counterexample $p \in P(x, x^\alpha)$ to (1) or (2) is approximately $1 - 1/\alpha$. With the same probability of $1/2$, one counterexample to these claims might be expected in the intervals $(2^3, 2^6] = (8, 64)$, $(2^6, 2^{12}] = (64, 2048]$ and $(2^{12}, 2^{24}] = (2048, 16793216]$. The probability of finding counterexamples in $(2^n, 2^{n+1}]$ is approximately $1/(n+1)$. The complexity of the search for counterexample $\leq x$ by the obvious algorithm is $O(x^2/\ln x)$ [19], which makes it very difficult to check (1) or (2), if for example $p > 2^{24}$.

1.3. **The results of computation.** The search for values $p \in P$ satisfying $p \mid A_p$ was performed using a simple assembler routine for an Intel 80486 microcomputer (at 100MHz) calculating a_p. After approximately 130 hours it was found that $p \mid A_p$ for $p = p_1 = 3612703$. That fact gives a solution of [11, Problem B43], because for all $n \geq p_1$ we have $p_1 \mid A_n$, and so A_n is not prime if $n \geq p_1$.

The similar search for values $p \in P$ satisfying $p \mid\, !p$, approximately 600 hours long, ended without success. No counterexamples were found to (2) for $p < 2^{23}$.

Let a be an arbitrary integer. Consider now divisibilities from B44 of [11], i.e. the prime powers p^k $(k \geq 1)$ dividing $!n + a$ for all large n. For given $p \in P$ and $k \in N$ let

$$m(p,k) = \min\left\{i \in N \mid p^k \mid i!\right\}.$$

The number $m(p,k)$ is of course a multiple of p, and if $k \leq 3$ then $m(p,k) = (k - \delta_{p,2})p$. For all $n \geq m(p,k)$ we have

$$!n \equiv\ !m(p,k) \pmod{p^k}$$

Therefore, for all $n \geq m(p,k)$

$$p^k \mid\ !n + a \quad \text{iff} \quad p^k \mid\ !m(p,k) + a. \tag{4}$$

Especially, if $p > 2$ and $k \leq 3$ then for all $n \geq kp$

$$p^k \mid\ !n + a \quad \text{iff} \quad p^k \mid\ !(kp) + a. \tag{5}$$

The case $a = -1$ is considered by Mijajlović and Keller (B44 of [11]). Mijajlović noted that $3 \mid\ !n - 1$ for $n \geq 3$, $9 \mid\ !n - 1$ for $n \geq 6$, and $11 \mid\ !n - 1$ for $n \geq 11$ (by (5) this is the consequence of $3 \mid\ !3 - 1$, $3^2 \mid\ !6 - 1$ and $11 \mid\ !11 - 1$). Keller found no new divisibilities of $!n - 1$ for $n < 10^6$. From Table 1 it can be seen that 3 and 11 are the only primes $p < 2^{23}$ satisfying $r_p = 1$, and therefore dividing $!n - 1$ for all large n. In Table 2 the factorizations of $!n - 1$, $n \leq 42$, (obtained using [16]) are given. The consequence of $11^2 \nmid\ !(2 \times 11) - 1$ and $3^3 \nmid\ !(3 \times 3) - 1$ is that $11^2 \nmid\ !n - 1$ for $n \geq 22$ and $3^3 \nmid\ !n - 1$, for $n \geq 9$. We conclude that $p^k = 3^2$ is the only repeated factor of $!n - 1$ for all large n if $p < 2^{23}$.

The case $a = 0$ is somewhat simpler. Because $r_p \neq 0$ for all $p \in P(2, 2^{23})$, there is not any $p < 2^{23}$ such that $p \mid\ !n$ for all large n. The other cases $-10 < a < 10$ might be considered similarly using Table 1.

The other consequence of (4) is that if for the given prime power p^k, $k \geq 1$, we are looking for all $n \in N$ such that $p^k \mid\ !n + a$, then it is enough to check the values of $n \leq m(p,k)$. Let l be the smallest integer satisfying $p^l \nmid\ !m(p,l) + a$. If $l < k$ then it is enough to check if $p^k \mid\ !n + a$ for $n < m(p,l) \leq m(p,k)$ ($n < p$ if $l = 1$, which is most often the case). Otherwise, if $l \geq k$, then $p^k \mid\ !m(p,k) + a$ and so $p^k \mid\ !n + a$ for all $n \geq m(p,k)$. Some repeated factors of $!n - 1$ may be seen from Table 2: $3^4 \mid\ !8 - 1$, $11^2 \mid\ !13 - 1$, $11^2 \mid\ !21 - 1$ and $37^2 \mid\ !25 - 1$. By (5) there are no other numbers $!n - 1$ divisible by 3^3 or 11^2, because $3^3 \nmid\ !9 - 1$ and $11^2 \nmid\ !22 - 1$. In Table 3 the triads (p, n, r) are listed satisfying $r = !n \bmod p < 10$, $p \in P(2, 2^{20})$ and $n \leq 2p$, except those for which $!n < p$. We see that the only new solution of $p^2 \mid\ !n - 1$, $p < 2^{20}$, $n \in N$, is $41611^2 \mid\ !26144 - 1$. From Table 1 we see that $r_{41611} \neq 1$ and consequently $41611 \nmid\ !n - 1$ for $n \geq 41611$.

