TOTALLY POSITIVE MATRICES OVER FINITE FIELDS: THE MINIMAL ODD PRIME FOR NINE SHAPES, AND TWO CORRECTIONS

KOREA SUPERINTELLIGENCE LABS

Abstract. Call an element of a finite field *positive* when it is a nonzero square, and call a matrix over that field *totally positive* when every one of its minors is positive. Ayyer and Prasad, who introduced this class, ask for the least prime power q admitting an $m \times n$ totally positive matrix over $\mathbb{F}_q$; over odd q their own data reaches only the shapes 2×2 and 3×3. We answer the odd-prime half of that question for nine shapes. Two of the three regimes turn out to be classical under other names, and we say so: in characteristic 2 "positive" is "nonzero", so the problem is the existence of a full superregular matrix, equivalently of an $[m+n, m, n+1]_q$ MDS code; and for $m = 2$ an elementary totally positive $2 \times n$ matrix over $\mathbb{F}_q$ is exactly a clique of size $n + 1$ in the Paley graph ($q \equiv 1 \bmod 4$) or a transitive subtournament of order $n + 1$ in the Paley tournament ($q \equiv 3 \bmod 4$), so the $2 \times n$ values reproduce published data. What is left is the odd corner $m, n \geq 3$. There we prove that the minimal odd prime is 31 for each of the shapes 3×4, 4×4 and 3×5: the symmetric matrix over $\mathbb{F}_{31}$ with rows $(1, 1, 1, 1)$, $(1, 8, 5, 2)$, $(1, 5, 9, 10)$, $(1, 2, 10, 20)$ witnesses the first two shapes, an explicit 3×5 matrix over $\mathbb{F}_{31}$ the third, and nothing at all witnesses any of them over $\mathbb{F}_p$ for odd $p \leq 29$; the non-existence half is an exhaustive search over fewer than 70 000 candidates, made small by a normal form and by the fact that every off-border entry must be a square whose predecessor is also a square. We also record two corrections to the source. Six counts printed there contradict its own Proposition 5.2, which forces $|\mathbb{F}_q^+|^{m+n-1}$ to divide every such count; the values consistent with that proposition are 236 196, 966 306, 1 492 992 and 141 178 800, 23 640 923 250 000. And the $q \equiv 3 \pmod 4$ half of the proof of its Proposition 5.6 treats the set $\{a : a,\, a-1 \text{ positive}\}$ as totally ordered by "the difference is positive"; at $q = 19$ that set carries the directed 3-cycle $5 \to 6 \to 17 \to 5$, and $\{5, 6, 17\}$ is precisely the off-border entry set of the 3×3 totally positive matrix over $\mathbb{F}_{19}$ exhibited below. The *statement* of that proposition is not refuted by anything here. Every numbered result below is machine-checked in Lean 4, except where it is flagged as a paper argument or as a computation made outside the formal development; §8 says exactly what the machine checks and what it does not.

1. Introduction

Cooper, Hanna and Whitlatch [2] made a notion of positivity over a finite field explicit: an element $a \in \mathbb{F}_q^\times$ is *positive* if $a = b^2$ for some $b \in \mathbb{F}_q^\times$. Write $\mathbb{F}_q^+$ for the set of positive elements, so that $|\mathbb{F}_q^+| = (q-1)/2$ when q is odd and $|\mathbb{F}_q^+| = q - 1$ when q is even — in characteristic 2 every nonzero element is a square, hence positive.

Ayyer and Prasad [1] carry this notion through the matrix classes it suggests. Their Definition 5.1 reads, verbatim:

> A matrix $A \in M_{m,n}(\mathbb{F}_q)$ is said to be *totally positive* if all of its minors are positive; that is $\det(A_{I,J})$ is positive for all $I \subseteq [m]$, $J \subseteq [n]$ of same size. We denote by $\mathrm{TP}_{m,n}(\mathbb{F}_q)$ the set of all totally positive matrices in $M_{m,n}(\mathbb{F}_q)$.

Their Proposition 5.2 computes $|\mathrm{TP}_{m,n}(\mathbb{F}_q)| = r \cdot |\mathbb{F}_q^+|^{m+n-1}$, where r counts the *elementary* totally positive matrices — those whose first row and first column are all 1 (their Definition 5.3) — and their Lemma 5.4 evaluates r for 2×2 matrices over every q and for 3×3 matrices in characteristic 2. Their Proposition 5.6 bounds the shape against the field:

$$q \;\geq\; \begin{cases} \max(m+1, n+1) & q \text{ even}, \\ \max(4m+1, 4n+1) & q \equiv 1 \pmod 4, \\ 4(m+n) - 9 & q \equiv 3 \pmod 4, \end{cases}$$

whenever an $m \times n$ totally positive matrix over $\mathbb{F}_q$ exists and $m, n \geq 2$. They then observe that their proof uses only the order-2 minors $A_{\{1,i\},\{1,j\}}$, so the bound "is likely far from optimal", and ask:

Question 5.7 of [1]**.** For fixed positive integers m and n, find the minimal prime power q such that there exists an $m \times n$ totally positive matrix over $\mathbb{F}_q$. In particular how does this minimal value of q grow with m and n?

