EXCEPTIONAL PRIMES FOR KATRE'S MDS CONJECTURE ON THE JACOBI-SUM MATRIX D, AND A RANK-DROP CRITERION FREE OF JACOBI SUMS

KOREA SUPERINTELLIGENCE LABS

Abstract. Let l be an odd prime, $p \equiv 1 \pmod{l}$ a prime, γ a generator of $\mathbb{F}_p^\times$, and let $J(1,1)_l = \sum_i a_i \zeta_l^i$ be the Jacobi sum of order l attached to γ. Katre and Rajwade's condition (vi), the condition that pins down which conjugate of $J(1,1)_l$ belongs to γ, becomes after expansion a system of $l-1$ congruences modulo p that is *linear* in the $(l-1)/2$ unknowns $b, b^2, \dots, b^{(l-1)/2}$, where $b = \gamma^{(p-1)/l}$; write D for its $(l-1) \times (l-1)/2$ coefficient matrix. Katre has conjectured that any $(l-1)/2$ rows of D are linearly independent apart from finitely many p, so that D^{T} generates an MDS $[\,l-1, (l-1)/2\,]$ code. Katre and Jadhav proved this for $l = 3$ and $l = 5$ and reported, in one sentence and without data, a failure at $(p,l) = (79,13)$. We certify that failure and supply the data: exactly two of the twelve conjugates fail, $b = 62$ and $b = 65 = 62^{-1}$, and they fail by a *rank collapse*, $\operatorname{rank} D = 5 < 6$, so that all $\binom{12}{6} = 924$ maximal minors vanish at once; explicit kernel vectors are given. We then exhibit thirteen further exceptional pairs (p,l), which we did not find in the literature, reaching $l = 101$ and $p = 593141$; each is again a certified rank collapse, at a pair of conjugates $\{b, b^{-1}\}$ inverse to one another. We verify the conjecture for $l = 7, 11, 13$ on windows by exhaustive enumeration of all maximal minors. We also prove, for $q = p$, that $\operatorname{rank}_{\mathbb{F}_p} D < (l-1)/2$ if and only if an explicit determinant $\Delta(b)$ vanishes, where Δ is a function of (p, l, b) alone and involves no Jacobi sum; it costs $O(l^3)$ against $O(p \log p)$, and we machine-check its agreement with the Jacobi-sum rank cell by cell on a census window. Outside the formal development, wider sweeps and a divergence heuristic suggest that the exceptional set is infinite for every $l \geq 7$, with counting function $\asymp \log\log N$, so that the conjecture's clause "except possibly for finitely many primes p" is heuristically false. Every theorem below is machine-checked in Lean 4 except the criterion itself, whose proof is by hand.

1. Introduction

1.1. **Which MDS conjecture this is not.** "The MDS conjecture" almost always names Segre's conjecture: for $4 \leq k \leq q-3$, a linear MDS code over $\mathbb{F}_q$ of dimension k has length at most $q+1$; equivalently, an arc of $\mathrm{PG}(k-1, q)$ has at most $q+1$ points [8]. The dimensions left out, $k \in \{3, q-1\}$ with q even, are exactly the ones carrying the hyperoval codes of length $q+2$. Ball proved the conjecture when q is prime [7]. The name sometimes instead attaches to the GM-MDS conjecture of Dau, Song and Yuen, about generator matrices with prescribed zero patterns. The conjecture studied here is neither. It is a conjecture of S. A. Katre about one explicit matrix built from Jacobi sums, stated in [1]. The vocabulary overlaps completely and the content not at all, so we say so at the outset.

1.2. **The matrix.** Fix an odd prime l, a prime $p \equiv 1 \pmod{l}$ and $q = p^\alpha$. Everything in this paper takes $\alpha = 1$, that is $q = p$, which is where the failure reported in [1] lives — that report is about "generators of $\mathbb{F}_p^\times$".

Let $\zeta = \zeta_l$ be a primitive complex l-th root of unity, let γ generate $\mathbb{F}_p^\times$, put $b = \gamma^{(p-1)/l}$ — a primitive l-th root of unity *modulo* p — and let χ be the multiplicative character of order l on $\mathbb{F}_p^\times$ with $\chi(\gamma) = \zeta$. Write the Jacobi sum of order l in the normalisation of [1],

$$J(1,1)_l = \sum_{v \neq 0, -1} \chi(v)\chi(v+1) = \sum_{i=0}^{l-1} N_i \zeta^i = \sum_{i=1}^{l-1} a_i \zeta^i, \qquad a_i = N_i - N_0, \tag{1}$$

where $N_i = \#\{v : \operatorname{ind} v + \operatorname{ind}(v+1) \equiv i \pmod{l}\}$ and ind is the index relative to γ; the normalisation $a_0 = 0$ is legitimate because $1 + \zeta + \cdots + \zeta^{l-1} = 0$. Katre and Rajwade's condition (vi) of [2], the last of the conditions (i)–(vi) that determine the cyclotomic numbers of order l uniquely, reads in the case $n = 1$

$$p \,\Big|\, \overline{H} \prod_{k=1}^{(l-1)/2} \big(b - \zeta^{k^{-1}}\big), \qquad H = \sum_i a_i \zeta^i, \tag{2}$$

the inverses k^{-1} being taken modulo l. It is condition (vi) that resolves the classical ambiguity of cyclotomy: the conditions (i)–(v) determine $J(1,1)_l$ only up to conjugacy, and (vi) says which conjugate goes with which generator γ.