Table 3 contains a counterexample to (3): the relation $54503^2 \mid\ !26541$ shows that left factorials are not always squarefree. The existence of a counterexample also has a "probabilistic" explanation. Considering the values $!n \bmod p^2$, $1 \leq n \leq p$, as the independent realizations of R_{p^2}, the check of $!n \bmod p^2 \neq 0$, $1 \leq n \leq p$, for fixed $p \in P$ corresponds to the event T_p that p independent outcomes of R_{p^2} are all different from 0. Using the inequality

$$1 - \frac{1}{n} < \left(1 - \frac{1}{n^2}\right)^n < \left(1 - \frac{1}{n}\right) / \left(1 - \frac{1}{n^2}\right)$$

which can be easily proved, we conclude that

$$Pr(T_p) = (1 - 1/p^2)^p \simeq 1 - 1/p$$

for large p. It follows that (3) and (1) have the same asymptotic "counterexample densities".

Gallot [5] noted that the hypothesis (2) can be reformulated as follows: are there infinitely many primes among the numbers $!n/2$? He extended the computation of r_p to $p \leq 2^{26}$, but found no p, satisfying $r_p = 0$. Therefore, the hypothesis (2) is true for $p < 2^{26}$. Gallot found the interesting congruence $!11477429 \mod 11477429 = 9$.

2. The determinant absolute values of $(0,1)$ matrices

2.1. **Problem formulation.** The motivation and the starting point is the old problem (thanks to R. Dimitrić, who brought my attention to it; see [13, 1, 6]): what is the largest possible determinant value of determinant of a matrix from $\mathcal{A}_n$, the set of all $(0,1)$ matrices of order n? The consequence of the Hadamard inequality is that determinant of a ± 1 matrix of order n is at most $n^{n/2}$. An arbitrary $(0,1)$ matrix with determinant d can be transformed by elementary transformations into a ± 1 matrix of order $n+1$ with the determinant $2^n d$: by multiplying all rows by 2, then inserting a new first zero row, then inserting a new column of ones, and finally by subtracting the first column from all other columns. Therefore, the determinant of an arbitrary $(0,1)$ matrix of order n is $\leq (n+1)^{(n+1)/2}/2^n$. As these transformations are invertible, there is one-to-one correspondence between $(0,1)$ matrices of order n with the determinant absolute value d, and ± 1 matrices of order $n+1$ with the determinant absolute value $2^n d$. For $n = 4k-1$, if there exist an Hadamard matrix of order $n+1$ (a ± 1 matrix with the orthogonal row set) then this upper bound is attained. Sloane [22, Sequence A003432/M0720] lists the maximum determinants of $(0,1)$ matrices for $n \leq 13$. In the table below we give these values, together with the upper bounds from Hadamard inequality.

n	1	2	3	4	5	6	7	8	9	10	11	12	13
D_n	1	1	2	3	5	9	32	56	144	320	1458	3645	9477
A_n	1	1	2	3	6	14	32	76	195	521	1458	4248	12867

D-optimal designs are the matrices from $\mathcal{A}_n$, $n = 4k+2$, with the maximum determinant. Determinant of a $(0,1)$ matrix of order $n = 4k+1$ is bounded above by $\leq n((n-1)/2)^{((n-1)/2}$. The upper bound is attainable only if $2n = x^2 + y^2$ for some nonnegative integers x, y (see [7, 8, 9, 2, 20]). Cohn [3] gives an D-optimal design of order 102, and Gysin [12] has found D-optimal designs of order $14, 26, 38, 42, 62, 66, 74, 82, 86, 122, 146, 170, 182, 186, 226$.

Here we consider a somewhat more general problem. For a given integer n, as large as possible, we want to find the all possible determinant modules of matrices from $\mathcal{A}_n$. The simplest way to obtain such a result is to compute determinants of all 2^{n^2} matrices of order n. As the number of matrices grows very fast, it is reasonable to partition $\mathcal{A}_n$ into equivalence classes, so that the determinant module is constant inside a class. Williamson [24] used a similar idea while searching for matrices with a maximum determinant module. Craigen [4] also considers the range of the determinant function. He obtained that for $n = 7$ the range of determinant values is not a set of consecutive integers.

Let Ψ denote some set of elementary operations on matrices. For arbitrary two matrices A, B we say that they are ψ-equivalent if B can be obtained from A by applying finitely many elementary operations from Ψ. As the elementary operations are invertible, the set $\mathcal{A}_n$ is partitioned by the equivalence relation ψ into equivalence classes. The set $\mathcal{A}_n$ can be ordered lexicographically; for arbitrary two matrices $A, B \in \mathcal{A}_n$ we say that $A \le B$ if the sequence obtained by concatenating rows of A is less than or equal the corresponding sequence obtained from B. For an arbitrary $A \in \mathcal{A}_n$ let $\bar{A}^{\psi}$ denote the ψ equivalence class of A, and let A^{ψ} denote the ψ-canonical form of A, i.e. the smallest matrix in $\bar{A}^{\psi}$ — the representative of the class $\bar{A}^{\psi}$.

In what follows, we consider classes of elementary operations, preserving the matrix determinant absolute value (row/column permutations, transposition, addition of a row/column multiplied by an integer to another row/column). Then we consider possible approaches to classify matrices from $\mathcal{A}_n$, i.e. to obtain partition of $\mathcal{A}_n$ into equivalence classes, and to find the set of equivalence class representatives. The largest possible equivalence classes are the SNF-classes, the classes generated by all integer elementary operations preserving determinant module. The two matrices are SNF-equivalent if they have the same Smith normal form (SNF). Generally, a set of matrices from $\mathcal{A}_n$, having the same determinant absolute value, consists of a number of SNF classes. Here we succided in classifying matrices from $\mathcal{A}_n$, $n \le 7$. For $n = 8$ the set of possible determinant absolute values is obtained. Finally, for $n = 9$ the set of determinant absolute values is obtained, which is believed to be complete, or almost complete.