Over odd q their own data reaches exactly two shapes. Their Lemma 5.4 counts the elementary totally positive 2×2 matrices over every q, and that count — $(q-5)/4$ for $q \equiv 1$ and $(q-3)/4$ for $q \equiv 3 \pmod 4$ — vanishes at $q = 3$ and $q = 5$ and is first positive at $q = 7$, which fixes the 2×2 minimum; and one sentence, *"Using* `SageMath`*, we find that* $|\mathrm{TP}_{3,3}(\mathbb{F}_q)| = 0$ *for odd* q *and* $q \leq 17$*"*, together with the nonzero counts they then print at $q = 19, 23, 25$, fixes the 3×3 minimum at 19. Everything else they compute — closed formulas for $|\mathrm{TP}_{2,k}(\mathbb{F}_q)|$ and $|\mathrm{TP}_{3,3}(\mathbb{F}_q)|$ in characteristic 2, and counts for 3×4 at $q = 8, 16, 32$ — is even-q. For no other shape does anything there identify an odd minimum, and they state none.

This paper settles the *odd prime* part of that question for nine shapes. Write $p_{\min}(m,n)$ for the least odd prime p such that $\mathbb{F}_p$ carries an $m \times n$ totally positive matrix.

(m,n)	$(2,2)$	$(2,3)$	$(2,4)$	$(2,5)$	$(2,6)$	$(3,3)$	$(3,4)$	$(3,5)$	$(4,4)$
$p_{\min}(m,n)$	7	11	19	31	31	19	**31**	**31**	**31**

Of these nine values, six are not new, and saying which are and which are not is a large part of what this paper contributes. Two regimes of the question degenerate to classical problems that [1] does not name.

Characteristic 2 is the MDS problem. When q is even, "positive" is "nonzero", so an $m \times n$ totally positive matrix over $\mathbb{F}_q$ is exactly a *full superregular* matrix: one all of whose minors are nonzero. Almeida and Napp [4] state the terminology — "A matrix is superregular if all of its minors that are not trivially zero are nonzero ... When a superregular matrix has all its entries nonzero, it is called full superregular and these matrices are used to construct Maximum Distance Separable block codes". Equivalently $[\, I_m \mid A \,]$ generates an $[m+n, m, n+1]_q$ MDS code, and generalized Reed–Solomon codes supply such an A whenever $m + n \leq q + 1$; the structure of the generator matrices of MDS codes is the subject of Roth and Seroussi [3]. The even half of the Question is therefore a question about MDS code lengths, and none of that literature is cited in [1]: the strings `superregular`, `MDS`, `Cauchy matrix`, `coding theory`, `maximum distance`, `Reed-Solomon` and `totally nonsingular` do not occur in it.

The shape $2 \times n$ is the Paley clique problem. An elementary totally positive $2 \times n$ matrix over $\mathbb{F}_q$ has rows $(1, 1, \ldots, 1)$ and $(1, a_1, \ldots, a_{n-1})$, and its minors say exactly that in the list $0, 1, a_1, \ldots, a_{n-1}$ every later-minus-earlier difference is positive (Proposition 3.1). For $q \equiv 1 \pmod 4$ the relation "the difference is a nonzero square" is symmetric, and such a list is a clique of size $n + 1$ in the Paley graph on $\mathbb{F}_q$; for $q \equiv 3 \pmod 4$ it is a transitive subtournament of order $n + 1$ in the Paley tournament. Both quantities are recorded data: the Paley clique numbers are OEIS **A320757** [5], whose first six terms $2, 3, 3, 4, 4, 5$ at $p = 5, 13, 17, 29, 37, 41$ our computation reproduces exactly, and the transitive-subtournament side goes back to Erdős and Moser [6]. The word "Paley" occurs twice in [1]. Once in its introduction, in a list of places where quadratic residues appear; and once in its §2.3, where it remarks that "[t]he number of common neighbors of two neighboring vertices in a Paley graph can also be determined using" its Theorem 2.13, the count of the elements y for which y and $y - 1$ are both positive — the set called D_q in §2 below, which is exactly the pruning set of our searches. So the source comes within one step of the correspondence of Proposition 3.1; but neither passage connects the Paley graph with $\mathrm{TP}_{2,n}$, and the correspondence itself is nowhere in [1].

What is left is the corner $m, n \geq 3$ over odd q, where the constraints mix order-2 minors on four entries with order-3 minors on nine and neither reformulation applies. There, $(3,3)$ is already decided by the data in [1] itself — its scan gives 0 for odd $q \leq 17$ and it prints a nonzero count at $q = 19$ — and the three shapes $(3,4)$, $(4,4)$, $(3,5)$ are, as far as we could determine, new:

Theorems 5.2, 5.3, 5.4. $p_{\min}(3,4) = p_{\min}(4,4) = p_{\min}(3,5) = 31$. There is no totally positive matrix of any of these three shapes over $\mathbb{F}_p$ for any odd prime $p \le 29$, and

$$W = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 8 & 5 & 2 \\ 1 & 5 & 9 & 10 \\ 1 & 2 & 10 & 20 \end{pmatrix} \in M_4(\mathbb{F}_{31})$$

is totally positive, as is its leading 3×4 submatrix; the shape 3×5 has a witness of its own, given in Theorem 5.4.