Write $m = (l-1)/2$ and expand the left-hand side of (2) as a polynomial in the indeterminate T over $\mathbb{Z}[\zeta]$,

$$E(T) = \overline{H} \prod_{k=1}^{m} \big(T - \zeta^{k^{-1}}\big) = \sum_{i=0}^{l-1} c_i(T)\, \zeta^i, \qquad c_i \in \mathbb{Z}[T],\ \deg c_i \le m. \tag{3}$$

Rewriting in the $\mathbb{Z}$-basis $\zeta, \zeta^2, \ldots, \zeta^{l-1}$ of $\mathbb{Z}[\zeta]$ — that is, substituting $1 = -(\zeta + \cdots + \zeta^{l-1})$ — turns (2) into the $l - 1$ congruences

$$c_i(b) - c_0(b) \equiv 0 \pmod{p}, \qquad i = 1, \ldots, l-1, \tag{4}$$

and these are *linear* in $b, b^2, \ldots, b^m$. Let $D = D(p, l, b)$ be their $(l-1) \times m$ coefficient matrix and $Y = Y(p, l, b)$ their column of constant terms:

$$D_{ij} = \big[T^j\big]\big(c_i - c_0\big), \qquad Y_i = c_i(0) - c_0(0), \qquad 1 \le i \le l-1,\ 1 \le j \le m, \tag{5}$$

so that, by construction,

$$D \cdot (b, b^2, \ldots, b^m)^{\mathsf{T}} + Y \equiv 0 \pmod{p}. \tag{6}$$

The transpose D^{T} is an $m \times (l-1)$ matrix over $\mathbb{F}_p$ and generates a linear $[\,l-1,\, m\,]$ code, which [1] calls a *Gauss–Dickson code*. By the standard characterisation of MDS codes — a q-ary linear $[n, k]$ code is MDS if and only if every k columns of a generator matrix are linearly independent [6], which is Proposition 4.2 of [1] — that code is MDS, with parameters $[\,l-1,\, m,\, m+1\,]$, exactly when every m rows of D are linearly independent over $\mathbb{F}_p$. For $l = 3$ this is a $[2, 1, 2]$ code (the Gauss case) and for $l = 5$ a $[4, 2, 3]$ code (the Dickson case).

1.3. **The conjecture, and what was known.**

[1, §3] states, verbatim:

> **Conjecture (S. A. Katre).** Any $\frac{l-1}{2}$ rows of D are linearly independent, except possibly for finitely many primes p, and D^t is a generator matrix of an MDS code over F_q.

[1] proves this for $l = 3$ (§4) and $l = 5$ (Theorem 5.2), recording that these two orders had been verified earlier by Katre in his thesis, and for higher orders says only that "It is expected that these results can be carried forward for higher values of l, however the calculations become laborious even using a software". Its "Future Scope" section reports, in a single sentence and with no data:

> Vikas Jadhav and Katre have observed that for $p = 79$ and $l = 13$, we do not get MDS codes for certain generators of $\mathbb{F}_p^*$, however for other $p \equiv 1 \pmod{13}$ we get MDS codes. Thus there is a possibility of exceptional primes for the conjecture in §3.

That is the whole of what is on record: two proved orders, one reported exceptional pair without its data, and no verification at all for $l \ge 7$. We found no later work on the question. The searches behind that statement are summarised in §7; read them as "not found", not as "does not exist".

1.4. **Parametrisation by b.** The character χ is determined by b alone: $\chi(v) = \zeta^{c(v)}$, where $c(v)$ is the unique $c < l$ with $b^c = v^{(p-1)/l}$ in $\mathbb{F}_p$. As γ runs over the generators of $\mathbb{F}_p^\times$, b runs over the $l-1$ primitive l-th roots of unity modulo p, and distinct b give the $l-1$ conjugates of $J(1,1)_l$. So "for certain generators of $\mathbb{F}_p^\times$" in the quotation above means "for certain b", there are exactly $l-1$ matrices D per pair (p,l), and a *cell* of the problem is a triple (l,p,b). We call (p,l) an *exceptional pair* when at least one of its $l-1$ cells fails to give an MDS code. All statements below are indexed by b.

1.5. **Results.**

(1) *The reported exception, certified with its data* (Theorem 3.1). At $(p,l) = (79,13)$ exactly two of the twelve conjugates fail, $b = 62$ and $b = 65$, an inverse pair; each fails by a rank collapse, $\operatorname{rank}_{\mathbb{F}_{79}} D = 5 < 6$, so that all $\binom{12}{6} = 924$ maximal minors vanish simultaneously; the 924 vanishings are enumerated, and explicit right and left kernel vectors are exhibited.

(2) *Thirteen further exceptional pairs* (Theorems 3.2 and 3.3), from $(277,23)$ to $(593141,47)$ and up to $l = 101$. In every one the rank of D is exactly one short of full at a pair of conjugates b, b^{-1} inverse to one another. Together with (1) this certifies a failure at every one of the fourteen exceptional pairs found by the sweeps of §6.

(3) *The conjecture for the next three orders* (Theorem 4.1): $l = 7$ for every prime $p \equiv 1 \pmod 7$ with $p \le 5000$, $l = 11$ and $l = 13$ for every prime $p \le 3000$, by exhaustive enumeration of every one of the $\binom{l-1}{m}$ maximal minors at every conjugate. At $l = 13$ the exceptional set in the window is exactly $\{79\}$.

(4) *A rank-drop criterion free of Jacobi sums* (Theorem 5.1): for $q = p$, $\operatorname{rank}_{\mathbb{F}_p} D < m$ if and only if $\Delta(b) = 0$, where Δ is an explicit $m \times m$ determinant depending on (p,l,b) alone. It is machine-checked against the Jacobi-sum rank cell by cell on a census window (Theorem 5.2) and yields the complete list of exceptional pairs for $p \le 20000$, $3 \le l \le 47$ (Theorem 5.3).

(5) Outside the formal development (§6): wider sweeps, in which every failure ever observed is a rank drop by exactly one at exactly an inverse pair; and a heuristic predicting $\asymp \log\log N$ exceptional primes per order, which would make the conjecture's finiteness clause false for every $l \ge 7$.