2.2. **Elementary operations and the equivalence classes.** The row permutation does not change the absolute value of the matrix determinant. Therefore, if we want to find the all possible values of determinant module, it is enough to consider only matrices with lexicographically increasing sequence of rows, which are in fact the representatives of the corresponding equivalence classes. We call these classes the RP-classes, and the corresponding representatives are the RP-representatives. The number of matrices, determinants of which have to be compared, is reduced to $\binom{2^n-1}{n}$, i.e. it is reduced approximately by a factor of $n!$. Using the appropriate precomputation, the computation of individual determinants can be reduced to only one addition. Symmetrically, we can consider CP-classes and CP-representatives, generated by column permutations.

If we want to further reduce the number of determinants to be compared, we can try to consider wider equivalence classes, generated simultaneously by row and column permutations. Let Π denote the set of all row/column permutations. The set Π defines the π-classes and the π-representatives of these classes. It is not hard to derive that the number $p_n = |\mathcal{A}/\pi|$ of π-classes in $\mathcal{A}_n$ equals

(6)
$$\sum_{i_1+2i_2+\ldots+ni_n=n} \sum_{j_1+2j_2+\ldots+nj_n=n} C(i_1, i_2, \ldots, i_n) C(j_1, j_2, \ldots, j_n) \exp_2 \sum_{r,s=1}^{n} i_r j_s 2^{(r,s)},$$

where $C(i_1, i_2, \ldots, i_n) = n!/(1^{i_1} i_1! \ldots n^{i_n} i_n!)$ is the number of permutations of order n with i_r cycles of length r, $r = 1, 2, \ldots, n$. Computation is similar to the enumeration of bipartite graphs, see [14]. In fact, an arbitrary π-class corresponds to exactly one bipartite graph with n black and n white nodes. Using (6), it is not hard to compute p_n for a quite large values of n, see Table 4; the table is prepared using UBASIC [23]. The value of p_n is asymptotically close to $2^{n^2}/(n!)^2$; Table 4 illustrates that fact. However, it is not simple to generate all π-representatives sequentially.

The π-neighbors of a given matrix A are the matrices, that can be obtained from A by an elementary operation $P_{1,j}$ — the exchange of the first and the jth column, followed by lexicographically sorting the rows. The possible way to obtain the set of π-representatives is based on generating the sorted list of RP-representatives in the class $\bar{A}^\pi$ for the given matrix $A \in \mathcal{A}_n$. The sorted list L_A of RP-representatives from $\bar{A}^\pi$ is formed by breadth-first search: the list of representatives is extended by adding the neighbors of the next member, until the list is exhausted. The list is maintained in a balanced binary search tree, and so it is obtained in a sorted form.

In order to obtain the set of π-representatives in $\mathcal{A}_n$, we start from the sorted list L of all RP-representatives of length $\binom{2^n-1}{n}$. The first matrix $A = 0$ from the list is obviously a π-representative. We then mark (in L) all matrices from L_A. The first non-marked member B of L is the following π-representative; then the matrices from L_B are marked in L, and so on, until all matrices in L are marked. At the end, the sorted list of π-representatives is obtained. This algorithm is constrained by the space requirement: it is feasible for at most $n = 6$.

We now describe briefly the branch-and-bound algorithm to obtain the π-representative A^π of the given matrix A. Idea is to maximize lexicographically the ith row, $i = 1, 2, \dots, n$, by sequentially putting all remaining rows (by row exchange) in the place of ith row, and permuting accordingly the columns (branch); if the value of the ith row obtained is less than the best found so far, the variant is abandoned (bound). In the average, this algorithm is efficient; but if matrix A is highly symmetric (the unity matrix, for example), then the search tree cutting occurs very rarely, and the complexity, measured by row interchanges, approaches $n!$. Still, this algorithm is important, because it makes it possible to deal with π-representatives only.

The other approach to obtain the set of π-representatives, requiring less memory, but more time, uses the algorithm to find the π-representative A^π of the given matrix A. The RP-representatives are considered sequentially. The algorithm to find the π-representative is started for each RP-representative A. If the matrix $B < A$ is found during the search, the search is aborted and A is thrown away; otherwise RP-representative is at the same time the π-representative, and its determinant is computed.

Consider now the transformation XOR_i of $A = [a_{ij}] \in \mathcal{A}_n$: the row i is XOR-ed (added modulo 2) to all other rows of A, remaining itself unchanged. In other words, for each $j = 1, 2, \dots, n$, if $a_{ij} = 1$, then the element a_{kj} is replaced by $1 - a_{kj}$ for all $k \neq i$; the other elements of A are left unchanged. Williams [24] observed, by considering the corresponding ± 1 matrix of order $n+1$, that this operation does not change the determinant absolute value of a $(0, 1)$ matrix. There is another way to express this operation as the sequence of elementary operations:

(1) ith row is subtracted from all other rows; in the matrix obtained, the elements in columns corresponding to ones in the ith row, belong to the set $\{-1, 0\}$;
(2) the columns corresponding to ones in the ith row are multiplied by -1;
(3) the ith row is multiplied by -1.

Strictly speaking, row XOR is not an elementary row operation. Still, this operation is a composition of elementary operations, and preserves the determinant absolute value of a matrix. Similarly, the XORing of the jth column to all other columns can be considered. Denote by Ξ the set of all row/column permutations and the row/column XOR-s. These operations correspond to a relation on the set $\mathcal{A}_n$. The corresponding transitive closure, the equivalence relation ξ, defines the partition of $\mathcal{A}_n$. The composition of two row/column XOR-s is always equivalent to a single row/column XOR operation. Therefore, each class $\bar{A}^\xi$ consists of at most $(n+1)^2$ smaller classes $\bar{A}^\pi$. In other words, each class $\bar{A}^\xi$ contains at most $(n+1)^2$ π-representatives.