Finally we report two corrections to [1]. Its Proposition 5.2 forces $|\mathbb{F}_q^+|^{m+n-1}$ to divide $|\mathrm{TP}_{m,n}(\mathbb{F}_q)|$; all six counts printed in its §5.1 fail that divisibility (Theorem 7.1). And the $q \equiv 3 \pmod 4$ half of the proof of its Proposition 5.6 needs the set of a with a and $a-1$ both positive to be totally ordered by "the difference is positive"; at $q = 19$ it is not, and the obstruction is realised by the very matrix that witnesses $p_{\min}(3,3) = 19$ (Theorem 7.3). The second is a defect in a proof, not a counterexample to a statement: the inequality of Proposition 5.6 holds in every case we computed, and is tight twice.

Remark 1.1. Every section and result number of [1] quoted here is the number carried by v1, read off a local build of the v1 e-print source: Definition 2.6 for positivity, Definition 5.1, Proposition 5.2, Definition 5.3, Lemma 5.4, Lemma 5.5, Proposition 5.6, Question 5.7; the six printed counts sit in §5.1 "Enumeration", and Question 5.7 closes §5.2 "Bounds relating the order and q", just before §5.3 "Structural formula". A later version could of course renumber.

2. Preliminaries

Throughout, F is a finite field, $F^+ = \{a \in F^\times : a = b^2 \text{ for some } b \in F^\times\}$, and for $A \in M_{m,n}(F)$ and $I \subseteq [m]$, $J \subseteq [n]$ with $|I| = |J|$ we write $A_{I,J}$ for the corresponding submatrix. A matrix is *totally positive* when $\det(A_{I,J}) \in F^+$ for all such I, J, including the singletons; so every entry of a totally positive matrix is positive, and in particular nonzero. A totally positive matrix is *elementary* when its first row and first column consist of 1's.

The three facts below are what turn the existence question into a finite search. The first two are due to [1]; only the proofs are ours, and we give them in the generality of an arbitrary finite field.

Lemma 2.1 ([1], Proposition 5.2, Claim 1)**.** *Let $A \in M_{m,n}(F)$ be totally positive and let $u \in (F^+)^m$, $v \in (F^+)^n$. Then the matrix B with $b_{ij} = u_i a_{ij} v_j$ is totally positive.*

Proof. $B_{I,J} = \mathrm{diag}(u|_I) \cdot A_{I,J} \cdot \mathrm{diag}(v|_J)$, so $\det(B_{I,J}) = \left(\prod_{i \in I} u_i\right)\left(\prod_{j \in J} v_j\right)\det(A_{I,J})$. A product of positive elements is positive, and $\det(A_{I,J})$ is positive by hypothesis. □

Lemma 2.2 (the normal form; [1], after Proposition 5.2)**.** *Every totally positive $A \in M_{m,n}(F)$ ($m, n \ge 1$) is carried by a scaling as in Lemma 2.1 to an elementary totally positive matrix.*

Proof. All entries of A are positive, hence invertible with positive inverse, since the inverse of a nonzero square is a nonzero square. Take $u_i = a_{11}a_{i1}^{-1}$ and $v_j = a_{1j}^{-1}$. Then $b_{1j} = a_{11}a_{11}^{-1}a_{1j}a_{1j}^{-1} = 1$ and $b_{i1} = a_{11}a_{i1}^{-1}a_{i1}a_{11}^{-1} = 1$, and B is totally positive by Lemma 2.1. □

[1] states in addition that the elementary representative is unique. We do not use uniqueness and do not prove it.

Lemma 2.3. *If $A \in M_{m,n}(F)$ is totally positive and $m' \le m$, $n' \le n$, then the leading $m' \times n'$ submatrix of A is totally positive.*

Proof. A minor of the leading submatrix on rows I and columns J is the minor of A on the same index sets, viewed in $[m]$ and $[n]$. □

Corollary 2.4. *If no $m' \times n'$ totally positive matrix exists over F, then no $m \times n$ one exists for any $m \ge m'$, $n \ge n'$.*

The two minors that constrain a single off-border entry are cheap enough to name once and for all. Let

$$D_q \;=\; \{a \in \mathbb{F}_q :\; a \in \mathbb{F}_q^+ \text{ and } a-1 \in \mathbb{F}_q^+\}$$

be the *double-positive set*. If B is an elementary totally positive matrix then every off-border entry b_{ij} ($i, j \geq 2$) lies in D_q: positivity of the order-1 minor gives $b_{ij} \in \mathbb{F}_q^+$, and positivity of $\det B_{\{1,i\},\{1,j\}} = b_{ij} - 1$ gives the rest. For $m = n = 2$ this is the whole condition, which is Lemma 5.4 of [1] — and, stated directly as "the number of elements $y \in \mathbb{F}_q^+$ such that $y - 1 \in \mathbb{F}_q^+$", its Theorem 2.13: $|D_q|$ equals $q-2$, $(q-5)/4$ or $(q-3)/4$ according as q is even, $q \equiv 1$ or $q \equiv 3 \pmod 4$.

Proposition 2.5. *For the ten odd primes $p \leq 31$ the sizes $|D_p|$ are*

p	3	5	7	11	13	17	19	23	29	31
$\lvert D_p\rvert$	0	0	1	2	2	3	4	5	6	7

in agreement with Lemma 5.4 of [1].

This is a computation, recomputed here from the definition rather than from the formula, and it is the control that the pruning used in §6 prunes with the right set.

