UDC 519.61:511-33
doi:10.31799/1684-8853-2020-2-2-9

Articles

Prime Fermat numbers and maximum determinant matrix conjecture

N. A. Balonin[a]**,** *Dr. Sc., Tech., Professor, orcid.org/0000-0001-7338-4920, korbendfs@mail.ru*
M. B. Sergeev[a]**,** *Dr. Sc., Tech., Professor, orcid.org/0000-0002-3845-9277*
A. A. Vostricov[a]**,** *PhD, Tech., Associate Professor, orcid.org/0000-0002-8513-368*
[a]*Saint-Petersburg State University of Aerospace Instrumentation, 67, B. Morskaya St., 190000, Saint-Petersburg, Russian Federation*

Purpose: *Solution to the problem of optimizing the determinants of matrices with a modulus of entries < 1. Developing a theory of such matrices based on preliminary research results.* ***Methods:*** *Extreme solutions (in terms of the determinant) are found by minimizing the absolute values of orthogonal matrix elements, and their subsequent classification.* ***Results:*** *Matrices of orders equal to prime Fermat numbers have been found. They are special, as their absolute determinant maximums can be reached on a simple structure. We provide a precise evaluation of the determinant maximum for these matrices and formulate a conjecture about it. We discuss the close relation between the solutions of extremal problems with the limitation on the matrix column orthogonality and without it. It has been shown that relative maximums of orthogonality-limited matrix determinants correspond to absolute maximums of orthogonality-unlimited matrix determinants. We also discuss the ways to build extremal matrix families for the orders equal to Mersenne numbers.* ***Practical relevance:*** *Maximum determinant matrices are used extensively in the problems of error-free coding, compression and masking of video information. Programs for maximum determinant matrix search and a library of constructed matrices are used in the mathematical network "mathscinet.ru" along with executable online algorithms.*

Keywords *— determinant, determinant maximum, quasi-orthogonal matrices, Hadamard matrices, Mersenne matrices, Fermat matrices, Cretan matrices.*

For citation: Balonin N. A., Sergeev M. B., Vostricov A. A. Prime Fermat numbers and maximum determinant matrix conjecture. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2020, no. 2, pp. 2–9. doi:10.31799/1684-8853-2020-2-2-9

Introduction

Determinant optimization of matrices with modulus of entries ≤ 1 is a very difficult problem [1–4] without an universal algorithm for its solution. The first computer experiments were started in 1962 [5]; the further evolution of this subject has been discussed in [6–9] with algorithmic backgrounds [10–13], specific orders [14, 15] and websites [16, 17].

There are methods based on the interrelation between optimal solutions for various matrix classes [18]. For example, the determinant optimization method for orthogonal column matrices proposed in our paper [19] allows us to find, in particular, non-orthogonal matrices with an absolute determinant maximum (**D**-optimal matrices or **D**-matrices, in short) [20–23]. The key point here is that local and absolute extremums of determinants for these matrix types are interrelated [24].

Our vast experience in matrix determinant optimization allows us to make certain conclusions which lead us to a conjecture about maximum determinant matrices of orders equal to prime Fermat numbers.

Maximum determinant and relative maximum on the structure

The common and well known fact of the maximum determinant problem theory consists in the statement, that **D**-matrices have to have {1, −1} entries. Much less known orthogonal by string (columns) matrices, order n, having maximal value of determinant.

Let **M** be a matrix with modulus of entries ≤ 1 and M be a class of such matrices.

Theorem 1 (Hadamard inequality [25]). Determinant of **M** is bounded by $n^{n/2}$ following the inequality

$$\det(\mathbf{M}) \le \left(\prod_{i=1}^{n} \sum_{j=1}^{n} m_{ij}^2 \right)^{1/2} \le n^{n/2}.$$

Hadamard matrices belong to the class of square *quasi-orthogonal* matrices defined by equality $\mathbf{MM}^{\mathrm{T}} = \omega\mathbf{I}$, modulus of entries ≤ 1, **I** identity matrix, pure *orthogonal* matrices satisfy $\mathbf{MM}^{\mathrm{T}} = \mathbf{I}$. For all *quasi-orthogonal* matrices we can establish following theorem.

Theorem 2. Determinant of quasi-orthogonal matrix $|\det(\mathbf{M})| = \omega^{n/2}$.

The prove follows directly from definition: $\det(\mathbf{MM}^{\mathrm{T}}) = \det(\mathbf{M})^2$, $\det(\omega\mathbf{I}) = \omega^n$, so value of determinant is bounded by shown power of coefficient ω.

For Hadamard matrices **H**, $\omega = n$, for conference matrices (**C**-matrices) $\mathbf{CC}^{\mathrm{T}} = (n-1)\mathbf{I}$, $\det(\mathbf{C}) = (n-1)^{n/2}$. Hadamard matrices, can exists for orders 1, 2, $4t$ (due conjecture of Hadamard they exist for every $4t$). Let us note, that matrices of maximum determinant, taken for even orders $4t+2$, can exceed value $(n-1)^{n/2}$, it is a price for the strings (columns) pair wise orthogonal property $\mathbf{CC}^{\mathrm{T}} = (n-1)\mathbf{I}$.