2. Reconstruction of the matrix, and controls

The reduction from (2) to (5) involves one choice that [1] does not record: which $\mathbb{Z}$-basis of $\mathbb{Z}[\zeta]$ the congruence is read in. We derived the convention above — coordinates $\zeta, \dots, \zeta^{l-1}$, hence the differences $c_i - c_0$ — and then checked it against everything [1] prints. Nothing later in this paper was believed before that check passed.

Theorem 2.1 (the printed data of [1], reproduced)**.** *Let D, Y be as in* (5)*, built from the definitions* (1)–(3)*.*

(1) (The worked example of [1, §5].) *For $p = 61$, $l = 5$, $\gamma = 2$ one has $b = 2^{12} = 9$, $(N_0, \dots, N_4) = (12,12,6,15,14)$ and $J(1,1)_5 = -6\zeta^2 + 3\zeta^3 + 2\zeta^4$, and*

$$D^{\mathsf{T}} = \begin{pmatrix} 9 & 1 & 0 & 7 \\ 2 & 3 & 55 & 0 \end{pmatrix}, \qquad Y = (1, 53, 59, 59)^{\mathsf{T}},$$

and the code is MDS. The Jacobi sum and D^{T} are printed in [1] *verbatim; N and Y are not, and follow from the general formulas of part (2).*

(2) (The general matrices of [1].) *For every one of the four conjugates of every prime $p \equiv 1 \pmod 5$ with $p \le 400$,*

$$D = \begin{pmatrix} a_1 - a_2 + a_3 & a_4 \\ a_3 - a_4 & a_3 \\ a_1 & a_2 \\ a_1 - a_2 + a_3 - a_4 & a_1 \end{pmatrix}, \qquad Y = (a_3 - a_4,\ a_2 - a_4,\ a_1 - a_4,\ -a_4)^{\mathsf{T}},$$

the matrix and the constants of the equations (I)–(IV) *of* [1, §5]*; and for both conjugates of every prime* $p \equiv 1 \pmod 3$ *with* $p \le 300$*,* $D = (a_2, a_1)^{\mathsf{T}}$ *and* $Y = (a_1,\, a_1 - a_2)^{\mathsf{T}}$*, the two congruences of* [1, §4]*. The two ranges hold* 17 *and* 28 *primes respectively.*

(3) (The consistency identity.) *Congruence* (6) *holds at every conjugate of every prime* $p \equiv 1 \pmod l$ *with* $p \le 150$*, for* $l = 3, 5, 7, 11$*.*

(4) (Remark 5.1 of [1], the conjugate solutions.) $N_i^{(b^t)} = N_{ti}^{(b)}$ *for every* $t \not\equiv 0$*, at every conjugate of every prime* $p \equiv 1 \pmod l$ *with* $p \le 150$*, for* $l = 5, 7$*.*

Part (3) is the sharpest of these and is used throughout as a non-vacuity control: it says that the matrix really is the coefficient matrix of the system (4) and that $(b, \dots, b^m)$ really solves it. A wrong basis convention, a wrong half-system $\{k^{-1}\}$, a wrong normalisation of a_0 or an off-by-one in the ζ-indexing all break it; two such conventions were caught by it during development.

Theorem 2.2 (the proved orders, as a finite census)**.** *For* $l = 3$ *and for* $l = 5$*, every conjugate of every prime* $p \equiv 1 \pmod l$ *with* $p \le 600$ *gives an MDS code: no exceptional prime occurs in either window, which holds* 50 *and* 25 *primes respectively.*

Theorem 2.2 is a finite instance of what [1] proves in general, and is kept as the positive control that the census machinery agrees with a proved case.

Proposition 2.3 (negative controls)**.** *With* $p = 79$*,* $l = 13$*:*

(1) *the too-large claim "every conjugate at every* $p \equiv 1 \pmod{13}$ *is MDS" is false — the cell* $b = 62$ *refutes it;*

(2) *the too-small claim "the prime* 79 *fails outright" is false — ten of the twelve conjugates have* $\operatorname{rank} D = 6$*, and at* $b = 18$ *all* 924 *minors are nonzero;*

(3) *the test is sensitive to the data in both directions: adding* 1 *to a single entry of the exceptional matrix* $D(79, 13, 62)$ *restores* $\operatorname{rank} D = 6$ *(checked at two different positions), and adding* 1 *to the entry* $(0, 0)$ *of the good matrix* $D(79, 13, 18)$ *creates seven singular maximal minors and destroys the MDS property;*

(4) *a wrong index set is nonsingular: at* $b = 18$ *both the first six rows of* D *and the rows* $\{0, 2, 4, 6, 8, 10\}$ *have nonzero determinant;*

(5) *the hypothesis is not vacuous:* 62 *is a primitive* 13*-th root of unity modulo* 79*,* 1 *is not, and there are exactly twelve of them.*

These are controls, not results. They exist because "all 924 minors vanish" is exactly the shape of assertion that a mistaken construction of D would also produce. Part (3) carries one representative perturbation in each direction; measured outside the formal statement, 71 of the 72 single-entry $+1$ perturbations of $D(79, 13, 18)$ break the MDS property.