3. The shapes $2 \times n$, and what they already are

Proposition 3.1. *Let q be a prime power and $n \geq 2$. There is a $2 \times n$ totally positive matrix over $\mathbb{F}_q$ if and only if there are $n+1$ elements $y_0, y_1, \ldots, y_n$ of $\mathbb{F}_q$ with $y_j - y_i \in \mathbb{F}_q^+$ for all $i < j$. For $q \equiv 1 \pmod 4$ such a list is a clique of size $n+1$ in the Paley graph on $\mathbb{F}_q$, and for $q \equiv 3 \pmod 4$ it is a transitive subtournament of order $n+1$ in the Paley tournament on $\mathbb{F}_q$.*

Proof. By Lemma 2.2 we may take the matrix B elementary, with rows $(1, 1, \ldots, 1)$ and $(1, a_1, \ldots, a_{n-1})$. Its minors are the entries, the minors $\det B_{\{1,2\},\{1,j+1\}} = a_j - 1$, and the minors $\det B_{\{1,2\},\{i+1,j+1\}} = a_j - a_i$ for $i < j$. So B is totally positive exactly when the list $0, 1, a_1, \ldots, a_{n-1}$ has all later-minus-earlier differences positive. Conversely, given such a list $y_0, \ldots, y_n$, the map $x \mapsto (x - y_0)(y_1 - y_0)^{-1}$ is a bijection of $\mathbb{F}_q$ preserving the relation "the difference is positive", because $y_1 - y_0$ is positive, and it sends the list to one beginning $0, 1$. Finally, -1 is a square in $\mathbb{F}_q$ precisely when $q \equiv 1 \pmod 4$ (for q odd), so the relation is symmetric there and a tournament otherwise. ☐

Proposition 3.1 converts the $2 \times n$ row of the table into a table of Paley clique and transitive-subtournament numbers, which are known. We record the values for completeness, and because they are the base of the monotonicity ladder of Corollary 2.4 used in §5.

Theorem 3.2. *$p_{\min}(2,2) = 7$, $p_{\min}(2,3) = 11$, $p_{\min}(2,4) = 19$, and $p_{\min}(2,5) = p_{\min}(2,6) = 31$. Witnesses, written as the second row of the elementary matrix, are $(1,2)$ over $\mathbb{F}_7$, $(1,4,5)$ over $\mathbb{F}_{11}$, $(1,6,17,7)$ over $\mathbb{F}_{19}$, and $(1,8,5,2,9,10)$ over $\mathbb{F}_{31}$; the last also furnishes, in its leading 2×5 submatrix, the witness for $(2,5)$.*

Remark 3.3. None of these five values is new. $p_{\min}(2,2) = 7$ is immediate from Lemma 5.4 of [1], whose count vanishes at $q = 3, 5$ and is first positive at $q = 7$. The rest are the Paley data of Proposition 3.1. Our computation of the maximal chain length in $\mathbb{F}_q$ for the eighteen odd $q \leq 49$ gives, at the primes $q \equiv 1 \pmod 4$ namely $5, 13, 17, 29, 37, 41$, the values $2, 3, 3, 4, 4, 5$, which are exactly the first six terms of A320757 [5]. At $q = 7$ it gives 3: the Paley tournament of order 7 has no transitive subtournament of order 4. That is the example Erdős and Moser give. Writing $f(n)$ for the largest k such that every tournament on n vertices carries a transitive subtournament on k vertices, they remark, on p. 127 of [6], verbatim: *"We remark that $f(7) = 3$. That $f(7) \geq 3$ follows from the left hand side of the inequality above while $f(7) \leq 3$ is obtained by considering the directed graph on $1, 2, \ldots, 7$ in which $i \to j$ iff the number $i - j$ is a quadratic residue* $\pmod 7$.*"* And at $q = 27$ it gives 5: the Paley tournament of order 27 has no transitive subtournament of order 6. That is the tournament the directed-Ramsey literature writes ST_{27}, around which Sánchez-Flores' study of tournaments free of large transitive subtournaments [7] is organised; Neiman, Mackey and Heule [8] identify ST_3, ST_7 and ST_{27} as "the tournaments generated by quadratic residues on the appropriately-sized finite-fields" and record that the quadratic-residue tournaments on 31, 43 and 47 points all do contain a transitive 7-set — which our table gives as well.

4. Characteristic two

We record the even side only to delimit it, since it is not what we compute.

Proposition 4.1. *Let*

$$S = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \in M_3(\mathbb{F}_{17}).$$

All nineteen minors of S are nonzero — so it is full superregular, and $[\,I_3 \mid S\,]$ generates a $[6,3,4]_{17}$ MDS code — but S is not totally positive. By Theorem 5.1 no 3×3 matrix over $\mathbb{F}_{17}$ is.

So in odd characteristic "all minors are nonzero squares" is strictly stronger than "all minors are nonzero", and the gap is not a boundary phenomenon: at $q = 17$ the superregular matrices are plentiful and the totally positive ones do not exist at all.

Remark 4.2. Outside the formal development, an independent enumerator gives for the least *even* prime power admitting a totally positive matrix the values $4, 4, 8, 8, 8$ for $(2,2), \ldots, (2,6)$, 4 for $(3,3)$, and 8 for $(3,4)$, $(3,5)$ and $(4,4)$. These are the corresponding MDS values; e.g. the 3×3 case over $\mathbb{F}_4$ gives a $[6,3,4]_4$ MDS code, longer than the Reed–Solomon length $q + 1 = 5$. We state these as computations reported, not as machine-checked results.