So we can name conference matrices as matrices of local maximum determinant, i. e. relative (non absolute) maximum achieved on class M for square equality $\mathbf{CC}^{\mathrm{T}} - (n-1)\mathbf{I} = 0$.

Definition 1. Define the subclass of matrices

$$C_0 = \{\mathbf{M} \mid \mathbf{M} = \{M_{ij}\},\ i,\ j = 1,\ \ldots,\ n;$$
$$\text{for } i \neq j \ \mid M_{ij} \mid \leq 1,\ M_{ii} = 0\}.$$

For the class of matrices defined above, we state the following simple statement based on Hadamard approach. Let

$$\mathbf{M} = \begin{pmatrix} 0 & M_{12} & \cdots & M_{1n} \\ M_{21} & 0 & \cdots & M_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ M_{n1} & M_{n2} & \cdots & 0 \end{pmatrix},$$

where $\mathbf{M} \in C_0$. Then the determinant of $\mathbf{M}$ is maximized when $\mathbf{MM}^{\mathrm{T}}$ is a *scaled* identity matrix $(n-1)\mathbf{I}$, and the bound for the maximum value of determinant is $(n-1)^{n/2}$, i. e. conference matrices play a role of Hadamard matrices for orders $4t+2$ where $\max\limits_{\mathbf{M} \in C_0} |\mathbf{M}| = |\mathbf{C}|$. In the difference to Hadamard matrices, conference matrices can exists for orders 1, 2, $4t$ and for orders $4t+2$ (if $4t+1$ is a sum two squares a^2+b^2). There is no conference matrices of orders 22, 34, 58, 70, 78, 94 (sequence A000952 of OEIS). Conference matrices with orders 66, 86 are unknown today.

Example. Suppose

$$\mathbf{M} = \begin{pmatrix} 0 & M_{12} & M_{13} \\ M_{21} & 0 & M_{23} \\ M_{31} & M_{32} & 0 \end{pmatrix},$$

where M_{12}, M_{13}, and so on are real numbers such that $|M_{ij}| \leq 1$ for all $i \neq j$. Thus $\mathbf{M} \in C_0$, and $|\det(M)| = |M_{13}M_{21}M_{32} + M_{31}M_{12}M_{23}| \leq |M_{13}M_{21}M_{32}| + |M_{31}M_{12}M_{23}| \leq 2$. For any matrix of order 3 fixed structure gives estimation $(n-1)^{n/2} = 2\sqrt{2}$, so there is no conference matrix of order 3 (and any other odd order). With it, if conference matrix exists, for every $n = 4t+2$ it gives maximum determinant on the fixed structure, the same as Hadamard matrix — the structure of resolvable for all orders matrix is a non trivial subject of research (two negacirculant matrix, two border and two circulant matrix and so on).

If for Hadamard matrices the fixed structure is not defined, for conference matrices, historically, it was taken the diagonal structure C_0. Due conjecture of Seberry there are skew Hadamard matrices $(\mathbf{H} + \mathbf{H}^{\mathrm{T}} = 2\mathbf{I})$ for every $n = 4t$, conference matrices follows them on orders $4t$ due $\mathbf{C} = \mathbf{H} - \mathbf{I}$ for Hadamard matrices with positive diagonal. Maximum of determinant for the fixed structure, as we see, belongs to the conference matrices. We can try to generalize class C_0 by class of any quasi-orthogonal matrices (with no 0), but this estimation is enough for our aims to comment conference matrix property to be matrix of relative maximum determinant.

The following question of theory of matrices consists in the search of odd order matrices including matrices of local maximum determinant (having no fixed structure, but being not absolute maximum) defined by the square equality $\mathbf{MM}^{\mathrm{T}} - \omega\mathbf{I} = \mathbf{0}$.

For the latest task we can prepare an optimization procedure, that starts from some beginning $\mathbf{M}_0$ and tries to make determinant bigger for every new step, giving a chain of matrices $\mathbf{M}_k$: $\det(\mathbf{M}_k) > \det(\mathbf{M}_{k-1})$. To achieve this result we take in consideration so called m-norm of quasi-orthogonal matrix (it is not usual norm used for matrices).

Definition 2. m-norm of orthogonal matrix $\mathbf{Q}$, $\mathbf{QQ}^{\mathrm{T}} = \mathbf{I}$, $\mathbf{Q} = \{Q_{ij}\}$, is $m = \max\limits_{i,j} |Q_{ij}|$.

Quasi-orthogonal matrices $\mathbf{H}$, $\mathbf{C}$ and other ones defined by $\mathbf{MM}^{\mathrm{T}} = \omega\mathbf{I}$, modulus of entries ≤ 1, could be found by the corresponding orthogonal matrices divided by m-norm, so the maximum of their entries becoming be equal 1.