3. Certified exceptional pairs

3.1. The reported pair $(79, 13)$.

Theorem 3.1. *Let* $p = 79$*,* $l = 13$*,* $m = 6$*. Of the twelve primitive* 13*-th roots of unity modulo* 79*, exactly two give a failure of Katre's conjecture, namely* $b = 62$ *and* $b = 65$*, and these are an inverse pair,* $62 \cdot 65 \equiv 1 \pmod{79}$*. At each of them the failure is total:*

$$\operatorname{rank}_{\mathbb{F}_{79}} D(79, 13, b) = 5 < 6,$$

so that every *one of the* $\binom{12}{6} = 924$ *maximal minors of* D *is singular, and no set of six rows of* D *is linearly independent. Explicit certificates: at* $b = 62$ *the vector* $\lambda = (16, 6, 59, 4, 37, 1)$ *satisfies* $D\lambda \equiv 0$ *and the vector* $\mu = (51, 20, 50, 33, 57, 1)$ *satisfies* $\mu^{\mathsf{T}} D_{\{1,\dots,6\}} \equiv 0$*; at* $b = 65$ *the vectors are* $\lambda = (59, 66, 61, 45, 17, 1)$ *and* $\mu = (23, 30, 33, 53, 56, 1)$*.*

The existence of a failure at $(79, 13)$ is the observation of [1] quoted above. What is new here is everything else: *which* generators, *how many*, and *how badly*. The distinction matters, because a code can fail to be MDS through one unlucky vanishing minor while the generator matrix still has full

rank; that is not what happens. The rank drops, so the failure is simultaneous across all 924 minors, and the left kernel vector μ is a literal linear dependence among six rows of D — the direct negation of the conjecture's clause. Translated back into the indexing [1] uses: $\mathbb{F}_{79}^{\times}$ has $\varphi(78) = 24$ generators, and $\gamma \mapsto \gamma^6$ carries them two-to-one onto the twelve conjugates, so "certain generators of $\mathbb{F}_p^*$" there means exactly four of those twenty-four.

3.2. **Two further pairs, kernel-checked.**

Theorem 3.2. *Katre's conjecture fails at $(p, l) = (277, 23)$ and at $(p, l) = (659, 47)$. Precisely:*

1. *at $p = 277$, $l = 23$, $m = 11$, exactly two of the twenty-two conjugates fail, $b = 164$ and $b = 201 = 164^{-1}$, each with $\operatorname{rank}_{\mathbb{F}_{277}} D = 10 < 11$;*
2. *at $p = 659$, $l = 47$, $m = 23$, the two conjugates $b = 14$ and $b = 612 = 14^{-1}$ fail, each with $\operatorname{rank}_{\mathbb{F}_{659}} D = 22 < 23$.*

In each case an explicit nonzero right kernel vector of D and an explicit nonzero left kernel vector of its first m rows are exhibited.

Neither pair appears in [1], which reports only $(79, 13)$, nor in any work we could find (§7). The rank certificate is what makes these statements checkable at all: the two matrices have $\binom{22}{11} = 705\,432$ and $\binom{46}{23} = 8\,233\,430\,727\,600$ maximal minors respectively, and the second number is past any enumeration, whereas a rank drop together with a kernel vector is a claim about a single matrix–vector product. The completeness clause of (1) — exactly two conjugates, out of twenty-two — is verified by computing the rank at all twenty-two. The corresponding statement for $(659, 47)$, that no third conjugate of the forty-six fails, is deliberately not in (2): it comes from the criterion census of Theorem 5.3 below together with Theorem 5.1, and so, unlike everything in the theorem itself, leans on the one theorem here that is not machine-checked.

3.3. **Eleven more.**

Theorem 3.3. *Katre's conjecture fails at each of the following eleven pairs (p, l). For each pair, at each of the two conjugates listed, one has $\operatorname{rank}_{\mathbb{F}_p} D = m - 1$, exactly one short of full, with an explicit right kernel vector of D and an explicit left kernel vector of its first m rows.*

l	p	$(p-1)/l$	m	$b,\ b^{-1}$
31	14 447	466	15	3543, 12188
41	12 547	306	20	5366, 6194
47	593 141	12 620	23	118202, 515206
53	107	2	26	49, 83
71	21 727	306	35	13250, 19410
73	293	4	36	16, 55
73	3 067	42	36	633, 1158
73	73 877	1 012	36	5217, 47637
83	167	2	41	18, 65
97	14 551	150	48	4306, 6478
101	809	8	50	298, 790

The certificates here are per conjugate; that the two conjugates in each row are inverse to one another modulo p is one modular multiplication, carried out inside the development only for the three pairs of Theorems 3.1 and 3.2. That no *third* conjugate of these eleven pairs fails is not certified either: for $(14\,447, 31)$ and $(12\,547, 41)$ it follows from Theorem 5.3 together with Theorem 5.1, and for the other nine — which fall outside the window of Theorem 5.3, either because $p > 20\,000$ or because $l > 47$ — it rests on the sweeps of §6.

Corollary 3.4. *Fourteen exceptional pairs are known: $(79, 13)$ from [1], and the thirteen of Theorems 3.2 and 3.3. For every one of them a rank drop by exactly one is certified, at a pair of conjugates $\{b, b^{-1}\}$ inverse to one another. These are all the exceptional pairs found by the sweeps of §6, which*

cover $3 \le l \le 101$ *and* $p < 10^6$ *and, for* $3 \le l \le 47$, $p < 10^7$*; in those sweeps no pair has a third failing conjugate.*

The inverse-pair phenomenon is not an accident of the search: $b \mapsto b^{-1}$ corresponds to complex conjugation of $J(1,1)_l$, so the failure set of a pair (p,l) is closed under it. What the data adds is that the failure set has never been observed to be *larger* than one such pair.

4. The conjecture for $l = 7, 11, 13$

Theorem 4.1. *Every maximal minor of $D(p,l,b)$ was evaluated over $\mathbb{F}_p$, at every one of the $l-1$ conjugates b, at every prime $p \equiv 1 \pmod{l}$ in the stated window. The set of primes at which some conjugate fails is:*

l	*window*	*primes*	*conjugates*	*minors per cell*	*exceptional primes*
7	$p \le 5000$	110	660	$\binom{6}{3} = 20$	*none*
11	$p \le 3000$	42	420	$\binom{10}{5} = 252$	*none*
13	$p \le 3000$	35	420	$\binom{12}{6} = 924$	79 *only*

The consistency identity (6) *holds at every cell of all three windows.*

We know of no earlier verification of Katre's conjecture beyond the two orders proved in [1], which says of the higher orders that "the calculations become laborious even using a software". The statement is an equality of *lists* — the list of primes at which some conjugate fails — so "none" is the strongest available form: it asserts not that no failure was found but that the filtered list is empty.

