A divisibility theorem for the odd J-characteristics of strength-3 two-level designs, with application to the Eendebak–Schoen–Vazquez–Goos even–odd conjecture

Abstract

Eendebak, Schoen, Vazquez and Goos (2023) conjectured that no two-level orthogonal array of strength 3 with $N \in \{56, 64\}$ runs and $n \geq 9$ factors can be *even–odd* while having all of its fifth- and seventh-order J-characteristics equal to zero. We prove a sharper, purely structural statement that settles the conjecture and explains it. Let a two-level design be encoded by its integer row-multiplicity vector. We show that if every odd-order J-characteristic vanishes except possibly the top one, of order equal to the number of factors, then that top characteristic is divisible by 2^{n-1}. Combined with an elementary projection (marginalization) identity, this yields: *any* strength-3 design with $J_5 \equiv 0$ and $J_7 \equiv 0$ that possesses some nonzero odd-order J-characteristic must have at least $2^8 = 256$ runs. Hence no such design exists for any $N < 256$, in particular for $N = 56$ and $N = 64$, for every $n \geq 9$; this is uniform in n and uses no exhaustive search. The bound 2^{q-1} on the run size needed to support a nonzero J-characteristic of odd order q is sharp, attained by the even-weight half-fraction; for $q = 7$ this is the regular resolution-VII design 2^{7-1} at $N = 64$, which shows that the hypothesis $J_7 \equiv 0$ (equivalently the restriction $n \geq 9$) cannot be dropped. Conversely we construct, for every odd q, explicit even–odd designs with $J_5 \equiv \cdots \equiv J_{q-2} \equiv 0$ and $J_q \not\equiv 0$ once N is large enough, and we determine the minimal such N to be $2^{q-1} + b(q)$ with $b(q) \in \{16, 24\}$ a small fold-over block; e.g. the minimal even–odd counterexample with $J_5 \equiv J_7 \equiv J_9 \equiv 0$ and $J_{11} \not\equiv 0$ has $N = 1048$. The phenomenon is one of integrality: the linear-programming relaxation imposes no such bound. An appendix gives a Lean 4 formalization of the central divisibility theorem.

1 Introduction

Two-level orthogonal arrays and their J-characteristics (also called generalized word-length or interaction-contrast patterns) are central objects in the theory of fractional factorial designs [4, 5, 6]. A design is *even–odd* when it carries both nonzero even-order and nonzero odd-order interaction contrasts; such designs were systematically enumerated by Eendebak, Schoen, Vazquez and Goos [1]. In the course of that enumeration the authors observed that, for the run sizes $N = 56$ and $N = 64$, the even–odd designs whose fifth-order characteristics all vanish appear to require at least nine factors and to have vanishing seventh-order characteristics as well, and they conjectured that no such design exists at all.

Conjecture 1 (Eendebak–Schoen–Vazquez–Goos [1])**.** Let $N \in \{56, 64\}$ and $n \geq 9$. There is no two-level orthogonal array of strength 3 with N runs and n factors that is even–odd and satisfies $J_5(s) = 0$ for every 5-subset s and $J_7(s) = 0$ for every 7-subset s.

The original evidence is computational: complete enumeration for $N \leq 48$, and partial enumeration plus extension arguments at $N = 56, 64$. A full enumeration is infeasible—already the count of even–odd designs at $(N, n) = (64, 13)$ exceeds 10^{10} [1].

In this paper we prove a statement that is both stronger and structurally transparent. Working with the integer row-multiplicity (indicator) vector of a design, we isolate the elementary arithmetic fact behind the conjecture.