Definition 3. m-norm of quasi-orthogonal matrix $\mathbf{M}$, $\mathbf{MM}^{\mathrm{T}} = \omega\mathbf{I}$, is m-norm of corresponding orthogonal matrix $\mathbf{Q} = m\mathbf{M}$.

Theorem 3. Let be constructed a chain of $\mathbf{Q}_k$, $|\mathbf{Q}_k| = 1$, $m_k \leq m_{k-1}$ (their m-norms), so it follows $|\mathbf{M}_k| \to \max\limits_{\mathbf{MM}^{\mathrm{T}} - \omega\mathbf{I} = \mathbf{0}}$.

Lemma 1. Let $\mathbf{M}$ be quasi-orthogonal matrix, order n, with m-norma m, then $|\mathbf{M}| = \dfrac{1}{m^n}$.

It follows from $|\mathbf{Q}| = m^n|\mathbf{M}| = 1$. The tasks of determinant optimization, it is *maxmin*-task, when we minimize the maximal entry of orthogonal matrix $\mathbf{Q}_k$: $m_k \leq m_{k-1}$.

To realize this process, due Lemma 1, we choose initial condition $\mathbf{M}_0$ with m-norm m_0. Let us bound modulus of entries of corresponding matrix $\mathbf{Q}_0$ by value pm_0, where $p \leq 1$. Due this action matrix will lose property to be pair wise strings (columns) orthogonal, but we can restore it by a standard Gramm — Schmidt procedure giving us the next matrix $\mathbf{Q}_1$ saving general property $m_1 \leq m_0$ for enough little shift δ, $p = 1 - \delta$. As it is seen, this algorithm *leads to the extreme point* satisfying the equality $\mathbf{MM}^{\mathrm{T}} - \omega\mathbf{I} = \mathbf{0}$.

For the quasi-orthogonal matrices of low order, 2 or 3, we can build determinant as a function of one or two arguments, the latest one drawn on the Fig. 1.

For the quasi-orthogonal matrices of bigger orders algorithm based on the theorem 3 gives an effective multi-parametric optimization returning Hadamard or conference matrices which were build historically through the very different approach. Hadamard observed it as solution of square equation $\mathbf{HH}^{\mathrm{T}} - n\mathbf{I} = \mathbf{0}$. This approach is good, but it brings no guaranty that integer solution exists for all orders equal to $4t$.

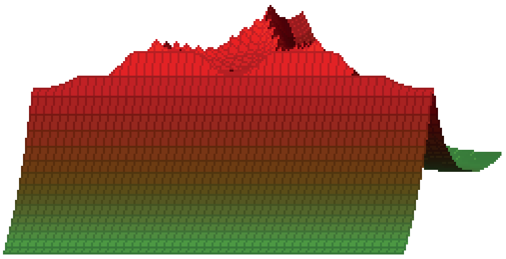
The second idea, that Hadamard matrices have biggest determinant *was forgotten* as a practical approach to calculate matrices due computations that were impossible for his time (but not today). This idea is interesting with many points of view as a bridge between solutions in integer and real numbers: theorem 3 makes Hadamard matrices a part of iteration process with clean prospective accordingly his famous conjecture by means of not combinatorial mathematics.

Theorem style review of determinant bounds known for odd orders well done by the work [26] having numerous details. Main problem of these functional bounds, they go through rational and irrational points, while rational matrices have rational determinant. So it gives some sharp bounds for narrow classes of observed matrices. Remember, that theory of maximum determinant matrices with 1, –1 entries cannot resolve just order 22 to our time. “Barba” matrices exist as a fact of abstract theory for many “resolved” points. It means, they are described by bound partially. Algorithm (to build matrices, if it works) has combinatorial character and cannot be used effectively for big orders.

We take other matrices for irrational values of bound. In such case these theorems lose their sense and cannot be used to describe the result given by “special points”.

There are rare orders equal to prime Fermat numbers (today known five ones).

In different to previous case there is algorithm that doesn’t work outside described area. But for given points it gives result no difference how big is the size of matrix — the latest prime Fermat numbers are very big. Matrix, order 17, can be constructed on the base of so called regular Hadamard matrix, order 16, adding the border. The same step is impossible for other regular structures, for example, it doesn’t work with order 64.



■ *Fig. 1.* Extremal points of determinant

The tiny details of numerical procedure from theorem 3 are discussed in [18]. Naturally, we have the global (absolute) and local maximum with given square bound. Algorithm was realized and maximum determinant quasi-orthogonal matrices were classified in the set of papers [18, 24]. Their property consists in the number of entry values ({1, –1} observed for even orders $4t$, and {0, 1, –1} observed for $2t$) for odd orders it arises and gives a set of values $\{a, b, c, \ldots\}$.

The local maximum determinant matrices appeared to be preferable due their simple structure and low number of entries $\{1, -b\}$. As a matter of fact, Hadamard matrices have these extreme structures as circulant or two-circulant blocks. It prolongates the other way to construct them. Non orthogonal extreme matrices of odd orders have two entries {1, –1}. The correspondence between Hadamard matrices and local maximum determinant matrices is continued on this case by change $-b$ on –1.