5. The odd corner

Theorem 5.1. $p_{\min}(3,3) = 19$*: there is no 3×3 totally positive matrix over $\mathbb{F}_p$ for $p \in \{3, 5, 7, 11, 13, 17\}$, and*

$$W_{3,3} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 5 & 6 \\ 1 & 6 & 17 \end{pmatrix} \in M_3(\mathbb{F}_{19})$$

is totally positive.

This value is not new: it is determined by the data in [1], whose scan gives $|\mathrm{TP}_{3,3}(\mathbb{F}_q)| = 0$ for odd $q \leq 17$ and which prints a nonzero count at $q = 19$. What Theorem 5.1 adds is an independent derivation of both halves, obtained from the definitions rather than from that scan, together with an explicit witness — and the witness is what makes Theorem 7.3 below possible.

The next three are the new cells.

Theorem 5.2. $p_{\min}(3,4) = 31$*: there is no 3×4 totally positive matrix over $\mathbb{F}_p$ for any odd prime $p \leq 29$, and the matrix in $M_{3,4}(\mathbb{F}_{31})$ with rows $(1,1,1,1)$, $(1,8,5,2)$, $(1,5,9,10)$ is totally positive.*

Theorem 5.3. $p_{\min}(4,4) = 31$*: there is no 4×4 totally positive matrix over $\mathbb{F}_p$ for any odd prime $p \leq 29$, and the symmetric matrix*

$$W_{4,4} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 8 & 5 & 2 \\ 1 & 5 & 9 & 10 \\ 1 & 2 & 10 & 20 \end{pmatrix} \in M_4(\mathbb{F}_{31})$$

is totally positive: all sixty-nine of its minors are nonzero squares modulo 31.

Theorem 5.4. $p_{\min}(3,5) = 31$*: there is no 3×5 totally positive matrix over $\mathbb{F}_p$ for any odd prime $p \leq 29$, and the matrix in $M_{3,5}(\mathbb{F}_{31})$ with rows $(1,1,1,1,1)$, $(1,8,5,2,9)$, $(1,5,9,10,19)$ is totally positive.*

The witness of Theorem 5.2 is the leading 3×4 submatrix of $W_{4,4}$, so Lemma 2.3 makes the existence halves of Theorems 5.2 and 5.3 one computation. The non-existence halves of all three rest on the same nine searches, as §6 explains.

Remark 5.5. All nine values of $p_{\min}$ in the table of §1 are $\equiv 3 \pmod 4$, and in this range $p_{\min}$ depends only on $m+n$:

$$m+n = 4,5,6,7,8 \longmapsto 7,\ 11,\ 19,\ 31,\ 31.$$

Outside the formal development the same enumerator, run over odd prime *powers* rather than primes, returns these same values and continues $m+n = 9, 10 \mapsto 59, 59$, realised at $(2,7)$, $(4,5)$ and $(5,5)$; and the odd prime powers $9, 25, 27, 49$ change none of the nine entries above. We have no proof of either pattern and offer none.

6. The search, and what it rests on

The non-existence halves of Theorems 5.1–5.4 are exhaustive computations. This section says exactly which, and why they are complete.

Reduction. By Lemma 2.2 it suffices to refute the *elementary* matrices of the shape, so the free data of an $m\times n$ candidate is the $(m-1)(n-1)$ entries b_{ij} with $i, j \geq 2$. By the paragraph before Proposition 2.5, each of them lies in D_p. So the search space has size $|D_p|^{(m-1)(n-1)}$, and by Proposition 2.5 that is at most $6^6 = 46\,656$ for every shape and prime we sweep — against $p^{(m-1)(n-1)} = 29^6 \approx 5.9\times 10^8$ without the pruning, and p^{mn} without the normal form.

The guard is the whole condition. For each shape the remaining minors — those of order ≥ 2 that are not of the form $B_{\{1,i\},\{1,j\}}$ — are assembled into one Boolean conjunction of the free entries, evaluated left to right so that the cheapest and most discriminating tests short-circuit first. The conjunct counts are $0, 1, 3, 6$ for the shapes $(2,2), (2,3), (2,4), (2,5)$, 6 for $(3,3)$ and 16 for $(3,4)$. Together with membership in D_p these account for every minor of the shape: the 3×3 matrix has 19 minors, of which 9 are entries, 4 are the border minors $b_{ij}-1$, and 6 remain; the 3×4 matrix has 34, of which 12 are entries, 6 are border minors, and 16 remain. The guard is therefore not a heuristic prefilter but the exact condition, and it is used only in the necessary direction: from "B is elementary and totally positive" we deduce "the guard holds of its free entries", and a search finding no tuple satisfying the guard refutes every elementary totally positive matrix of that shape.

What was actually enumerated. Fifteen searches, listed by the shape and prime at which they were run directly:

shape	primes swept directly	tuples enumerated
$(2,2)$	$3, 5$	0, 0
$(2,3)$	7	1
$(2,4)$	$11, 13, 17$	8, 8, 27
$(2,5)$	$19, 23, 29$	256, 625, 1296
$(3,3)$	$11, 13, 17$	16, 16, 81
$(3,4)$	$19, 23, 29$	4096, 15 625, 46 656

That is 68 711 tuples in total. Every other non-existence claim in Theorems 3.2–5.4 is inherited from one of these by Corollary 2.4: for instance the nine primes $p \leq 29$ of Theorem 5.3 are covered by the $(2,2)$ sweeps at $3,5$, the $(2,3)$ sweep at 7, the $(3,3)$ sweeps at $11, 13, 17$ and the $(3,4)$ sweeps at $19, 23, 29$, since a 4×4 totally positive matrix has totally positive leading submatrices of all those shapes. Theorems 5.2 and 5.4 use the same nine. The existence halves are separate: for each witness, every minor of every order up to $\min(m,n)$ is evaluated and tested for being a nonzero square, 69 minors in the case of $W_{4,4}$.