Consider next the elementary operation SUB_{ij}, denoting the replacement of the jth row by the row obtained by subtraction of ith row from the jth row. The operation SUB_{ij}, applied to the matrix $A \in \mathcal{A}_n$, gives the matrix from the same set, iff the set of ones in the row i is the subset of the set of ones in the row j (i.e. each element of the ith row is $\leq$ than the corresponding element in the jth row; or shortly: if the ith row is the subset of the jth row). The SUB operation on columns is analogously defined. We suppose that the SUB operation is allowed only if the result is inside $\mathcal{A}_n$; the SUB-neighbors of a given matrix $A \in \mathcal{A}_n$ are all matrices that can be obtained applying a row/column SUB operation to A.

It seems that, in order to have a complete set of linear operations on matrices, one must also consider the operation ADD_{ij}, the addition of ith row/column to jth row/column, under the condition that all elements of the row/column sum are ≤ 1. However, the row operation ADD_{ij} is equivalent to the sequence of tree operations: XOR_i, SUB_{ij}, XOR_i, and so it is unnecessary to consider that operation — the transitive closure remains the same.

Denote by Σ the set of all row/column permutations, and the row/column XOR-s, and the row/column SUB-s. These operations correspond to a relation on $\mathcal{A}_n$. The corresponding transitive closure, the equivalence relation σ, defines the partition of $\mathcal{A}_n$. Unlike the class $\bar{A}^\xi$, which consists of at most $(n+1)^2$ π-representatives, the number of ξ-representatives in a single class $\bar{A}^\sigma$ is not bounded by any such simple almost uniform bound.

The largest possible equivalence classes are the SNF-classes, the classes generated by all integer elementary operations preserving determinant module. If all integer elementary operations are allowed (except multiplying a row/column by an integer different from ± 1), then there are matrices $A \in \mathcal{A}_n$, that can be transformed into a matrix outside $\mathcal{A}_n$. Using such elementary operations, an arbitrary integer matrix can be transformed into its canonical form (the SNF) — a diagonal matrix, such that each diagonal element is a nonnegative integer, dividing the all remaining diagonal elements. Therefore, for arbitrary two matrices $A, B \in \mathcal{A}_n$ we say that they are SNF-equivalent if they have the same SNF. The relation of SNF-equivalence defines SNF-classes in $\mathcal{A}_n$. In the general case the set of matrices from $\mathcal{A}_n$ with the fixed determinant absolute value, consists of one or more SNF-classes. For example, the two SNF-classes in $\mathcal{A}_5$ with the representatives $(03, 05, 09, 11, 1E)$ and $(03, 0C, 15, 16, 19)$ (the rows of these matrices are represented by hexadecimal numbers) have the equal determinant absolute value 4, but their SNF's $\operatorname{diag}(1, 1, 1, 1, 4)$ and $\operatorname{diag}(1, 1, 1, 2, 2)$ are different.

Unlike the other equivalence classes, the SNF classes cannot be constructed in a usual manner, by a depth-first search, starting from an arbitrary member.

2.3. **Iterative classification of** $(0, 1)$ **matrices.** By bordering of a matrix $A \in \mathcal{A}_n$ we mean the construction of all matrices $B \in \mathcal{A}_{n+1}$, such that the lower left $n \times n$ block in B is equal to A. In other words, all possible matrices obtained by bordering A from the left and upper side by $2n+1$ elements from $\{0,1\}$ are generated.

Williamson [24] observed the following useful fact. If the matrices $A, B \in \mathcal{A}_n$ are ξ-equivalent (i.e. $A^\xi = B^\xi$), then the set of ξ-representatives of matrices obtained by bordering A is equal to the the set of ξ-representatives of matrices obtained by bordering B. More precisely, if A' is the ξ-representative of an arbitrary matrix obtained by bordering A, then there exists a matrix B', the ξ-representative of some matrix obtained by bordering B, such that $A' = B'$. Indeed, from $A^\xi = B^\xi$ it follows that there exists a sequence of row/column permutations/XOR's, that transforms A into B. The same sequence of transformations, applied to the last n rows and columns of A', transforms it into a matrix $C \in \mathcal{A}_{n+1}$, whose lower right $n \times n$ block is B. We can take the matrix C as the matrix B'.

Using that observation, we conclude that if we search for all ξ-representatives of order $n+1$, then it is enough to consider matrices, obtained by bordering all ξ-representatives of order n. The task could be divided in two phases. The first part is to find π-representatives of all matrices obtained by bordering the set of ξ-representatives of order n. This is less time consuming, than finding the ξ-representatives. Then the list of π-representatives is filtered. For each matrix A from the list, the class $\bar{A}^\xi$ (as the collection of π-representatives) and the representative A^ξ is found, and then all π-representatives from $\bar{A}^\xi$ are eliminated from the list. As the size of ξ-classes is bounded, the number of ξ-representativves grows fast with n. But for $n = 7$ the classes fitted in the memory of a PC, and the complete set of ξ-representatives is obtained. The sets of ξ-representatives are checked by summing the numbers of π-representatives in each ξ-class. The figures obtained agree completely with the values given in Table 4.

The following task was to classify the ξ-representatives into σ- and SNF-classes. The ξ-representatives were classified first according to SNF, by computing the SNF of each representative. Then, the each sorted group L of representatives with the same SNF is treated separately. The main loop of the procedure is to take from L the next ξ-representative (and therefore the σ-representative), the matrix A, then to traverse its class $\bar{A}^\sigma$ (considering only the π-representatives of its elements), and to eliminate the elements of L contained in $\bar{A}^\sigma$. The problem arises if the number of π-representatives in $\bar{A}^\sigma$ is very large. For example, the class $\bar{A}^\sigma$ of $A = (00, 01, 02, 04, 08, 10, 20)$ contains 13834240 π-representatives.