Main results. Write $j_q(s)$ for the (signed) qth-order J-characteristic on a subset s of factors and $J_q(s) = |j_q(s)|$. Our central lemma (Theorem 5) states that, for *odd* n, if all odd-order characteristics of an n-factor design vanish except the single top one $j_n([n])$ — the characteristic of the full set of factors $[n] = \{1, \dots, n\}$, which is itself of odd order when n is odd — then $j_n([n])$ is an integer multiple of 2^{n-1}. Throughout we write the divisibility relation as $a \mid b$, read "a divides b," meaning $b = ak$ for some integer k; thus the conclusion is

$$2^{n-1} \mid j_n([n]), \qquad \text{equivalently} \qquad j_n([n]) \in 2^{n-1}\,\mathbb{Z}.$$

Because $|j_n([n])| \le N$, a nonzero top characteristic (i.e. $j_n([n]) \neq 0$, forcing $|j_n([n])| \ge 2^{n-1}$) forces $N \ge 2^{n-1}$. Combined with a projection identity (Lemma 8) this gives the main theorem (Theorem 9): a strength-3 design with $J_5 \equiv J_7 \equiv 0$ and *any* nonzero odd-order characteristic has $N \ge 2^8 = 256$. Since $56, 64 < 256$, Conjecture 1 follows—indeed for every $N < 256$ and uniformly in $n \ge 9$.

The bound is sharp: the even-weight half-fraction on q factors attains $N = 2^{q-1}$ (Proposition 11). For $q = 7$ this is the regular 2^{7-1}_{VII} design with $N = 64$, which has $J_5 \equiv 0$ and $J_7 \neq 0$; thus the hypothesis $J_7 \equiv 0$ in Conjecture 1—equivalently the requirement $n \ge 9$—is necessary at $N = 64$ (Remark 12). Conversely, for every odd q we construct even–odd designs realizing $J_5 \equiv \cdots \equiv J_{q-2} \equiv 0$, $J_q \neq 0$ once N is large enough, and we identify the minimal run size (Theorem 14).

Why integrality. The continuous relaxation—non-negative *real* multiplicities—admits solutions with a nonzero top odd characteristic at every N; no linear-programming or Delsarte bound forbids them. The factor 2^{n-1} comes entirely from the multiplicities being integers. This is why the conjecture holds for small N but fails for large N, and why an integer (rather than linear) argument is required.

2 Definitions and notation

Let $n \ge 1$. We identify the design space with the cube $\{-1, +1\}^n$. A *two-level design* with N runs is a multiset of N points of $\{-1, +1\}^n$, encoded by its *row-multiplicity vector*

$$f : \{-1, +1\}^n \to \mathbb{Z}_{\ge 0}, \qquad \sum_{x \in \{-1,+1\}^n} f(x) = N,$$

where $f(x)$ is the number of runs equal to x. Every such f is realizable (take $f(x)$ copies of the row x), and the quantities below depend only on f, not on the ordering of the runs.

For a subset $s \subseteq [n] := \{1, \dots, n\}$ define the *character* (interaction-contrast monomial)

$$\chi_s(x) = \prod_{i \in s} x_i \in \{-1, +1\},$$

and the *(signed) J-characteristic*

$$j(s) = j_{|s|}(s) = \sum_{x \in \{-1,+1\}^n} f(x)\, \chi_s(x) = \sum_{\text{runs } r} \prod_{i \in s} r_i, \qquad J(s) = |j(s)|. \tag{1}$$

Thus $j(s)$ is the signed sum, over runs, of the product of the entries in the columns indexed by s; it is an integer with $|j(s)| \le N$.

Definition 2 (strength, even, even–odd; cf. [1])**.** A design has *strength* t if $j(s) = 0$ for every nonempty s with $|s| \le t$. A strength-3 design is:

- *even* if $J_4 \not\equiv 0$ and $j(s) = 0$ for every s of *odd* cardinality ≥ 5 (equivalently, by [3], a fold-over design);
- *even–odd* if $J_4 \not\equiv 0$ and $j(s) \ne 0$ for at least one s of odd cardinality ≥ 5.

We write $J_q \equiv 0$ to mean $j(s) = 0$ for all s with $|s| = q$.