5. A rank-drop criterion free of Jacobi sums

Every failure observed anywhere in this work is a rank drop. The following theorem explains why a rank drop is much cheaper to detect than the Jacobi sum that seems to define it. It is proved by hand and is *not* part of the machine-checked development: its proof runs through the ideal factorisation of $J(1,1)_l$ quoted as Lemma 2.3 of [1], which rests on the whole Katre–Rajwade apparatus [2, 3], and no formal library we know of contains cyclotomic numbers of order l. Its machine-checked shadow is Theorem 5.2, a cell-by-cell agreement over a census window.

Theorem 5.1 (not machine-checked)**.** *Let l be an odd prime, $p \equiv 1 \pmod{l}$ a prime, $q = p$, and let b be a primitive l-th root of unity modulo p. Put $m = (l-1)/2$ and let*

$$S = \{k^{-1} \bmod l : 1 \le k \le m\}, \qquad F_j(T) = \prod_{u \in S} \big(T - b^{ju}\big) \in \mathbb{F}_p[T],$$

$$\Delta(b) = \det\Big[\, [T^i] F_j(T) \,\Big]_{1 \le j,i \le m}.$$

Then $\operatorname{rank}_{\mathbb{F}_p} D(p,l,b) < m$ if and only if $\Delta(b) = 0$.

Proof. Write $R = \mathbb{Z}[\zeta]/p$. Since $p \equiv 1 \pmod{l}$, p splits completely in $\mathbb{Q}(\zeta)$ and $R \cong \prod_{j \in (\mathbb{Z}/l)^\times} \mathbb{F}_p$, the j-th projection being $\pi_j : x \mapsto x(b^j)$, that is, evaluation of a representative polynomial at b^j. Let

$$f(T) = \prod_{u \in S} (T - \zeta^u), \qquad s_i = [T^i] f \in R,$$

so that $E(T) = \overline{H} f(T)$ has $[T^i]E = \overline{H} s_i$. Reading R in the basis $\zeta, \dots, \zeta^{l-1}$ is precisely the normalisation $c_i - c_0$ of (5), so the columns of D *are* the elements $\overline{H}s_1, \dots, \overline{H}s_m$ of R, and

$$\operatorname{rank} D = \dim_{\mathbb{F}_p} \overline{H} \cdot V, \qquad V = \operatorname{span}(s_1, \dots, s_m).$$

Now S is a half-system modulo l: the set $\{1, \dots, m\}$ meets each pair $\{\pm k\}$ exactly once, hence so does its image under $k \mapsto k^{-1}$, so $S \sqcup (-S) = (\mathbb{Z}/l)^\times$. By Lemma 2.3 of [1] (attributed there to [3, 4]),

$$\big(J(1,1)_l\big) = \prod_{k=1}^{m} \big(\mathcal{P}^{\sigma_{k^{-1}}}\big)^{\alpha},$$

where $\mathcal{P}$ is the prime of $\mathbb{Z}[\zeta]$ above p determined by $\zeta \equiv b$. With $\alpha = 1$, and taking π_1 to be the component attached to $\mathcal{P}$, the element $J(1,1)_l$ vanishes at exactly the components π_v with $v \in \{1,\dots,m\}$; hence $\overline{H}$, its complex conjugate, vanishes at exactly the components π_w with $w \in -\{1,\dots,m\}$ and is a unit at the remaining m components $\pi_1,\dots,\pi_m$. Therefore, for $\lambda \in \mathbb{F}_p^m$,

$$\sum_i \lambda_i \overline{H} s_i = 0 \text{ in } R \iff \sum_i \lambda_i \pi_j(s_i) = 0 \text{ for } j = 1,\dots,m.$$

Finally $\pi_j(f)(T) = \prod_{u\in S}(T - b^{ju}) = F_j(T)$, so $\pi_j(s_i) = [T^i]F_j$, and a nonzero such λ exists if and only if the $m \times m$ matrix $\left[[T^i]F_j\right]$ is singular, that is, $\Delta(b) = 0$. □

The point of Δ is what it does *not* contain. It involves no Jacobi sum, no cyclotomic number, no index table: it is a function of (p,l,b) alone, computable in $O(l^3)$ operations in $\mathbb{F}_p$, whereas assembling one Jacobi sum requires the cyclotomic class of every $v \in \{1,\dots,p-2\}$ and costs $O(p\log p)$. On the machines used here, the exhaustive minor census at $l = 23$ costs 16.6 seconds per prime, while the criterion sweep covers every $l \le 29$ and every $p < 5000$ in 0.15 seconds — a factor of roughly 10^6 on the rank-drop question. Theorem 5.1 is what makes the wide sweeps of §6 possible at all.

Since Theorem 5.1 is not formalised, we formalise its consequence as a finite fact, cell by cell.

Theorem 5.2. *Let $\mathcal{R}(l,B)$ be the list of pairs (p,b), $p \le B$ prime with $p \equiv 1 \pmod l$ and b a primitive l-th root of unity modulo p, at which $\operatorname{rank}_{\mathbb{F}_p} D(p,l,b) < m$, computed from the Jacobi sum; and let $\mathcal{Z}(l,B)$ be the corresponding list at which $\Delta(b) = 0$, computed from (p,l,b) alone. Then*

$$\mathcal{R}(l,B) = \mathcal{Z}(l,B) \quad \text{for } l \in \{7,11,13\},\ B = 2000, \qquad \text{and for } l \in \{17,19,23,29,31\},\ B = 1000.$$

Both sides are nonempty: in the first window the common list is $\{(79,62),(79,65)\}$ at $l = 13$ and empty at $l = 7, 11$; in the second it is $\{(277,164),(277,201)\}$ at $l = 23$ and empty at $l = 17, 19, 29, 31$. The windows are not empty either: they contain 24 primes $p \equiv 1 \pmod{13}$ and 8 primes $p \equiv 1 \pmod{23}$ respectively.