The final task was to obtain some information about $\mathcal{A}_8$ and $\mathcal{A}_9$. The determinants of all matrices obtained by bordering given matrix $A \in \mathcal{A}_n$ can be computed very efficiently using the cofactors of A. Using that procedure, determinants of all matrices obtained by bordering ξ-representatives in $\mathcal{A}_7$ were computed. Procedure to find SNF's of matrices obtained by bordering A is more complicated. That procedure is applied only to σ-representatives in $\mathcal{A}_7$. Therefore the set of different SNF's of order 8 might not be complete. In Table 5 the number 129, the lower bound for the number of different SNF's of order 8, is therefore marked by an asterisk. The set of determinant absolute values in $\mathcal{A}_9$ is also estimated from below, by doubly bordering all ξ-representatives in $\mathcal{A}_7$, and by computing determinants of all obtained matrices of order 9.

The results are summarized in Table 5. For $n = 1, 2, \ldots$ let p_n, q_n, r_n, s_n, d_n denote the number of π-, ξ-, σ-, SNF- representatives and the number of different determinant absolute values in $\mathcal{A}_n$, respectively. The smallest n for which there exist a SNF class, consisting of more than one σ-class, is 5. In Table 6 the complete list of σ-representatives in $\mathcal{A}_n$ is given for $n \leq 7$. The representatives are given by hexadecimaly coded rows. For each representative the diagonal elements of its SNF are given.

References

1. J. Brenner, L. Cummings, *The Hadamard maximum determinant problem*, Amer. Math. Monthly **79** (1972) 626-630
2. J. H. E. Cohn, *On determinants with elements* ± 1. *II*, Bull. Lond. Math. Soc. **21**, No.1, 36-42 (1989).
3. J. H. E. Cohn, *A D-optimal design of order* 102, Discrete Mathematics **102** (1992), 61-65
4. R. Craigen, *The range of the determinant function on the set of* $n \times n$ $(0,1)$*-matrices*, J.-Combin.-Math.-Combin.-Comput. **8** (1990), 161–171.
5. http://perso.wanadoo.fr/yves.gallot/papers/index.html.
6. R. Damboianu, V. Draghici, *Maximal values in a special class of determinants*, Proceedings of the Algebra Conference (Brasov, 1988), 89–94
7. H. Ehrlich, K. Zeller, *Binaere Matrizen*, Z. angew. Math. Mechanik **42**, T20-21, 1962.
8. H. Ehlich, *Determinantenabschaetzungen fuer binaere Matrizen*, Math. Z. **83**, 123-132 (1964)
9. H. Ehlich, *Determinantenabschaetzung fuer binaere Matrizen mit* $n \equiv 3 \mod 4$ Math. Z. **84**, 438-447 (1964).
10. G. Gogić, *Parallel algorithms in arithmetic*, Master thesis, Belgrade University, 1991.
11. R. Guy, *Unsolved problems in number theory*, Second Edition, Springer–Verlag, 1994.
12. M. Gysin, *New D-optimal designs via cyclotomy and generalised cyclotomy*, Australas. J. Comb. **15**, 247-255 (1997).
13. J. Hadamard, *Resolution d'une question relative aux determinants*, Bull. Sci. Math. **17**, 30-31, 1893.
14. F. Harary, E. M. Palmer, *Graphical Enumeration*, Academic Press, New York, 1973.
15. A. Ivić, Ž. Mijajlović, *On Kurepa's problems in number theory*, Publ. Inst. Math. (Beograd) (N. S.), **57(71)**, 1995, 19–28
16. Y. Kida, *ECMX, Prime Factorization by ECM*, UBASIC program, 1987–1990.
17. Dj. Kurepa, *On the left factorial function*, Math. Balkanica, **1**, 1971, 147–153
18. B. Malešević, *Personal communication*
19. Ž. Mijajlović, *On some formulas involving* $!n$ *and the verification of the* $!n$ *hypothesis by use of computers*, Publ. Inst. Math. (Beograd), **47**(61), 1990, 24–32
20. M. G. Neubauer, A. J. Radcliffe, *The maximum determinant of* ± 1 *matrices*, Linear Algebra Appl. **257**, 289-306 (1997).
21. H. Riesel, *Prime numbers and computer methods for factorization*, Birkhauser, Boston, 1985.
22. N. J. A. Sloane, *An On-Line Version of the Encyclopedia of Integer Sequences*, http://www.research.att.com/ njas/sequences/eisonline.html
23. *UBASIC*, version 8.74, 1994.
24. J. Williamson, *Determinants whose elements are* 0 *and* 1, Amer. Math. Monthly **53**(1946), 427-434
25. M. Živković, *The number of primes* $\sum_{i=1}^{n}(-1)^{n-i}i!$ *is finite*, Mathematics of Computation, **68**, No. 225, Jan. 1999, 403-409.

Matematički Fakultet, Beograd, Studentski trg 16
E-mail address: `ezivkovm@matf.bg.ac.yu`

TABLE 1. The values of a_p, $p < 2^{22}$, and r_p, $p < 2^{23}$, close to 0 or p

p	a_p	p	$p - a_p$	p	r_p	p	$p - r_p$
2	1	2	1	2	0		
3	1	3	2	3	1	3	2
5	4	5	1	5	4	5	1
7	3	7	4	7	6	7	1
11	4	11	7	11	1	13	3
17	8	13	1	19	9	17	4
31	9	17	9	31	2	23	2
41	1	19	5	37	5	67	2
43	5	23	5	41	4	71	3
47	6	37	1	163	4	113	4
67	5	71	7	197	9	139	5
79	4	109	5	277	7	227	2
157	6	131	3	373	2	349	6
191	6	197	2	467	3	2437	5
307	5	229	9	7717	7	4337	5
641	3	367	4	11813	6	10331	2
647	5	463	1	33703	9	77687	3
1109	2	691	2	2275843	3	126323	8
2741	3	983	3	3467171	5	274453	1
3559	3	1439	2			4709681	9
394249	1	11119	3				
2934901	1	16007	4				
3612703	0	22619	3				
		32833	6				
		3515839	2				