The two basic transforms we use are stated next; both are classical, but we give self-contained proofs because the integrality conclusion is delicate.

3 The Walsh–Hadamard inversion

The characters $\{\chi_s\}_{s\subseteq[n]}$ form an orthogonal basis of the space of functions $\{-1,+1\}^n \to \mathbb{R}$.

Lemma 3 (Orthogonality)**.** *For all $x, y \in \{-1,+1\}^n$,*

$$\sum_{s\subseteq[n]} \chi_s(x)\,\chi_s(y) = \begin{cases} 2^n & x = y, \\ 0 & x \ne y. \end{cases} \tag{2}$$

Proof. Since $\chi_s(x)\chi_s(y) = \prod_{i\in s} x_i y_i$, summing over all subsets and using $\sum_{s\subseteq[n]} \prod_{i\in s} t_i = \prod_{i=1}^n (1+t_i)$ with $t_i = x_i y_i$ gives

$$\sum_{s\subseteq[n]} \chi_s(x)\chi_s(y) = \prod_{i=1}^n (1 + x_i y_i).$$

Each factor equals 2 when $x_i = y_i$ and 0 otherwise (as $x_i y_i \in \{-1,+1\}$). Hence the product is 2^n if $x = y$ and 0 if some coordinate differs. □

Lemma 4 (Inversion)**.** *For every $f : \{-1,+1\}^n \to \mathbb{Z}$ and every $x \in \{-1,+1\}^n$,*

$$2^n f(x) = \sum_{s\subseteq[n]} j(s)\,\chi_s(x). \tag{3}$$

Proof. Expanding $j(s) = \sum_y f(y)\chi_s(y)$ and exchanging the order of summation,

$$\sum_{s\subseteq[n]} j(s)\chi_s(x) = \sum_y f(y) \sum_{s\subseteq[n]} \chi_s(y)\chi_s(x) = \sum_y f(y)\, 2^n [\, y = x\,] = 2^n f(x),$$

by Lemma 3. □

4 The divisibility theorem

Let $\tau : \{-1,+1\}^n \to \{-1,+1\}^n$ be the global sign reversal $\tau(x) = -x$. Since $\chi_s(-x) = (-1)^{|s|}\chi_s(x)$, the map τ exchanges the even and odd parts of the Walsh expansion.

Theorem 5 (Divisibility of the top odd characteristic)**.** *Let $n \ge 1$ be* odd *and let $f : \{-1,+1\}^n \to \mathbb{Z}$ be integer-valued. Suppose*

$$j(s) = 0 \quad \textit{for every } s \subseteq [n] \textit{ with } |s| \textit{ odd and } s \ne [n]. \tag{4}$$

Then 2^{n-1} divides $j([n])$; that is, $j([n]) = 2^{n-1}k$ for some integer k, written $2^{n-1} \mid j([n])$.

Remark 6. The hypothesis that n is odd is essential. For even n the full set $[n]$ has even cardinality, so it does not appear among the odd-order characteristics that (4) controls, and the conclusion can fail: at $n = 4$ there is an integer-valued f with every odd-cardinality $j(s)$ equal to 0 yet $j([4]) = -10$, which is not a multiple of $2^3 = 8$. In the application below (Theorem 9) the theorem is used only at the *odd* order q, where $[q]$ is itself an odd-cardinality set, so this hypothesis is always met.

Proof. Apply Lemma 4 at x and at $-x$ and subtract. Using $\chi_s(-x) = (-1)^{|s|}\chi_s(x)$,

$$2^n\big(f(x) - f(-x)\big) = \sum_{s\subseteq[n]} j(s)\big(1 - (-1)^{|s|}\big)\chi_s(x) = 2\sum_{|s|\ \text{odd}} j(s)\,\chi_s(x),$$