Controls. A search of this kind is worthless if the encoded condition is weaker than the intended one, or if the search machinery accepts everything. Three checks guard against that. First, Proposition 2.5 pins the pruning set against the published Lemma 5.4. Second, the two matrices below separate the condition from its neighbours in both directions. Third, three deliberately false statements — that no 3×3 totally positive matrix exists over $\mathbb{F}_{19}$, that none of shape 3×4 exists over $\mathbb{F}_{31}$, and that the 2×2 matrix with rows $(1,1)$ and $(1,2)$ is totally positive over $\mathbb{F}_5$ — were put through the identical machinery and were all rejected by it.

Proposition 6.1. *Over $\mathbb{F}_{19}$ the matrix with rows $(1,1,1)$, $(1,5,6)$, $(1,17,7)$ is not totally positive: its order-2 minor on rows $\{2,3\}$ and columns $\{1,2\}$ equals 12, which is nonzero and not a square modulo*

19. *Of the nineteen minors of this matrix that one is the only failure; the count of failures is reported here, not part of the formal statement.*

Proposition 6.2. *Over* $\mathbb{F}_{19}$ *the matrix with rows* $(7,9,6)$*,* $(4,4,7)$*,* $(11,17,11)$ *is totally positive and is not elementary. It is the image of* $W_{3,3}$ *of Theorem 5.1 under the scaling of Lemma 2.1 with row factors* $(4,5,9)$ *and column factors* $(16,7,11)$*, all six of which are squares modulo* 19*.*

Proposition 6.2 is the non-vacuity check for Lemma 2.2: without that lemma, a search over elementary matrices would say nothing about matrices such as this one, which is what the sweeps must in fact exclude.

7. Two corrections

7.1. **The six printed counts.** Proposition 5.2 of [1] asserts $|\mathrm{TP}_{m,n}(\mathbb{F}_q)| = r\cdot|\mathbb{F}_q^+|^{m+n-1}$, so $|\mathbb{F}_q^+|^{m+n-1}$ divides $|\mathrm{TP}_{m,n}(\mathbb{F}_q)|$; for 3×3 over odd q the divisor is $((q-1)/2)^5$ and for 3×4 over even q it is $(q-1)^6$. Every one of the six counts printed in §5.1 of [1] fails this.

Theorem 7.1. *None of* 9^5*,* 11^5*,* 12^5*,* 7^6*,* 15^6*,* 31^6 *divides, respectively,* $9\,904\,396$*,* $38\,618\,058$*,* $58\,593\,750$*,* $1\,200$*,* $2\,075\,472$*,* $415\,217\,040$*. Moreover*

$$9\,904\,396 = 4\cdot19^5,\qquad 38\,618\,058 = 6\cdot23^5,\qquad 58\,593\,750 = 6\cdot25^5,$$

and

$$4\cdot9^5 = 236\,196,\quad 6\cdot11^5 = 966\,306,\quad 6\cdot12^5 = 1\,492\,992,$$
$$1200\cdot7^6 = 141\,178\,800,\qquad 2\,075\,472\cdot15^6 = 23\,640\,923\,250\,000.$$

The six non-divisibilities are the correction; the identifications that follow them are our reading of where the discrepancy comes from, and we state them as such. For the three odd-q 3×3 values, the printed number equals $r\cdot q^5$ rather than $r\cdot((q-1)/2)^5$, with $r=4,6,6$ — and $r=4,6,6$ are exactly the leading factors 2^2, $2\cdot3$, $2\cdot3$ that [1] itself prints in its factorisations, and are the numbers of elementary totally positive 3×3 matrices over $\mathbb{F}_{19},\mathbb{F}_{23},\mathbb{F}_{25}$. For the three even-$q$ 3×4 values, the printed number is r itself, with the factor $(q-1)^6$ omitted. We reproduced $r=1200$ over $\mathbb{F}_8$ and $r=2\,075\,472$ over $\mathbb{F}_{16}$ from the definitions with an independently written enumerator, which is how the second identification was found; the $\mathbb{F}_{32}$ value $415\,217\,040$ fits the same pattern but was not re-derived here, and the corrected value for it is therefore not asserted. Nothing in the qualitative use [1] makes of these numbers is affected — in particular, that a 3×3 totally positive matrix over $\mathbb{F}_{19}$ exists, which Theorem 5.1 confirms. We found no fault with Proposition 5.2 or Lemma 5.4 themselves: $|\mathrm{TP}_{2,2}(\mathbb{F}_q)|$ agrees with $r\cdot|\mathbb{F}_q^+|^3$ by brute force over all q^4 matrices for the twelve prime powers $q\le19$; $|\mathrm{TP}_{3,3}(\mathbb{F}_4)|=486$ over all 4^9 matrices, as Lemma 5.4's even-q formula predicts; and that formula's value $24\,206$ at $q=16$ is the elementary 3×3 count we get there.