TABLE 2. The factorizations of $!n - 1$, $n \leq 42$.

n	The factorization of $!n - 1$
3	3
4	3^2
5	3×11
6	$3^2 \times 17$
7	$3^2 \times 97$
8	$3^4 \times 73$
9	$3^2 \times 11 \times 467$
10	$3^2 \times 131 \times 347$
11	$3^2 \times 11 \times 40787$
12	$3^2 \times 11 \times 443987$
13	$3^2 \times 11^2 \times 23 \times 20879$
14	$3^2 \times 11 \times 821 \times 83047$
15	$3^2 \times 11 \times 2789 \times 340183$
16	$3^2 \times 11 \times 107 \times 509 \times 259949$
17	$3^2 \times 11 \times 225498914387$
18	$3^2 \times 11 \times 163 \times 20143 \times 1162943$
19	$3^2 \times 11 \times 19727 \times 3471827581$
20	$3^2 \times 11 \times 29 \times 43 \times 1621 \times 641751001$

TABLE 3. Continued

n	The factorization of $!n-1$
21	$3^2 \times 11^2 \times 53 \times 67 \times 662348503367$
22	$3^2 \times 11 \times 877 \times 3203 \times 41051 \times 4699727$
23	$3^2 \times 11 \times 1189548482266089 8387$
24	$3^2 \times 11 \times 139 \times 2129333 \times 922459185301$
25	$3^2 \times 11 \times 37^2 \times 29131483 \times 163992440081$
26	$3^2 \times 11 \times 454823 \times 519472957 \times 690821017$
27	$3^2 \times 11 \times 107 \times 173 \times 7823 \times 12227 \times 1281439 \times 1867343$
28	$3^2 \times 11 \times 431363 \times 2882477797 \times 91865833117$
29	$3^2 \times 11 \times 191 \times 47793258077 \times 349882390108241$
30	$3^2 \times 11 \times 37 \times 283 \times 5087 \times 1736655143086866180331$
31	$3^2 \times 11 \times 277182644919335489100710889 8387$
32	$3^2 \times 11 \times 1231547 \times 306730217 \times 227214279676815713$
33	$3^2 \times 11 \times 41 \times 163 \times 224677 \times 278437 \times 6562698554476756561$
34	$3^2 \times 11 \times 109 \times 839 \times 2819 \times 40597679 \times 8642572321688037037$
35	$3^2 \times 11 \times 30726034822709330195783430032688 98387$
36	$3^2 \times 11 \times 7523968684626643 \times 14280739323850758510209$
37	$3^2 \times 11 \times 542410073 \times 71255243574341086719465256590 19$
38	$3^2 \times 11 \times 379 \times 2677 \times 5685998930867 \times 247694227623686689665 67$
39	$3^2 \times 11 \times 127 \times 338944799 \times 1260500588720209796289828102408 19$
40	$3^2 \times 11 \times 956042657 \times 22118799919684374721083871186756 3891$
41	$3^2 \times 11 \times 845303368010419703225497617317228174246889 8387$
42	$3^2 \times 11 \times 1652359939 \times 276306566079013 \times 7586274213949066873557 41$

TABLE 3. The small values of $!n \bmod p^2 < 10$, for $p \in P$, $p < 2^{20}$, $1 \le n \le 2p$

p	n	$!n \bmod p^2$	p	n	$!n \bmod p^2$
2	3	0	83	60	5
2	4	2	163	183	4
3	4	1	163	273	4
3	5	7	173	152	3
3	6	1	197	355	9
5	5	9	373	185	6
5	6	4	373	514	2
5	9	9	467	730	3
7	6	7	467	902	3
11	13	1	3119	306	6
11	21	1	4357	837	7
17	7	7	7717	9402	7
17	11	6	7717	15415	7
19	17	9	8297	4727	7
19	20	9	33703	39795	9
37	25	1	33703	43801	9
37	63	5	33703	52337	9
41	55	4	41611	26144	1
43	9	9	54503	26541	0
47	19	8	302837	283148	8
59	41	9	351731	135646	8
67	29	8			

TABLE 4. The number p_n of π-classes in $\mathcal{A}_n$ for $n \leq 17$

n	$p_n/(2^{n^2}/n!^2)$	p_n
1	1.0000000000	2
2	1.7500000000	7
3	2.5312500000	36
4	2.7861328125	317
5	2.4135589600	5624
6	1.8980735913	251610
7	1.5180343955	33642660
8	1.2942373440	14685630688
9	1.1691457540	21467043671008
10	1.0983637472	105735224248507784
11	1.0574704398	1764356230257807614296
12	1.0335474282	100455994644460412263071692
13	1.0194975307	19674097197480928600253198363072
14	1.0112617871	13363679231028322645152300040033513414
15	1.0064595112	31735555932041230032311939400670284689732948
16	1.0036786649	265481580762520930072845197261091304921260990676802
17	1.0020805061	7878332940506569588782402627237881550737859569467984886964

TABLE 5. The equivalence classes sizes, and the determinant absolute value ranges

n	p_n	q_n	r_n	s_n	d_n	det. abs. val. range
1	2	2	2	2	2	$0-1$
2	7	3	3	3	2	$0-1$
3	36	12	5	5	3	$0-2$
4	317	39	8	8	4	$0-3$
5	5624	388	15	14	6	$0-5$
6	251610	8102	30	26	10	$0-9$
7	33642660	656103	81	56	22	$0-18, 20, 24, 32$
8	14685630688			^{*129}	46	$0-40, 42, 44, 45, 48, 56$
9	21467043671008				^{*114}	$0-102, 104, 105, 108, 110, 112,$ $116, 117, 120, 125, 128, 144$