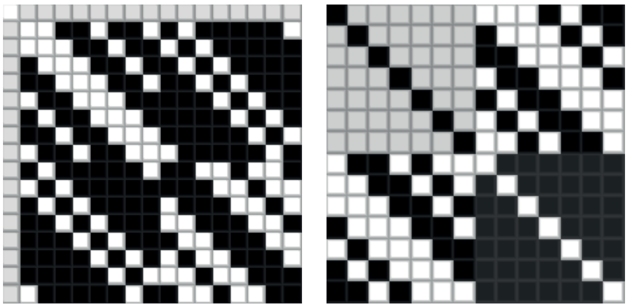
Numerical sequences and number theory

Hadamard was the first one to consider a numerical sequence with a determinant maximum [25]. He showed that for a set of matrices with entries {1, –1} the determinant is maximum, for example, in **H** matrices (Hadamard matrices) of orders 1, 2 and $n = 4t$, t an integer, for which $\mathbf{H}^{\mathrm{T}}\mathbf{H} = n\mathbf{I}$, $\mathbf{I} = \mathrm{diag}(1, 1, \ldots, 1)$.

Columns (and rows) of {1, –1} matrices which have a maximal determinant are strictly orthogonal; such matrices are called Hadamard matrices. Thereby, the absolute maximum determinants of matrices with orthogonal columns and those of **D**-matrices are the same. This statement is not true for other orders, but the difference of absolute maximum determinant for matrices of the two above-mentioned sets is very small. The absolute maximum determinant on the class of non-orthogonal matrices is related to the local extremum (not the absolute one) on the class of quasi-orthogonal matrices.

Let us consider, for example, suboptimal (without an absolute determinant maximum on their set) quasi-orthogonal matrices of orders 17 and 14 shown on Fig. 2. The variety of matrix entry values is depicted by shades of gray.

Rounding of the entries of these matrices to integers {1, –1} produces matrices which are not orthogonal by columns, but *strictly optimal* by determinants. The rule, demonstrated on the pictures, is a general one. The determinant maximums of matrices which



■ *Fig. 2.* Suboptimal quasi-orthogonal matrices of orders 17 and 14

are non-orthogonal or orthogonal by columns (quasi-orthogonal) usually correspond to each other.

The structures of optimal matrices are the same, and the entry values described by parametric dependencies allow us to obtain matrices of both types. Maximum determinant matrices can be obtained by *rounding*. It gives entries 1 and –1.

However, there is a shift in strict optimums: the absolute determinant maximum in non-orthogonal matrices corresponds to a local optimum on the quasi-orthogonal matrix class which is not the biggest one. The opposite is also true. Extreme quasi-orthogonal matrices with a small number of entries are called *Cretan* (see more precise definitions in [24, 27]). The interrelation of extremal problems allows us to use the same numerical method to find both Cretan and maximum determinant matrices [20–23]. However, this brings up a question: on which orders should we seek for a family of matrices extreme by their determinants?

Apart from Sylvester orders $n = 2^k$, k an integer, Mersenne numbers $n = 2^k - 1$ embedded in a sequence of numbers $4t - 1$ are known. Fermat numbers are embedded in a $4u^2 + 1$ sequence which, in turn, is embedded in a $4t + 1$ sequence.

Quasi-orthogonal matrices of odd orders $n = 2^k - 1$ and $n = 2^{2^k} + 1$ which have a *local maximum* of determinant are called Mersenne and Fermat matrices [28, 29] respectively. The definition of Mersenne matrices can be expanded to orders $4t - 1$. The definition of Fermat matrices can be expanded to “quadratic” orders $4u^2 + 1$. These families are discussed more specifically in [18, 24, 27].

Orders of Mersenne and Fermat [18, 28] matrices with entry values rounded to integer (rounded matrices, for short) are neighboring with the orders of Hadamard matrices which have absolute determinant maximums. Determinants of rounded Mersenne matrices of small orders are maximal only for a few first prime numbers of their sequence.

This sequence of extreme matrices is regressing by the relative (with reference to the global maximum) values of the determinant. Rounded Fermat matrices of orders equal to *the first three* Fermat prime numbers are different, having strictly maximal determinants. Fermat prime numbers are a rapidly increasing sequence; therefore checking the matrices of all orders $n = 2^{2^k} + 1$ is numerically impossible. However, their difference from the first matrices with Mersenne prime numbers as orders is obvious. It allows us to assume that a sequence of Fermat matrices is not regressing, and its determinant is always a global maximum.

The two mentioned sets of matrices neighboring with Hadamard matrices are similar, but not identical in relation to the determinant maximums. Let us discuss some important details.

Guido Barba’s inequality

The odd orders for which the upper formally attainable bound of determinants of maximum determinant matrices is known, are obtained from the Guido Barba’s inequality [1, 26].