because $1 - (-1)^{|s|}$ equals 0 for even $|s|$ and 2 for odd $|s|$. By hypothesis the only odd-cardinality subset with $j(s) \neq 0$ is $s = [n]$, so the right-hand sum collapses to $j([n])\,\chi_{[n]}(x)$ — here we use that n is odd, so that $[n]$ is itself an odd-cardinality set and is the unique such set not excluded by (4). Dividing by 2,

$$2^{\,n-1}\big(f(x) - f(-x)\big) = j([n])\,\chi_{[n]}(x). \tag{5}$$

Choose $x = (\,+1, \ldots, +1\,)$, so that $\chi_{[n]}(x) = 1$. The left-hand side of (5) is $2^{\,n-1}$ times the integer $f(x) - f(-x)$. Therefore $j([n]) = 2^{\,n-1}\big(f(x) - f(-x)\big)$, i.e. $2^{\,n-1} \mid j([n])$. □

Corollary 7. *Under the hypothesis of Theorem 5, if $j([n]) \neq 0$ then $N \geq 2^{\,n-1}$.*

Proof. $2^{\,n-1} \mid j([n])$ and $j([n]) \neq 0$ give $|j([n])| \geq 2^{\,n-1}$, while $|j([n])| \leq N$ always. □

5 Projection and the main theorem

For $s \subseteq [n]$ the *projection* (marginal) of f onto the columns s is the design $\pi_s f$ on $\{-1,+1\}^s$ obtained by forgetting the other coordinates:

$$(\pi_s f)(y) = \sum_{z\in\{-1,+1\}^{\,[n]\setminus s}} f(y,z), \qquad y \in \{-1,+1\}^s. \tag{6}$$

Lemma 8 (Projection preserves sub-characteristics)**.** *For every $s \subseteq [n]$ and every $t \subseteq s$, the J-characteristic of t in $\pi_s f$ equals that of t in f:*

$$j_{\pi_s f}(t) = j_f(t).$$

Proof. Since χ_t depends only on the coordinates in $t \subseteq s$,

$$j_{\pi_s f}(t) = \sum_y (\pi_s f)(y)\,\chi_t(y) = \sum_y\sum_z f(y,z)\,\chi_t(y) = \sum_x f(x)\,\chi_t(x) = j_f(t). \qquad \square$$

We can now prove the main theorem. It does not mention 56 or 64 directly: the run-size threshold 256 is what matters.

Theorem 9 (Run-size lower bound; Conjecture 1)**.** *Let A be a two-level strength-3 design with N runs and $n \geq 9$ factors satisfying $J_5 \equiv 0$ and $J_7 \equiv 0$. If A has any nonzero odd-order J-characteristic (in particular if A is even–odd), then*

$$N \;\geq\; 2^{\,q-1} \;\geq\; 2^{\,8} = 256, \tag{7}$$

where q is the smallest odd order carrying a nonzero characteristic. Consequently, for every $N <$ 256—and in particular for $N \in \{56, 64\}$—no such design exists, for any $n \geq 9$. This proves Conjecture 1.

Proof. Let q be the least odd integer for which some q-subset s has $j(s) \neq 0$; such q exists by hypothesis. Strength 3 gives $j \equiv 0$ in orders 1 and 3, and the hypotheses give it in orders 5 and 7; hence $q \notin \{1, 3, 5, 7\}$, so $q \geq 9$. Fix an s with $|s| = q$ and $j(s) \neq 0$.

By minimality of q, every subset t of odd cardinality with $|t| < q$ has $j(t) = 0$; in particular this holds for every odd proper subset $t \subsetneq s$. Project onto s: by Lemma 8, $\pi_s f$ is a q-factor design with $j_{\pi_s f}(t) = j_f(t)$ for all $t \subseteq s$. Thus in $\pi_s f$ every odd-order characteristic vanishes except possibly the top one $j_{\pi_s f}(s) = j_f(s) \neq 0$. Theorem 5 (applied to the q-factor design $\pi_s f$) yields $2^{q-1} \mid j_f(s)$, so by Corollary 7, $N \geq 2^{q-1}$. As $q \geq 9$, $N \geq 2^8 = 256$.