The nonvacuity clause is part of the statement, so this is not an agreement of two empty lists. It is the licence for the criterion-only sweeps that follow.

Theorem 5.3. *Let l range over the odd primes in the stated range, p over the primes $p \le 20000$ with $p \equiv 1 \pmod l$, and b over the $l-1$ conjugates. The complete list of cells with $\Delta(b) = 0$ is:*

$$\begin{aligned} 3 \le l \le 23: &\quad (l,p,b) = (13,79,62),\ (13,79,65),\ (23,277,164),\ (23,277,201);\\ 29 \le l \le 47: &\quad (31,14447,3543),\ (31,14447,12188),\ (41,12547,5366),\\ &\quad (41,12547,6194),\ (47,659,14),\ (47,659,612). \end{aligned}$$

This is a complete list, not a sample: the statement is an equality of the whole filtered list, so it says both that these cells are exceptional and that no other cell in the window is. With Theorem 5.1 it identifies the exceptional pairs of the window exactly. [1] gives one pair and no list.

6. Computations outside the formal development

The statements of this section were produced by an implementation in C and cross-checked against an independent implementation in Python; they are *not* machine-checked, and we label them as such. They are reported because they place the certified results in their range and because they are what the heuristic below is measured against. The consistency identity (6) was verified at every cell of every sweep; the census program aborts on a violation.

Remark 6.1 (wide censuses, outside the formal development). *(a) Exhaustive minor enumeration.* Every maximal minor of D, at every conjugate, at every admissible prime: for $l = 7, 11, 13$ and $p < 10^6$ (27 460 pairs, 235 426 conjugates), the only MDS failure is $(79, 13)$; for $l = 17, 19$ and $p < 10^5$ (1 128 pairs, 19 098 conjugates) there is none; for $l = 3, 5$ and $p < 10^5$ there is none.

(b) Criterion sweeps. Using Δ: for $3 \le l \le 47$ and $p < 10^7$ (950 317 pairs), 12 vanishing cells, that is 6 exceptional pairs including $(593141, 47)$; for $53 \le l \le 101$ and $p < 3 \cdot 10^5$ (3 981 pairs), 16

vanishing cells, 8 pairs; and, on the unified window $3 \le l \le 101$, $p < 10^6$ (124 131 pairs, 1 954 784 conjugates), 28 vanishing cells — exactly the fourteen pairs of Corollary 3.4 and no fifteenth.

(c) Two observations that hold throughout. In every failure found anywhere, the rank drops by exactly one, and exactly the inverse pair $\{b, b^{-1}\}$ fails. No failure at *full* rank — a vanishing maximal minor with $\operatorname{rank} D = m$ — has ever been observed, in 235 426 conjugates at $l = 7, 11, 13$, 19 098 more at $l = 17, 19$, or at any conjugate of any exceptional pair. Nothing proved here excludes one; see §9.

(d) Orders with no exception at all. In the swept ranges, the fourteen orders $l = 3$, 5, 7, 11, 17, 19, 29, 37, 43, 59, 61, 67, 79 and 89 have no exceptional prime at all.

Remark 6.2 (a divergence heuristic; not a theorem). $\Delta(b)$ is a single determinant in $\mathbb{F}_p$, so one may guess that it vanishes with probability about $1/p$, independently across cells. Since there are $l - 1$ conjugates per admissible prime, the expected number of failing conjugates with $p \le N$ would be

$$\mathbb{E}_l(N) = \sum_{\substack{p \le N \\ p \equiv 1 \ (l)}} \frac{l-1}{p} \;\approx\; \log\log N + C_l,$$

which *diverges*. Failures come in inverse pairs, so the count should behave like $2 \cdot \mathrm{Poisson}(\mathbb{E}/2)$, with standard deviation $\sqrt{2\mathbb{E}}$. Computing $\mathbb{E}_l(N)$ from the exact prime sums and comparing with the sweeps of Remark 6.1(b):

window	predicted	observed	deviation
$3 \le l \le 47$, $p < 10^7$	21.2 ± 6.5	12	-1.4σ
$53 \le l \le 101$, $p < 3 \cdot 10^5$	10.7 ± 4.6	16	$+1.2\sigma$
$3 \le l \le 101$, $p < 10^6$ (unified)	30.70 ± 7.8	28	-0.4σ

All three are ordinary fluctuations, and the largest window — the only one that is a single uniform range — sits within half a standard deviation. If the heuristic is right, the clause "except possibly for finitely many primes p" in Katre's conjecture is false for every $l \ge 7$: the exceptional set should be infinite, with counting function $\asymp \log\log N$. It would fail only just, since one expects about one new exceptional prime per order per factor e^e in N, which is why no finite computation can settle it and why [1] was right to hedge to "a possibility of exceptional primes". We stress that nothing here proves that Δ equidistributes; the agreement in the table is a consistency check, not evidence of a mechanism.

7. The extent of the computation

We state exactly which claims rest on exhaustive computation, and how large each search was.