Theorem 4. It states that matrices **A** of orders n with modulus of entries ≤ 1 satisfy the inequality: $|\det(\mathbf{A})|^2 \le \det((n-1)\mathbf{I} + \mathbf{J}) = (n-1)^{n-1}(2n-1)$, where $\mathbf{I} = \mathrm{diag}(1, 1, ..., 1)$, and **J** is a unity matrix. The maximum can be attained on orders for which $2n - 1$ is a square.

This necessary condition for extreme solutions follows the fact that optimal matrix entries are integers 1 and –1. Note that the Barba’s bound is attainable for orders $n = a^2 + b^2$, $b = a + 1$ [1] nested in the same sequence $4t + 1$ that the Fermat number sequence is embedded.

For Fermat numbers different from 5, $2n - 1$ is not a square, which means that the Barba’s bound is not attainable. It is an optimistic determinant estimation, certainly not pragmatic, because it is irrational.

The non-attainability of the bound is not critical.

The orders of matrices described by certainly attainable integer values of the bound are 5, 13, 25, 41, 61, 85, 113..., and the structures of every second one of these matrices of orders 13, 41, 85, ... are significantly more complex than those of the others. There is no algorithm to construct these matrices: the existence of matrices for the orders we have listed is theoretically possible, but not all of them are known [1, 5, 17].

Matrices of orders equal to Mersenne numbers and Fermat matrices of prime orders $F_k = 3, 5, 17, 257, 65\,537...$ have an advantage over all other matrices, because they have an algorithm for their construction, which is a modified Sylvester algorithm [28, 29] producing matrices of a local determinant maximum [18, 24] and, as we believe, maximum determinant matrices for orders equal to prime Fermat numbers.

At the same time, an irrational Mersenne matrix, after its irrational elements are rounded to integer values, becomes equal to the {1, –1}-core of a normalized Hadamard matrix, and the core of a Fermat matrix after rounding its irrational elements to {1, –1} becomes equal to a regular Hadamard matrix of order $4u^2$. Thus, matrices of non-strict determinant optimums of orders equal to Mersenne numbers are findable and can be used for indirect finding of Hadamard matrices strictly optimal by their determinants.

Maximum determinant matrix conjecture

Based on the preliminary study, we identified that:

— skew-symmetric circulant Mersenne matrices correspond to prime Mersenne numbers [27, 28];

— prime numbers and the symmetry types of circulant optimal and sub-optimal structures are synonyms of a certain hyperquality of such different mathematical objects as numbers and matrices.

The first person (if not the legendary Pythagoras) who noticed the correlation between objects from different areas of mathematics was Karl Friedrich Gauss. In 1796, he discovered a relation between prime numbers and geometric figures, after he inscribed a regular heptadecagon into a circle.

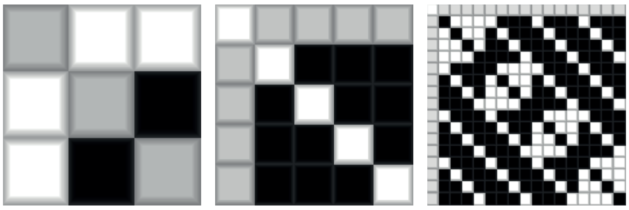
Later, Gauss formulated a generic case about the relation between the number of sides of a regular polygon inscribed in a circle, and the Fermat prime numbers.

The peculiarity of Fermat prime numbers allows us to formulate a conjecture about the relation between matrix orders and the maximums of their determinants.

Generalised Gauss conjecture. Quasi-orthogonal local maximum determinant matrices [24, 27] of orders equal to prime Fermat prime numbers $F_k = 3$, 5, 17, 257, 65 537, ... and only they for all matrices of orders within a sequence which nests Fermat numbers, when rounded to {1, –1}, give global maximum determinant matrices.

First three Fermat matrices $\mathbf{F} = \begin{pmatrix} a & s^{\mathrm{T}} \\ s & \mathbf{H} \end{pmatrix}$ of orders 3, 5 and 17 are based on regular Hadamard matrices **H** with entries changed to $\{a, -b\}$ to get F orthogonal by rows (columns) [18, 24], the latter of which is shown on Fig. 3, can be rounded to $\{a = 1,$ $b = 1$, entries of s are 1} and checked to validate the conjecture. It was noted earlier that $2n - 1$ is not a square for Fermat numbers different from 5.

The Barba's bound $B = (n-1)^{(n-1)/2}(2n-1)^{1/2}$ is an irrational and unattainable number for Fermat matrices rounded by entries (integer). However, this is just an optimistic upper-bound estimate of the determinant, an abstract bound deducted in the work [1] which may or may not be attained by an integer matrix.



■ *Fig. 3*. Quasi-orthogonal Fermat matrices

In case this optimistic irrational bound B is unattainable, the pragmatic estimate differs from it by an irrational scale multiplier, multiplying by which makes the real bound integer-valued and attainable. Since we know the Fermat matrix stricture, and the irrational multiplier of the bound can be found, the determinant for a Fermat matrix of order $n = F_k$ should be estimated as $F_{k-1}/(2F_k - 1)^{1/2} \times B$.