TABLE 6. Classification of $(0,1)$ matrices of order $n \leq 7$

n	SNF							det	ξ-size	π-size	the σ-representative					
2	1	0	0					0	1	1	0	0				
	2	1	0					0	1	4	0	1				
	3	1	1					1	1	2	1	2				
3	1	0	0	0				0	1	1	0	0	0			
	2	1	0	0				0	4	9	0	0	1			
	3	1	1	0				0	4	18	0	1	2			
	4	1	1	1				1	2	7	1	2	4			
	5	1	1	2				2	1	1	3	5	6			
4	1	0	0	0	0			0	1	1	0	0	0	0		
	2	1	0	0	0			0	4	16	0	0	0	1		
	3	1	1	0	0			0	12	84	0	0	1	2		
	4	1	1	1	0			0	14	150	0	1	2	4		
	5	1	1	2	0			0	1	5	0	3	5	6		
	6	1	1	1	1			1	5	49	1	2	4	8		
	7	1	1	1	2			2	1	10	1	6	A	C		
	8	1	1	1	3			3	1	2	3	5	9	E		
5	1	0	0	0	0	0		0	1	1	0	0	0	0	0	
	2	1	0	0	0	0		0	9	25	0	0	0	0	1	
	3	1	1	0	0	0		0	37	260	0	0	0	1	2	
	4	1	1	1	0	0		0	113	1346	0	0	1	2	4	
	5	1	1	2	0	0		0	5	25	0	0	3	5	6	
	6	1	1	1	1	0		0	141	2589	0	1	2	4	8	
	7	1	1	1	2	0		0	17	210	0	1	6	A	C	
	8	1	1	1	3	0		0	2	15	0	3	5	9	E	
	9	1	1	1	1	1		1	39	831	1	2	4	8	10	
	10	1	1	1	1	2		2	15	254	1	2	C	14	18	
	11	1	1	1	1	3		3	5	51	1	6	A	12	1C	
	12	1	1	1	1	4		4	1	2	3	5	9	11	1E	
									1	10	3	5	A	16	19	
	13	1	1	1	1	5		5	1	3	3	5	E	16	19	
	14	1	1	1	2	2		4	1	2	3	C	15	16	19	
6	1	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0
	2	1	0	0	0	0	0	0	9	36	0	0	0	0	0	1
	3	1	1	0	0	0	0	0	76	660	0	0	0	0	1	2
	4	1	1	1	0	0	0	0	472	7586	0	0	0	1	2	4
	5	1	1	2	0	0	0	0	10	86	0	0	0	3	5	6
	6	1	1	1	1	0	0	0	1913	47605	0	0	1	2	4	8
	7	1	1	1	2	0	0	0	115	2120	0	0	1	6	A	C
	8	1	1	1	3	0	0	0	9	91	0	0	3	5	9	E
	9	1	1	1	1	1	0	0	3262	112080	0	1	2	4	8	10
	10	1	1	1	1	2	0	0	511	14986	0	1	2	C	14	18
	11	1	1	1	1	3	0	0	75	1618	0	1	6	A	12	1C
	12	1	1	1	1	4	0	0	2	15	0	3	5	9	11	1E
									14	292	0	3	5	A	16	19
	13	1	1	1	1	5	0	0	3	46	0	3	5	E	16	19
	14	1	1	1	2	2	0	0	4	78	0	3	C	15	16	19
	15	1	1	1	1	1	1	1	952	39637	1	2	4	8	10	20

Table 6. Continued

n		SNF							det	ξ-size	π-size	the σ-representative						
	16	1	1	1	1	1	2		2	442	17642	1	2	4	18	28	30	
	17	1	1	1	1	1	3		3	128	4079	1	2	C	14	24	38	
	18	1	1	1	1	1	4		4	52	1685	1	6	A	12	22	3C	
	19	1	1	1	1	1	5		5	17	427	1	6	A	1C	2C	32	
										1	2	3	5	9	11	21	3E	
	20	1	1	1	1	2	2		4	17	473	1	6	18	2A	2C	32	
	21	1	1	1	1	1	6		6	9	263	3	5	9	16	2E	31	
	22	1	1	1	1	1	7		7	1	6	3	5	9	1E	2E	31	
										2	48	3	5	E	18	29	36	
	23	1	1	1	1	1	8		8	1	6	3	5	E	19	29	36	
										1	21	3	C	15	1A	26	39	
	24	1	1	1	1	2	4		8	1	12	3	C	15	1A	26	29	
	25	1	1	1	1	1	9		9	1	7	3	D	15	1A	26	39	
	26	1	1	1	2	2	2		8	1	2	7	19	1E	2A	2D	33	
7	1	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0
	2	1	0	0	0	0	0	0	0	16	49	0	0	0	0	0	0	1
	3	1	1	0	0	0	0	0	0	170	1428	0	0	0	0	0	1	2
	4	1	1	1	0	0	0	0	0	1908	31994	0	0	0	0	1	2	4
	5	1	1	2	0	0	0	0	0	34	246	0	0	0	0	3	5	6
	6	1	1	1	1	0	0	0	0	17596	501563	0	0	0	1	2	4	8
	7	1	1	1	2	0	0	0	0	694	13645	0	0	0	1	6	A	C
	8	1	1	1	3	0	0	0	0	30	400	0	0	0	3	5	9	E
	9	1	1	1	1	1	0	0	0	105808	4358421	0	0	1	2	4	8	10
	10	1	1	1	1	2	0	0	0	9295	316904	0	0	1	2	C	14	18
	11	1	1	1	1	3	0	0	0	853	22902	0	0	1	6	A	12	1C
	12	1	1	1	1	4	0	0	0	9	92	0	0	3	5	9	11	1E
										159	3622	0	0	3	5	A	16	19
	13	1	1	1	1	5	0	0	0	23	413	0	0	3	5	E	16	19
	14	1	1	1	2	2	0	0	0	58	1032	0	0	3	C	15	16	19
	15	1	1	1	1	1	1	0	0	261882	13834240	0	1	2	4	8	10	20
	16	1	1	1	1	1	2	0	0	53874	2624469	0	1	2	4	18	28	30
	17	1	1	1	1	1	3	0	0	8633	376699	0	1	2	C	14	24	38
	18	1	1	1	1	1	4	0	0	3024	123510	0	1	6	A	12	22	3C
	19	1	1	1	1	1	5	0	0	631	23474	0	1	6	A	1C	2C	32
										2	15	0	3	5	9	11	21	3E
	20	1	1	1	1	2	2	0	0	927	37489	0	1	6	18	2A	2C	32
	21	1	1	1	1	1	6	0	0	361	13823	0	3	5	9	16	2E	31
	22	1	1	1	1	1	7	0	0	6	93	0	3	5	9	1E	2E	31
										58	2040	0	3	5	E	18	29	36
	23	1	1	1	1	1	8	0	0	6	113	0	3	5	E	19	29	36
										19	415	0	3	C	15	1A	26	39
	24	1	1	1	1	2	4	0	0	27	893	0	3	C	15	1A	26	29
	25	1	1	1	1	1	9	0	0	7	189	0	3	D	15	1A	26	39
	26	1	1	1	2	2	2	0	0	2	25	0	7	19	1E	2A	2D	33
										1	2	0	F	33	3C	55	5A	66
	27	1	1	1	1	1	1	1	1	91764	5593528	1	2	4	8	10	20	40
	28	1	1	1	1	1	1	2	2	58179	3493129	1	2	4	8	30	50	60