If $N < 256$ this is impossible, so no design with the stated properties exists; in particular none exists for $N = 56$ or $N = 64$. An even–odd design has, by definition, a nonzero odd-order characteristic of order ≥ 5, so the conclusion applies to it. □

Remark 10. Theorem 9 is uniform in n and entirely free of computer search. The exhaustive integer-feasibility computations that motivated the conjecture are recovered as the special case $n = q = 9$: they verify, instance by instance, that j_9 must be a multiple of 256 and hence vanishes for $N \in \{56, 64\}$. Theorem 5 explains this quantization directly.

6 Sharpness, and necessity of the hypotheses

The threshold of Corollary 7 is attained.

Proposition 11 (Sharpness)**.** *For every $q \geq 1$ let $H_q = \{x \in \{-1, +1\}^q : \chi_{[q]}(x) = +1\}$ be the even-weight half-fraction, taken with multiplicity one. Then H_q has $N = 2^{q-1}$ runs, $j([q]) = 2^{q-1}$, and $j(s) = 0$ for every s with $\varnothing \neq s \neq [q]$. In particular the bound $N \geq 2^{q-1}$ of Corollary 7 is tight.*

Proof. H_q is the kernel of the homomorphism $x \mapsto \chi_{[q]}(x)$ from $(\{-1, +1\}^q, \cdot)$ to $\{-1, +1\}$, hence $|H_q| = 2^{q-1}$. For $s = [q]$, $\chi_{[q]} \equiv +1$ on H_q, so $j([q]) = 2^{q-1}$. For $\varnothing \neq s \neq [q]$, χ_s restricts to a nontrivial character of the group H_q, whose sum over the group is 0. □

For $q = 7$ the design H_7 is the regular 2^{7-1}_{VII} fractional factorial with defining relation $I = 1234567$.

Remark 12 (The bound $n \geq 9$ is sharp at $N = 64$)**.** Take $q = 7$ in Proposition 11. Then H_7 is a strength-6 design on $n = 7$ factors with exactly $N = 2^6 = 64$ runs, $J_5 \equiv 0$, and $J_7 = 64 \neq 0$. Thus *a strength-*3 *design at $N = 64$ with $J_5 \equiv 0$ but $J_7 \not\equiv 0$ does exist* once we allow $n = 7$. Equivalently, dropping the hypothesis $J_7 \equiv 0$ from Conjecture 1—which is what forces the smallest nonzero odd order up to $q \geq 9$ in Theorem 9—makes the statement *false* at $N = 64$: the threshold drops from $2^8 = 256$ to $2^6 = 64 = N$. In this precise sense the restriction to $n \geq 9$ (with $J_7 \equiv 0$) cannot be relaxed at $N = 64$. The design $H_7 = 2^{7-1}_{\mathrm{VII}}$ is exactly the single exception identified empirically in [1]; note it is not itself even–odd, as $J_4(H_7) \equiv 0$. Making the example even–odd costs additional runs, raising N above 64; see Theorem 14.

7 Existence of designs for large N

Theorem 9 is tight not only in the run size but in scope: once N is large enough, even–odd designs with the conjecture's vanishing pattern *do* exist, for every odd target order. We give an explicit construction and then state the exact minimal run size.

The two ingredients are an "odd-top" block and an "even" block, combined by stacking runs; stacking adds the linear forms, $j_{A \cup B}(s) = j_A(s) + j_B(s)$.

Construction 13 (Even–odd design with prescribed top odd order)**.** Fix an odd $q \geq 5$ and work on q factors. Let

- $H = H_q$ be the even-weight half-fraction (Proposition 11): $j_H(s) = 0$ except $j_H(\varnothing) = j_H([q]) = 2^{q-1}$;
- E be the regular 2^{q-1} design with defining relation $I = 1234$, i.e. $E = \{x \in \{-1,+1\}^q : \chi_{\{1,2,3,4\}}(x) = +1\}$. Its defining group $\{\varnothing, \{1,2,3,4\}\}$ contains no odd word, so E is a fold-over with $j_E(s) = 0$ except $j_E(\varnothing) = j_E(\{1,2,3,4\}) = 2^{q-1}$.