As noted above, $F_{k-1}/(2F_k - 1)^{1/2}$ is an irrational number, in the general case.

It gives a relative (as compared to the bound B) determinant value described by the following formulae: $|\det(\mathbf{A})| = (n-1)^{(n-1)/2}(2n-1)^{1/2}F_{k-1}/(2n - 1)^{1/2} = (n-1)^{(n-1)/2}F_{k-1}$, $n = F_k$ the Fermat number. This is an estimate of the attainable value of an integer matrix determinant.

The first Fermat number $F_0 = 3$ is a starting one, without a preliminary Fermat number, but this matrix, like the matrix of order 5, is known. In this matrix, the –1 entries which are different from 1 are placed on the diagonal.

For order $F_1 = 5$, we have an integer determinant correction value equal to 1.

This is an exception: the Fermat matrix determinant attains the Barba's bound and we have $F_0/(2F_1 - 1)^{1/2} = 3/9^{1/2} = 1$. The optimal matrix structure matches the starting one (for order 3), so these are two diagonal structures with a simple form.

The first matrix which is different from them is a Fermat matrix of order 17.

For $F_2 = 17$, we have $2F_2 - 1 = 33$, which is not a square. Its relative (in reference to the Barba's bound) determinant equals $F_1/(2F_2 - 1)^{1/2} = 5/33^{1/2} = 0.8704...$ This irrational number is a scale multiplier which is a correction to the unattainable Barba's bound $B = 16^8 \times 33^{1/2}$.

Their product is an integer $5/33^{1/2} \times B = 5 \times 16^8 = 21\ 474\ 836\ 480$. This is the determinant for the Fermat matrix of order 17. This estimation is the same as $327\ 680 \times 2^{16}$ stated on the website [15].

Fermat matrices can be found for orders into which Fermat numbers are nested, like 37, 65, etc. According to the same resource [15], the determinant of a determinant maximum matrix of order

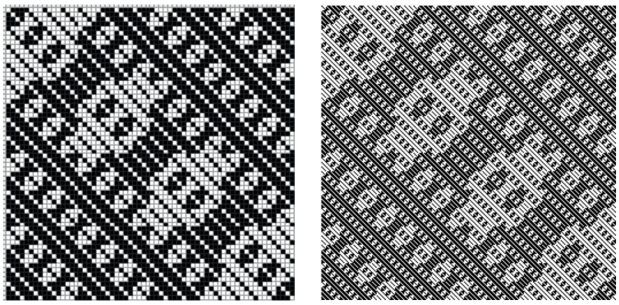
37 is equal to $72 \times 9^{17} \times 2^{36}$. The determinant of a determinant maximum matrix of order 65 is estimated as $148 \times 16^{31} \times 2^{64}$.

The determinant of the Cretan matrix of order 37 given in [30] and rounded by its entries is approximately equal to 7.22×10^{28}, being less than the estimate 8.25×10^{28} for the integer matrix in the table [17]. For the order 65 (Fig. 4 illustrates it and the next order 257), the determinant of a rounded Cretan matrix is 5.65×10^{58}, whereas the table [15] gives the value of 5.81×10^{58} for an integer matrix of the same order.

The data above confirm the conjecture: a determinant maximum can be attained only for matrices of orders equal to prime Fermat numbers. On orders equal to prime and composite numbers of a sequence, which nests the Fermat sequence (without them), the statement is not true. An interesting analogy is noticeable here: according to the conjecture, and the Gauss's theorem, regular polygons with 37 and 65 angles cannot be completed with just a ruler and a compass.

We believe that the similarity between hyper objects of mathematics and the conditions of the Gauss's theorem can apply, among others, to determinant maximum matrices.

Extremal matrices of orders 257 and 65 537 are very difficult to calculate and check the values of their determinants (to match with determinants of Fermat matrices) due to the large number of possible permutations. However, we have calculated the Fermat matrix of order 257 using a modified Sylvester algorithm [27–29]. The correspondence of symmetries to matrix orders was studied in [31, 32]. The symmetric matrix image is shown in Fig. 4.



■ *Fig. 4.* Image of Fermat matrices of orders 65 and 257

According to our conjecture, the Fermat matrix of order 257 has a relative (in reference to the Barba's bound) determinant value $F_2/(2F_3 - 1)^{1/2} = 0.7505...$ This irrational number corresponds to the integer value of $|\det(\mathbf{A})| = (n - 1)^{(n-1)/2}F_{k-1} = 256^{128} \times 17$ (approximately 0.31×10^{310}). This estimation is absent in the table on the website [17] and should be considered new.

Conclusion

Fermat matrices differ from the matrices of orders where the Barba's bound is attainable, because we know an algorithm of finite complexity for their calculation. Hence, for a rounded Fermat matrix of order 65 537, for instance, you can predict a precise value of its relative determinant 0.7099 (absolute value is $65\,536^{32768} \times 257$), and build its matrix image. It will be close to the one depicted in Fig. 2, but with significantly more fractal details.