- Theorem 5.1 rests on no computation. It is a proof, uniform in p, l and b, from Lemma 2.3 of [1]. It is the only theorem in this paper that is not machine-checked.
- Theorem 2.1 is a finite reproduction: one worked example; then all conjugates of all 17 primes $p \equiv 1 \pmod 5$, $p \le 400$, and of all 28 primes $p \equiv 1 \pmod 3$, $p \le 300$; then the consistency identity at all conjugates of all admissible primes $p \le 150$ for $l = 3, 5, 7, 11$; then Remark 5.1 for $l = 5, 7$ over the same range.
- Theorem 2.2 evaluates all $\binom{2}{1} = 2$ and $\binom{4}{2} = 6$ maximal minors at every conjugate of every admissible prime $p \le 600$: 50 primes for $l = 3$, 25 for $l = 5$.
- Theorem 3.1 enumerates all 924 maximal 6×6 minors of $D(79, 13, b)$ over $\mathbb{F}_{79}$ for $b = 62$ and $b = 65$, and computes the rank at all twelve conjugates. Proposition 2.3 is of the same size.
- Theorems 3.2 and 3.3 rest on *no* minor enumeration: each certified cell is one rank computation over $\mathbb{F}_p$ on an $(l-1) \times m$ matrix plus two matrix–vector products verifying the kernel vectors, and the completeness clause of Theorem 3.2(1) adds one rank computation at each of the twenty-two conjugates of $(277, 23)$. The number of maximal minors is irrelevant to the certificate and reaches $\binom{46}{23} = 8\,233\,430\,727\,600$; assembling D at $p = 593\,141$ is the dominant cost, being $O(p)$.

- Theorem 4.1 is the largest exhaustive claim in the paper: 1 500 conjugates in all, carrying 20, 252 and 924 maximal minors each, evaluated by a division-free subset-Laplace recursion over row bitmasks.
- Theorem 5.2 computes both sides at every cell of its two windows; Theorem 5.3 computes Δ at every cell with $p \le 20000$ for the fourteen orders $3 \le l \le 47$.
- The statements of §6 are outside the formal development. Their sizes are given in Remark 6.1; the largest are 235 426 conjugates with full minor enumeration and 1 954 784 conjugates by the criterion.
- Costs, measured. The C censuses: 16 minutes for $l = 7, 11, 13$ with $p < 10^6$, 12 minutes for $l = 17, 19$ with $p < 10^5$, 40 minutes for $l = 23$ with $p < 2 \cdot 10^4$; the criterion sweeps: 29, 9 and 32 minutes for the three windows of Remark 6.1(b). The formal development: about 17 minutes for Theorem 2.1 together with Proposition 2.3, 12 for Theorem 3.1 and Theorem 3.2, 1 to 4 minutes for each block of Theorem 3.3, about 4 for Theorem 4.1 and 13 for Theorems 5.2 and 5.3. These come to about 3.2 CPU-hours; with the Python cross-checks and two abandoned runs (§9), the family's total was about 4.5. One run is over budget and we record it: the kernel check behind Theorem 2.1 peaked at 11.3 GB of memory, because the kernel materialises the whole reduction of a list-based sweep; halving the windows in that file would bring it down.
- Cross-checking. Three independent implementations were written — Python (the arbiter, deliberately slow and direct), C (the censuses), and the formal development, which imports nothing and is list-based — and every number reported here comes from at least two of them. The fourteen exceptional pairs are a three-way agreement: found by the criterion in C, re-derived from the Jacobi sums in Python, and certified against the formally built D.
- Provenance. On 3 September 2026 the source [1] had no citing work (OpenAlex and Semantic Scholar both report a citation count of zero), no successor by either author, and no occurrence in a 72 GB local corpus of arXiv mathematics through July 2026 beyond its own record. The survey [5] of this exact area states condition (vi) and never treats D as a matrix. Read all of this as "not found".

8. Verification

Theorems 2.1, 2.2, 3.1, 3.2, 3.3, 4.1, 5.2 and 5.3 and Proposition 2.3 are machine-checked in Lean 4 [10]; Theorem 5.1 alone is a hand proof, for the reason given in §5. The development defines N_i, a_i, $E(T)$, D, Y, the maximal minors, the rank, and Δ from scratch and imports no library at all — in particular not Mathlib [11], whose treatment of Jacobi sums is at the level of [9, §8.3] and which contains neither cyclotomic numbers of order l nor any coding theory — so that the certificates reduce in the kernel rather than needing compiled evaluation. Of the 54 theorems in the development, 22 are checked by the kernel alone: 18 depend on propositional extensionality and 4 on no axiom whatever, and they comprise the whole of Theorem 2.1, Theorem 2.2, Proposition 2.3, Theorem 3.1 including the enumeration of all 924 singular minors, and Theorem 3.2. The other 32 — the twenty-two certificates of Theorem 3.3, the five of Theorem 4.1, and the five of Theorems 5.2 and 5.3 — each carry one per-declaration axiom recording a single appeal to compiled evaluation: 28 carry it together with propositional extensionality, three of those (the three census statements) also quotient soundness, and one carries the compiled-evaluation axiom alone. Compiled evaluation is used there because assembling D requires the cyclotomic class of every $v \in \{1, \dots, p-2\}$, which is $O(p)$, and because the minor recursion is array-based. There is no `sorry` anywhere in the development, and neither choice nor the reduction of compiled booleans appears: the lists above are the complete axiom closures, as printed by `#print axioms` on all 54 declarations. The development is eight modules: the definitions; the gate, the $l = 3, 5$ census and the controls; the kernel-clean certificates of Theorems 3.1 and 3.2; three blocks of compiled-evaluation certificates for Theorem 3.3; the minor census; and the criterion. The computations of §6 are outside the development entirely. Repository reference to be added at submission.