The first of the corrected values can be pinned down from inside the formal development.

Proposition 7.2. *Over* $\mathbb{F}_{19}$ *there are at most four elementary totally positive* 3×3 *matrices, and their off-border entries* $(b_{22},b_{23},b_{32},b_{33})$ *lie among*

$$(17,7,7,5),\quad (6,17,17,5),\quad (17,5,5,6),\quad (5,6,6,17).$$

Consequently the value of $|\mathrm{TP}_{3,3}(\mathbb{F}_{19})|$ *consistent with Proposition 5.2 of* [1] *is at most* $4\cdot9^5=236\,196$*.*

All four tuples are symmetric ($b_{23}=b_{32}$), and the last is $W_{3,3}$ of Theorem 5.1. That the count is exactly four, and not merely at most four, follows from the completeness of the guard, and is confirmed by two independent enumerators; only the upper bound is formally proved.

7.2. **The ordering assumption in the proof of Proposition 5.6.** The $q\equiv3\pmod 4$ half of the proof of Proposition 5.6 in [1] begins, verbatim:

> Now consider the case when $q\equiv3\pmod 4$. Let $X=\{x_1,x_2,\dots,x_k\}$ be a ordered subset of positive elements such that x_i-1 is positive for all i, and x_j-x_i is positive whenever $j>i$. Suppose $A=(a_{i,j})_{m\times n}$ is an elementary totally positive matrix. For $i\in[2,m]$ and $j\in[2,m]$, the submatrix $A_{[\{1,i\},\{1,j\}]}$ is totally positive; hence $a_{i,j}\in X$.

It then defines $f(i,j) = \ell$ when $a_{i,j} = x_\ell$, derives $f(i,j) \geq i + j - 3$, concludes $m + n \leq k + 3$, and finishes with $k \leq (q-3)/4$ — the size of the whole double-positive set D_q, by Lemma 5.4. For that chain to close, X must be all of D_q and D_q must be totally ordered by "the difference is positive". At $q = 19$ it is not.

Theorem 7.3. *In $\mathbb{F}_{19}$ the elements $6-5$, $17-6$ and $5-17$ are nonzero squares while $17-5$ is not; and $5, 6, 17$ are exactly the off-border entries of the totally positive matrix $W_{3,3}$ of Theorem 5.1.*

So $D_{19} = \{5, 6, 7, 17\}$ carries the directed 3-cycle $5 \to 6 \to 17 \to 5$, and no ordered set X of the kind the proof uses contains $\{5, 6, 17\}$: any linear order on those three elements has a backward step whose difference is not positive. In particular the function f cannot be defined for $W_{3,3}$, and the argument as written does not apply to it.

We state the consequence as narrowly as it is: this is a defect in a proof, not a counterexample to a statement. The inequality of Proposition 5.6 — $q \geq 4(m+n) - 9$ for $q \equiv 3 \pmod 4$ — holds in every case computed here, and is tight twice, at $(2,2)$ with $q = 7$ and at $(2,3)$ with $q = 11$. Nothing above refutes it. What the example shows is that a different argument is needed, and Remark 5.5 suggests the truth is some distance from the bound: at $m + n = 8$ the bound gives $q \geq 23$ and the answer is 31.

8. Verification

Every numbered theorem, proposition, lemma and corollary above has been machine-checked in Lean 4 [11] against Mathlib [12], with the exceptions and caveats stated here. The development is three files. The first carries the definitions and Lemmas 2.1–2.3 with Corollary 2.4, over an arbitrary finite field, with no appeal to compiled evaluation; the second defines the double-positive set, the free-entry map and the per-shape guards, and proves that the guard is implied by total positivity and that a guard-free search refutes the shape, again with no compiled evaluation; the third runs the fifteen searches and the witness checks of §6 and states the results. Everything in the first two files has the standard axiom closure (`propext`, `Classical.choice`, `Quot.sound`), and so do Theorem 7.3 and Proposition 6.1; Theorem 7.1, being pure arithmetic on integers, uses `propext` alone. Each of the fifteen searches and each of the seven witness checks carries in addition exactly one named axiom recording a compiled evaluation of a finite computation, and the cell theorems inherit the axioms of the searches and witnesses they invoke — ten apiece for Theorems 5.2–5.4. Propositions 4.1, 6.2 and 7.2 each rest on one such compiled evaluation, and Proposition 2.5 on ten, one per prime. Four things above are outside the formal development and are labelled where they occur: Proposition 3.1 and its consequence in Remark 3.3, which are paper arguments together with a computation of maximal chain lengths; the even-characteristic values of Remark 4.2 and the odd prime powers of Remark 5.5, which come from an independently written enumerator that validates its own field arithmetic by exhaustion before use; the identification of the three even-q counts in Theorem 7.1 as elementary counts, of which the $\mathbb{F}_8$ and $\mathbb{F}_{16}$ cases were reproduced and the $\mathbb{F}_{32}$ case was not; and the four tuples listed in Proposition 7.2, which are the value of a compiled evaluation and are not named inside the checked statement — what is checked there is that the filtered list has length four and that every elementary totally positive matrix maps into it injectively. We reproduced those four tuples with an independent enumerator. Two readings of formal statements are also worth separating out: the coding-theoretic gloss on Proposition 4.1 (that $[\, I_3 \mid S \,]$ generates an MDS code) is the standard consequence of all minors being nonzero and is not itself part of the checked statement; and in Proposition 6.1 the checked statement is only that the matrix is not totally positive, the Lean proof deriving that from the named order-2 minor, while the value 12 of that minor and the count of failing minors are reported here. There is no `sorry` anywhere in the development. Repository reference to be added at submission.