Quasi-orthogonal Fermat matrices tend to Hadamard matrices with a rise in order, and the values of their entries tend to values 1 and –1. The determinants of rounded Fermat matrices of known prime orders do not go below 0.7 (in reference to the Barba's estimation). These facts allow us to consider the matrices of orders equal to prime Fermat numbers a family of maximum determinant matrices.

Acknowledgements

The authors would like to acknowledge the great help of Professor Jennifer Seberry with the translation and discussion of the content of this paper. The authors also wish to sincerely thank Tamara Balonina for converting this paper into a printable format.

Financial support

This research received funding from the Ministry of Education and Science of Russian Federation according to the project part of the state funding assignment No 2.2200.2017/4.6.

References

1. Barba G. Intorno al teorema di Hadamard sui determinanti a valore Massimo. *Giorn. Mat. Battaglini*, 1933, vol. 71, pp. 70–86 (In Italian).
2. Ehlich H. Determinantenabschätzungen für binäre Matrizen. *Math. Z.*, 1964, vol. 83, pp. 123–132 (In German).
3. Wojtas W. On Hadamard's inequality for the determinants of order non-divisible by 4. *Colloq. Math.*, 1964, vol. 12, pp. 73–83.
4. Osborn J. H. *The Hadamard maximal determinant problem*. Honours thesis. University of Melbourne, 2002. 144 pp. Available at: http://maths-people.anu.edu.au/~osborn/publications/pubsall.html (accessed 5 April 2020).

5. Baumert L. D. Golomb S. W., Hall M. Jr. Discovery of an Hadamard matrix of order 92. *Bull. Amer. Math. Soc.*, 1962, vol. 68, pp. 237–238.
6. Brouwer A. E. An infinite series of symmetric designs. *Math. Centrum Amsterdam Report ZW*, 1983, iss. 202/83, 5 p.
7. Cohn J. H. E. On determinants with elements ±1, II. *Bull. London Math. Soc.*, 1989, vol. 21, iss. 1, pp. 36–42. https://doi.org/10.1112/blms/21.1.36
8. Seberry J., Xia T., Koukouvinos C., Mitrouli M. The maximal determinant and subdeterminants of ±1 matrices. *Linear Algebra and its Applications*; *Special Issue on the Combinatorial Matrix Theory Conference*, 2003, vol. 373, pp. 297–310. doi:10.1016/S0024-3795(03)00584-6
9. Koukouvinos C., Mitrouli M., Seberry J. Bounds on the maximum determinant for (1, –1) matrices. *Bull. Inst. Combin. Appl.*, 2000, vol. 29, pp. 39–48.
10. Koukouvinos C., Mitrouli M., Seberry J. An algorithm to find formulae and values of minors of Hadamard matrices. *Linear Algebra Appl.*, 2001, vol. 330 pp. 129–147.
11. Koukouvinos C., Mitrouli M., Seberry J. An algorithm to find formulae and values of minors of Hadamard matrices: II. *Linear Algebra Appl.*, 2003, vol. 371, pp. 111–124.
12. Brent R. P. Finding many D-optimal designs by randomized decomposition and switching. *The Australasian Journal of Combinatorics*, 2013, vol. 55, pp. 15–30.
13. Djokovic D. Z., Kotsireas I. S. Compression of periodic complementary sequences and applications. *Des. Codes Cryptogr.*, 2015, vol. 74, pp. 365–377.
14. Orrick W. P. The maximal {–1, 1}-determinant of order 15. *Metrika*, 2005, vol. 62(2), pp. 195–219.
15. Orrick W. P., Solomon B. Large determinant sign matrices of order $4k + 1$. *Discrete Math.*, 2007, vol. 307. pp. 226–236.
16. Seberry J. *The Hadamard Matrices*. Available at: http://www.uow.edu.au/~jennie (accessed 16 April 2016).
17. Orrick W. P., Solomon B. *The Hadamard Maximal Determinant Problem*. Available at: http://indiana.edu/~maxdet (accessed 16 April 2016).
18. Balonin N. A., Sergeev M. B. Quasi-orthogonal local maximum determinant matrices. *Applied Mathematical Sciences*, 2015, vol. 9, no. 6, pp. 285–293. doi:10.12988/ams.2015.4111000
19. Balonin N. A., Sergeev M. B. Initial approximation matrices in search for generalized weighted matrices of global or local maximum determinant, *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2015, no. 6, pp. 2–9 (In Russian). doi:10.15217/issn1684-8853.2015.6.2
20. Kharaghani H. and Orrick W. P. *D-optimal matrices*. In: *Handbook of Combinatorial Designs* (Discrete Mathematics and its Applications). 2nd ed. C. J. Colbourn, J. H. Dinitz (eds). Chapman & Hall/CRC, Boca Raton, FL, 2007. Pp. 296–298.
21. Brent R. P., Orrick W. P., Osborn J. H., Zimmermann P. *Maximal Determinants and Saturated D-optimal Designs of Orders 19 and 37 (preprint)*. Available at: http://arxiv.org/abs/1112.4160 (accessed 5 April 2020).
22. Djokovic D. Z., Kotsireas I. S. New results on D-optimal designs. *J. Combin. Designs*, 2012, vol. 20, pp. 278–289.
23. Djokovic D. Z., Kotsireas I. S. *D-optimal matrices of orders 118, 138, 150, 154 and 174*. In: *Algebraic Design Theory and Hadamard Matrices* (Springer Proceedings in Mathematics & Statistics). Lethbridge, Alberta, Canada, 2014. Pp. 71–282.
24. Balonin N. A., Seberry J. Remarks on extremal and maximum determinant matrices with real entries ≤ 1. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2014, no. 5, pp. 2–4.
25. Hadamard J. Résolution d'une Question Relative aux Déterminants. *Bulletin des Sciences Mathématiques*, 1893, vol. 17, pp. 240–246 (In French).
26. Neubauer M. G., Radcliffe A. J. The maximum determinant of ±1 matrices. *Linear Algebra and its Applications*, 1997, vol. 257, pp. 289–306.
27. Balonin N. A., Sergeev M. B. Mersenne and Hadamard matrices. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2016, no. 1, pp. 92–94 (In Russian). doi:10.15217/issn1684-8853.2016.1.2
28. Sergeev A. M. Generalized Mersenne matrices and Balonin's conjecture. *Automatic Control and Computer Sciences*, 2014, vol. 48, no. 4, pp. 214–220. doi:10.3103/S0146411614040063
29. Balonin N., Sergeev M. Expansion of the orthogonal basis in video compression. *Frontiers in Artificial Intelligence and Applications*, 2014, vol. 262, pp. 468–474. doi:10.3233/978-1-61499-405-3-468
30. Balonin N. A., Seberry Jennifer, Sergeev M. B. Three level Cretan matrices of order 37. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2015, no. 2, pp. 2–3. doi:10.15217/issn1684-8853.2015.2.2
31. Balonin N. A., Djokovic D. Z. Symmetry of two circulant Hadamard matrices and periodic Golay pairs. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2015, no. 3, pp. 2–16 (In Russian). doi:10.15217/issn1684-8853.2015.3.2
32. Balonin N. A., Djokovic D. Z. Negaperiodic Golay pairs and Hadamard matrices. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2015, no. 5, pp. 2–17. doi:10.15217/issn1684-8853.2015.5.2