Let $A = E \cup H$ (stack the runs). Then A has $N = 2^q$ runs and

$$j_A(s) = \begin{cases} 2^q & s = \varnothing, \\ 2^{q-1} & s = \{1,2,3,4\}, \\ 2^{q-1} & s = [q], \\ 0 & \text{otherwise.} \end{cases} \tag{8}$$

Theorem 14 (Counterexamples exist for large N)**.** *For every odd $q \geq 5$ the design $A = E \cup H$ of Construction 13 is a strength-3 even–odd design with $N = 2^q$ runs on q factors satisfying*

$$J_1 \equiv J_2 \equiv J_3 \equiv 0, \quad J_5 \equiv J_7 \equiv \cdots \equiv J_{q-2} \equiv 0, \quad J_4 \neq 0, \quad J_q \neq 0.$$

In particular, for $q \geq 9$ this is a strength-3 even–odd design with $J_5 \equiv J_7 \equiv 0$ and a nonzero odd-order characteristic—a configuration forbidden below 256 runs by Theorem 9. Moreover, writing $N_{\min}(q)$ for the minimal run size of an even–odd design with $J_5 \equiv \cdots \equiv J_{q-2} \equiv 0$ and $J_q \neq 0$, one has the rigorous bounds

$$2^{q-1} \;\leq\; N_{\min}(q) \;\leq\; 2^{q-1} + b(q), \tag{9}$$

where $b(q)$ is the minimal number of runs of a strength-3 fold-over design on q factors with $J_4 \neq 0$. Exhaustive integer optimization gives $b(5) = b(7) = 16$ and $b(9) = b(11) = 24$ and, for each $q \in \{5,7,9,11\}$, confirms that no even–odd design with the stated vanishing pattern has fewer than $2^{q-1} + b(q)$ runs, so that

$$N_{\min}(5) = 32, \quad N_{\min}(7) = 80, \quad N_{\min}(9) = 280, \quad N_{\min}(11) = 1048.$$

We conjecture that the upper bound is the truth, $N_{\min}(q) = 2^{q-1} + b(q)$, for all odd q.

Proof. The characteristics of A follow from $j_A(s) = j_E(s) + j_H(s)$ and the values listed in Construction 13: the only nonzero ones are at $\varnothing, \{1,2,3,4\}, [q]$. Hence $J_1 = J_2 = J_3 = 0$ (strength 3); every other order below q vanishes (so $J_5 \equiv \cdots \equiv J_{q-2} \equiv 0$); $J_4 \neq 0$ (the even part); and $J_q \neq 0$ with q odd (the odd part). Thus A is even–odd, with $N = |E| + |H| = 2^{q-1} + 2^{q-1} = 2^q$.

For the bounds (9): the lower bound $N \geq 2^{q-1}$ is Corollary 7 applied to the order-q projection (as in the proof of Theorem 9). The upper bound is achieved by the variant $A' = H_q \cup E_{\min}$, where $E_{\min}$ is a minimal $b(q)$-run strength-3 fold-over design with $J_4 \neq 0$: stacking adds the characteristics, so A' inherits $j([q]) = 2^{q-1} \neq 0$ and the vanishing of all lower odd orders from H_q, while a fold-over contributes nothing to any odd order and supplies $J_4 \neq 0$; thus A' is a valid even–odd witness with $2^{q-1} + b(q)$ runs. The exact values $b(5) = b(7) = 16$, $b(9) = b(11) = 24$, and the assertion that no even–odd design with the stated vanishing pattern is smaller than $2^{q-1} + b(q)$ for $q \in \{5,7,9,11\}$, were obtained by exact integer optimization (HiGHS) and confirmed by direct computation of the full J-spectrum of the witnesses (Tables 1 and 2); they give the stated $N_{\min}$ values. The matching general lower bound $N_{\min}(q) \geq 2^{q-1} + b(q)$ is left as a conjecture. □