9. What remains

The full-rank gap. Theorem 5.1 decides rank drops, and every failure ever observed is a rank drop, but nothing proved here excludes a vanishing maximal minor at full rank; such a cell would be an MDS failure invisible to Δ, and would mean that the sweeps of Remark 6.1(b) are not the complete searches they appear to be. One cheap sufficient condition for a singular maximal minor at full rank is a column of D with at least m zeros, since the corresponding m rows then give a submatrix with a zero column. The last column of D, at $j = m$, is $(a_{l-1}, a_{l-2}, \dots, a_1)$ — the coefficient of b^m in E is $\overline{H}$ itself — so this asks for m vanishing a_i, which is plausible only where the a_i are small, that is at small p. Over every conjugate of every admissible prime $p < 2 \cdot 10^4$ we measured the largest number of zeros in a single column of D: it is 2 at $l = 7$, 3 at $l = 11$, 4 at $l = 13, 17, 19$, 6 at $l = 23$, 5 at $l = 31$ — and 13 at $l = 29$, attained at $p = 59 = 2 \cdot 29 + 1$, the smallest admissible prime, where $|J(1,1)_l| = \sqrt{59}$ forces very small a_i. That is one short of the fourteen zeros that would force a singular minor by this route. A cell at $(l, p) = (29, 59)$ therefore deserves an exhaustive test: $\binom{28}{14} = 40\,116\,600$ minors, about 25 CPU-seconds and 1.05 GB by the subset-Laplace recursion. We attempted it twice on a loaded machine and it did not finish; it is the cheapest open experiment here. (Those measurements are outside the formal development.)

Larger orders, exhaustively. The exhaustive minor census needs 2^{l-1} words for the Laplace table, so $l = 29$ needs 1.05 GB and $l = 31$ needs 4.3 GB; the whole window $l = 29$, $p < 10^5$ would cost about 2.3 CPU-hours. Beyond $l = 23$ we replaced it by Δ, which reaches $l = 101$ and $p < 10^6$ in half an hour — but only on the rank-drop question.

A second decade for the heuristic. Δ makes $p < 10^8$ for $l \le 23$ cost about 2 CPU-hours, extrapolating from the $p < 10^7$ run. That would test the $\log\log$ prediction of Remark 6.2 against a second decade, which is the only cheap way to discriminate between "infinitely many exceptional primes" and "the fourteen we have".

The arithmetic of the exceptional primes. Across the fourteen pairs, $(p-1)/l$ takes the values $6, 12, 466, 306, 14, 12620, 2, 306, 4, 42, 1012, 2, 150, 8$, and we see no pattern; the heuristic of Remark 6.2 predicts none. But $\Delta(b) = 0$ is one explicit determinantal condition on b, so its factorisation over $\mathbb{F}_p[b]/\Phi_l(b)$ might be tractable for small l, and would turn "heuristically infinite" into a statement about a specific variety.

The case $\alpha \ge 2$. Everything here is $q = p$. For $q = p^\alpha$ the rejection condition (v) of [2] is no longer automatic and Lemma 2.3 of [1] carries the exponent α, so the proof of Theorem 5.1 needs redoing. Katre's conjecture is stated over $\mathbb{F}_q$, so this is a real part of it that we have not touched.

References

[1] S. A. Katre and V. S. Jadhav, *Gauss–Dickson Codes*, e-print arXiv:2510.13376 [math.NT], 15 October 2025. Cited as an e-print: v1 is the only version at the time of writing, it is not withdrawn, and the record carries no journal reference and no DOI beyond the arXiv one. All numbering cited here is that of v1, as resolved from the e-print's own LaTeX: the Conjecture of §3, Lemma 2.3 of §2 (the ideal factorisation), Proposition 4.2 of §4 (the MDS characterisation), the $l = 3$ argument of §4, Remark 5.1 and Theorem 5.2 of §5, the worked $p = 61$ example of §5, and the "Future Scope" report of the exception at $(p, l) = (79, 13)$.

[2] S. A. Katre and A. R. Rajwade, *Complete solution of the cyclotomic problem in F_q for any prime modulus l, $q = p^\alpha$, $p \equiv 1 \pmod{l}$*, Acta Arith. **45** (1985), 183–199; DOI 10.4064/aa-45-3-183-199. Condition (vi), which pins the conjugate of $J(1,1)_l$ to the generator γ, is quoted from this paper in [1, §2].

[3] J. C. Parnami, M. K. Agrawal and A. R. Rajwade, *Jacobi sums and cyclotomic numbers for a finite field*, Acta Arith. **41** (1982), 1–13; DOI 10.4064/aa-41-1-1-13. The Diophantine system (i)–(v), and one of the two papers [1, §2] cites for its Lemma 2.3.

[4] S. A. Katre and J. Tanti, *Euler's criterion for eleventh power nonresidues*, Proc. Indian Acad. Sci. Math. Sci. **129** (2019), no. 3, Paper No. 41, 14 pp.; DOI 10.1007/s12044-019-0482-z. The other paper [1, §2] cites for Lemma 2.3, the factorisation of the ideal $(J(1,1)_l)$ into conjugates of a prime above p. (Its bibliography dates this as **129** (2018), no. 2; the year and issue above are those of Crossref and zbMATH.)

[5] Md. H. Ahmed and J. Tanti, *Jacobi sums and cyclotomic numbers: A survey report*, e-print arXiv:1906.09960v1 [math.NT]. The survey of this area; it states condition (vi) and does not treat D as a matrix.

[6] W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*, Cambridge University Press, 2003; DOI 10.1017/CBO9780511807077. The standard reference for the characterisation of MDS codes by the independence of

every k columns of a generator matrix; [1] states that characterisation as its Proposition 4.2 and lists this book among its coding-theory references.

[7] S. Ball, *On sets of vectors of a finite vector space in which every subset of basis size is a basis*, J. Eur. Math. Soc. (JEMS) **14** (2012), no. 3, 733–748; DOI 10.4171/jems/316. The MDS conjecture for prime fields; cited in §1 only to distinguish it from the conjecture studied here.

[8] S. Ball and M. Lavrauw, *Arcs in finite projective spaces*, EMS Surv. Math. Sci. **6** (2019), 133–172; DOI 10.4171/emss/33; e-print arXiv:1908.10772. The source of the statement of the MDS conjecture quoted in §1.

[9] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, 2nd ed., Graduate Texts in Mathematics 84, Springer, 1990. §8.3 is the level at which Jacobi sums are available in [11].

[10] 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.

[11] 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.