9. What remains

The Question of [1] asks for the least prime *power*. We answer for primes; the odd prime powers $9, 25, 27, 49$ were checked outside the formal development and change none of the nine values, and the source's own scan covers $q = 9$ among the odd $q \leq 17$. Carrying those into the formal development is a matter of building the fields concretely, not of compute. The shapes $(2,7)$, $(4,5)$ and $(5,5)$ have minimal odd prime power 59 by the same outside enumerator; the encoding used here enumerates $|D_p|^{(m-1)(n-1)}$ tuples, and $|D_{53}| = 12$, so at $p = 53$ that is 12^{12} for $(4, 5)$ and 12^{16} for $(5, 5)$. Those cells need a search that builds candidate rows as Paley chains rather than entry by entry. Beyond that, three questions seem worth asking. Is $p_{\min}(m, n)$ really a function of $m + n$ alone, and if so for how long? Is every $p_{\min}(m, n)$ congruent to 3 modulo 4 — equivalently, is the Paley tournament always a better host for these configurations than the Paley graph? And is there an argument, rather than a search, that separates 31 from 19 and 23 at $m + n = 7$? Proposition 5.6 of [1], once its $q \equiv 3 \pmod 4$ case is reproved, gives $q \geq 19$ there; the true answer is 31, so the missing factor is not small.

References

[1] A. Ayyer and S. Prasad, *Positive definite, positive semidefinite and totally positive matrices over finite fields*, arXiv:2608.17702v1 [math.RA] (18 August 2026). All quotations, result numbers and printed values are from this e-print, which as of 3 September 2026 is its only version and carries no journal reference.

[2] J. Cooper, E. Hanna and H. Whitlatch, *Positive-definite matrices over finite fields*, Rocky Mountain J. Math. **54** (2024), no. 2, 423–438; DOI 10.1216/rmj.2024.54.423. The source of the notion of a positive element used throughout, cited as [CHW24] in [1].

[3] R. M. Roth and G. Seroussi, *On generator matrices of MDS codes*, IEEE Trans. Inform. Theory **31** (1985), no. 6, 826–830; DOI 10.1109/TIT.1985.1057113.

[4] P. Almeida and D. Napp, *Superregular matrices over small finite fields*, arXiv:2008.00215 [math.CO] (1 August 2020). The sentence quoted in §1 for the terms *superregular* and *full superregular* is from its abstract; its introduction states the equivalence used here, that "a systematic generator matrix $G = [I \mid B]$ generates a maximum distance separable (MDS) block code if and only if B is full superregular".

[5] OEIS Foundation Inc., *The On-Line Encyclopedia of Integer Sequences*, sequence A320757: "For p the n-th prime congruent to 1 (mod 4), a(n) is the clique number of the quadratic residue (Paley) graph over F_p, the field of order p", contributed by J. F. Alm, 20 October 2018; `https://oeis.org/A320757`.

[6] P. Erdős and L. Moser, *On the representation of directed graphs as unions of orderings*, Magyar Tud. Akad. Mat. Kutató Int. Közl. (Publ. Math. Inst. Hungar. Acad. Sci.) **9** (1964), 125–132; the journal name is in use in both the Hungarian and the English form. The passage quoted in Remark 3.3 is on p. 127 of the scan in the Erdős archive of the Alfréd Rényi Institute, `users.renyi.hu/~p_erdos/1964-22.pdf`, which is what we read.

[7] A. Sánchez-Flores, *On tournaments free of large transitive subtournaments*, Graphs Combin. **14** (1998), no. 2, 181–200; DOI 10.1007/s003730050025.

[8] D. Neiman, J. Mackey and M. Heule, *Tighter bounds on directed Ramsey number $R(7)$*, Graphs Combin. **38** (2022), no. 5, paper no. 156; DOI 10.1007/s00373-022-02560-5. The text quoted in Remark 3.3 is from arXiv:2011.00683v2 [math.CO], which is the version we read.

[9] J. Machacek, *A finite totally nonnegative Grassmannian*, arXiv:2410.06177 [math.CO] (v1, 8 October 2024; v2, 27 October 2025). The closest relative we found: the same notion of positivity, and a totally positive finite Grassmannian, but constraining only the maximal minors and computing no minimal q. It is not cited by [1].

[10] D. Guillot, H. Gupta, P. K. Vishwakarma and C. H. Yip, *Positivity preservers over finite fields II*, arXiv:2608.18978 [math.RA] (19 August 2026). The only work we found citing [1]; it concerns entrywise positivity preservers and does not discuss totally positive matrices or minimal q.

[11] L. de Moura and S. Ullrich, *The Lean 4 theorem prover and programming language*, in: Automated Deduction — CADE 28, Lecture Notes in Computer Science 12699, Springer, 2021, 625–635; DOI 10.1007/978-3-030-79876-5_37.

[12] The mathlib Community, *The Lean mathematical library*, in: Proceedings of the 9th ACM SIGPLAN International Conference on Certified Programs and Proofs (CPP 2020), ACM, 2020, 367–381; DOI 10.1145/3372885.3373824.