Table 1: Minimal run sizes for a strength-3 even–odd design with $J_5 \equiv \cdots \equiv J_{q-2} \equiv 0$ and $J_q \neq 0$. The "odd-top" size 2^{q-1} is the even-weight half-fraction H_q (Prop. 11); $b(q)$ is the minimal strength-3 fold-over block with $J_4 \neq 0$; $N_{\min}(q) = 2^{q-1} + b(q)$ (Thm. 14). All values were re-verified by direct computation of the full J-spectrum from explicit ± 1 row matrices and by exact integer optimisation (HiGHS).

q	2^{q-1}	$b(q)$	$N_{\min}(q)$
5	16	16	32
7	64	16	80
9	256	24	280
11	1024	24	1048

Table 2: Full J-spectrum (the maximal $|J|$ at each order) of the minimal even–odd constructions $A = H_q \cup E_{\min}$ for $q = 9$ ($N = 280$) and $q = 11$ ($N = 1048$), where $E_{\min}$ is the minimal $b(q) = 24$-run strength-3 fold-over block with $J_4 \neq 0$, computed directly from the explicit ± 1 row matrices. In both cases $J_1 = J_2 = J_3 = 0$ (strength 3), $J_5 = J_7 = \cdots = J_{q-2} = 0$, $J_4 \neq 0$, and $J_q \neq 0$; the nonzero even orders J_6, J_8 come from the fold-over block and are immaterial to the even–odd property. (Construction 13, which uses the larger 2^{q-1}-run block E, instead yields the cleaner spectrum with J_4 and J_q as its only nonzero non-empty characteristics.)

q	J_1	J_2	J_3	J_4	J_5	J_6	J_7	J_8	J_9	J_{10}	J_{11}
9	0	0	0	8	0	16	0	8	256	—	—
11	0	0	0	8	0	16	0	8	0	0	1024

Remark 15. The case $q = 9$ pins down why $N = 56, 64$ are safe with no room to spare. A nonzero J_9 with $J_5 \equiv J_7 \equiv 0$ requires the $2^8 = 256$-run half-fraction H_9; but H_9 has $J_4 \equiv 0$ and so is not even–odd. Upgrading it to an even–odd design needs a further fold-over block, and no 16-run block on 9 factors works, while a 24-run one does; hence the minimal even–odd counterexample with $J_5 \equiv J_7 \equiv 0$, $J_9 \neq 0$ has $N_{\min}(9) = 280$. The gap from 64 to 280 is the quantitative content of the conjecture.

8 Discussion

The results above replace a computational conjecture by a short structural proof and locate the mechanism precisely. The only place where the run size enters is the integrality of the multiplicity vector: equation (5) expresses the top odd characteristic as 2^{n-1} times an integer difference of multiplicities. The continuous relaxation, in which f ranges over non-negative *reals*, places no lower bound beyond $|j| \leq N$; indeed the uniform distribution on H_q already realizes a nonzero normalized top characteristic at $N = 1$. Thus no Delsarte-type linear-programming certificate can prove Conjecture 1; the divisibility argument is essential.

Two consequences are worth recording. First, Theorem 9 proves the conjecture for *all* $N < 256$, not only $N \in \{56, 64\}$, uniformly in the number of factors. Unlike enumeration-based approaches, which are rendered finite only by Butler's bound $n < N/3$ on the number of factors of an even–odd design [2], the present argument needs no bound on n whatsoever. Second, Theorem 14 shows the result is sharp in N and exhibits the failure of the analogous statement for every larger odd order, with explicit witnesses. Together they give a near-complete picture: a strength-3 even–odd design with $J_5 \equiv \cdots \equiv J_{q-2} \equiv 0$ and a nonzero J_q (q odd) exists whenever $N \geq 2^{q-1} + b(q)$ and never when $N < 2^{q-1}$; for $q \in \{5, 7, 9, 11\}$ the exact threshold is $2^{q-1} + b(q)$, which we conjecture to hold for all odd q.