УДК 519.61:511-33
doi:10.31799/1684-8853-2020-2-2-9

Простые числа Ферма и гипотеза о матрицах максимального детерминанта

Н. А. Балонин[a], доктор техн. наук, профессор, orcid.org/0000-0001-7338-4920, korbendfs@mail.ru
М. Б. Сергеев[a], доктор техн. наук, профессор, orcid.org/0000-0002-3845-9277
А. А. Востриков[a], канд. техн. наук, доцент, orcid.org/0000-0002-8513-368
[a]Санкт-Петербургский государственный университет аэрокосмического приборостроения, Б. Морская ул., 67, Санкт-Петербург, 190000, РФ

Цель: решение задачи оптимизации определителей матриц с модулем элементов ≤ 1, разработка теории таких матриц на основе предварительных результатов исследования. **Методы:** экстремальные (по определителю матрицы) решения устанавливаются путем минимизации абсолютных значений элементов ортогональных матриц с последующей классификацией. **Результаты:** матрицы порядков, равных простым числам Ферма, являются особыми, так как их абсолютные максимумы детерминантов могут быть достигнуты на простой структуре. Дана точная оценка максимума детерминанта для этих матриц и сформулирована соответствующая гипотеза. Проанализирована тесная связь между решениями экстремальных задач с ограничением на ортогональность столбцов матриц и без него. Показано, что относительные максимумы определителей ортогональных матриц соответствуют абсолютным максимумам определителей матриц, не ограниченных ортогональностью. Рассмотрены способы построения экстремальных матричных семейств для порядков, равных числам Мерсенна. **Практическая значимость:** матрицы максимального детерминанта широко используются в задачах помехозащищенного кодирования, сжатия и маскирования видеоинформации. Программы для поиска матриц максимальной детерминанты и библиотеки построенных матриц используются в математической сети «mathscinet.ru» вместе с исполняемыми онлайн-алгоритмами.

Ключевые слова — определитель, максимальный определитель, квазиортогональные матрицы, матрицы Адамара, матрицы Мерсенна, матрицы Ферма, критские матрицы.

Для цитирования: Balonin N. A., Sergeev M. B., Vostricov A. A. Prime Fermat numbers and maximum determinant matrix conjecture. *Информационно-управляющие системы*, 2020, № 2, с. 2–9. doi:10.31799/1684-8853-2020-2-2-9
For citation: Balonin N. A., Sergeev M. B., Vostricov A. A. Prime Fermat numbers and maximum determinant matrix conjecture. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2020, no. 2, pp. 2–9. doi:10.31799/1684-8853-2020-2-2-9