Table 6. Continued

n	SNF								det	ξ-size	π-size	the σ-representative						
	29	1	1	1	1	1	1	3	3	17707	1020752	1	2	4	18	28	48	70
	30	1	1	1	1	1	1	4	4	10189	581948	1	2	C	14	24	44	78
	31	1	1	1	1	1	1	5	5	3169	172714	1	2	C	14	38	58	64
	32	1	1	1	1	1	2	2	4	3220	184475	1	2	C	30	54	58	64
	33	1	1	1	1	1	1	6	6	3319	185686	1	6	A	12	2C	5C	62
										1	2	3	5	9	11	21	41	7E
	34	1	1	1	1	1	1	7	7	749	39068	1	6	A	12	3C	5C	62
	35	1	1	1	1	1	1	8	8	645	32490	1	6	A	1C	32	52	6C
	36	1	1	1	1	1	2	4	8	317	15119	1	6	18	2A	34	4C	52
	37	1	1	1	1	1	1	9	9	252	12603	1	6	1A	2A	34	4C	72
										1	6	3	5	9	11	3E	5E	61
	38	1	1	1	1	2	2	2	8	29	750	1	E	32	3C	54	5A	66
	39	1	1	1	1	1	1	10	10	1	3	3	5	9	1E	2E	4E	71
										198	10091	3	5	9	1E	30	51	6E
	40	1	1	1	1	1	1	11	11	1	11	3	5	9	1E	31	51	6E
										54	2587	3	5	E	16	38	59	66
	41	1	1	1	1	1	1	12	12	1	7	3	5	E	16	39	59	66
										69	3235	3	5	E	19	32	56	69
										1	21	3	5	19	2E	36	4E	61
	42	1	1	1	1	1	1	13	13	1	9	3	5	E	19	36	56	69
										15	658	3	5	18	29	36	4E	71
										1	19	3	5	19	29	3E	4E	71
	43	1	1	1	1	1	3	3	9	37	1358	3	5	18	28	49	4E	71
	44	1	1	1	1	1	2	6	12	1	21	3	5	19	29	36	4E	51
										26	962	3	5	19	2A	36	4E	61
										1	14	3	D	31	3E	55	5A	66
	45	1	1	1	1	1	1	14	14	1	19	3	5	19	29	36	4E	71
										9	496	3	C	15	26	39	5A	65
										2	100	3	D	15	26	38	5A	61
	46	1	1	1	1	1	1	16	16	1	30	3	C	15	36	39	5A	65
										3	62	3	D	16	2A	31	58	65
										1	21	3	D	16	2A	35	59	66
	47	1	1	1	1	2	2	4	16	2	10	3	C	30	55	5A	66	69
	48	1	1	1	1	1	2	8	16	5	89	3	C	31	55	5A	66	69
										1	13	3	D	31	55	5A	66	69
	49	1	1	1	1	1	4	4	16	1	6	3	C	35	3A	55	66	69
										1	7	3	D	16	2A	31	59	66
	50	1	1	1	1	1	1	15	15	3	59	3	D	15	26	38	5E	61
										1	28	3	D	15	26	39	5A	65
										2	128	3	D	16	2A	35	58	66
	51	1	1	1	1	1	1	17	17	1	19	3	D	16	2E	39	5A	65
										1	8	7	19	2A	35	4C	69	72
	52	1	1	1	1	1	3	6	18	1	2	3	1D	2D	36	3A	4E	71
										1	8	7	19	2A	34	4D	56	63
	53	1	1	1	1	2	2	6	24	1	5	7	19	2A	34	4C	52	61
	54	1	1	1	1	1	2	10	20	1	10	7	19	2A	34	4C	52	63
	55	1	1	1	1	1	1	18	18	1	24	7	19	2A	34	4C	53	65
	56	1	1	1	2	2	2	4	32	1	1	F	33	3C	55	5A	66	69