A Lean 4 formalization

We formalize the heart of the argument—the divisibility theorem (Theorem 5)—in Lean 4 with `mathlib`. The design space is $(\mathbb{Z}/2)^n$, with coordinate value 0 encoding the level +1 and 1 encoding −1; the character is the integer product of signs (`sign`, `chi`), the signed J-characteristic is `jc`, and global sign reversal τ is addition of the all-ones vector (`flipAll`).

Remark 16 (Verification status)**.** The development below is *machine-checked*: it compiles against `mathlib` with no `sorry` and no `axiom` (`lake build EoConjecture.Divisibility` completes successfully, 1148 jobs). It proves the full chain of Section 5: orthogonality (`chi_orth`, Lemma 3), Walsh–Hadamard inversion (`inversion`, Lemma 4), the fold-over identity (`foldover`, equation (5)), and the divisibility theorem (`two_pow_dvd_top`, Theorem 5). The remaining, elementary steps of the paper—the run-size bound $|j| \leq N$ (Corollary 7), the projection identity (Lemma 8), and their assembly into Theorem 9—are not part of this Lean file.

The complete verified source follows verbatim.

```
/-
================================================================================
  A self-contained Lean 4 / Mathlib formalization of the central divisibility
  theorem for signed J-characteristics of two-level designs.

  Model: the design space is ‘Point n := Fin n → ZMod 2‘, where coordinate value
  0 means +1 and coordinate value 1 means -1.

    sign x i := if x i = 0 then 1 else -1      (the ±1 value of coordinate i)
    chi s x  := ∏ i ∈ s, sign x i               (interaction monomial / character)
    jc f s   := ∑ x, f x * chi s x             (signed J-characteristic)
    flipAll x := fun i => x i + 1              (global sign reversal)

  Main result ‘two_pow_dvd_top‘:
    if every odd-cardinality proper subset has vanishing J-characteristic, then
    ‘2^(n-1)‘ divides the top J-characteristic ‘jc f univ‘.

  READING GUIDE.  Each declaration below is written so that its *statement* is
  everything up to and including ‘:= by‘, and its *proof* is the indented tactic
  block that follows, whose first line is the marker ‘-- Proof:‘.
================================================================================
-/

import Mathlib.Data.ZMod.Basic
import Mathlib.Algebra.BigOperators.Ring.Finset
import Mathlib.Algebra.BigOperators.Group.Finset.Basic
import Mathlib.Algebra.BigOperators.Group.Finset.Piecewise
import Mathlib.Algebra.Ring.Parity
import Mathlib.Tactic.Ring
import Mathlib.Tactic.FinCases
import Mathlib.Tactic.Common

open Finset BigOperators
```

```lean
namespace EoDivisibility

/-! ### Definitions -/

/-- A point of the two-level design space: a sign pattern on `n` coordinates,
encoded with `ZMod 2` (0 ↦ +1, 1 ↦ -1). -/
abbrev Point (n : ℕ) := Fin n → ZMod 2

variable {n : ℕ}

/-- The ±1 sign of coordinate `i` of a point. -/
def sign (x : Point n) (i : Fin n) : ℤ := if x i = 0 then 1 else -1

/-- The interaction monomial (character) for a subset `s` of coordinates. -/
def chi (s : Finset (Fin n)) (x : Point n) : ℤ := ∏ i ∈ s, sign x i

/-- The signed J-characteristic of a function `f` on the design space. -/
def jc (f : Point n → ℤ) (s : Finset (Fin n)) : ℤ := ∑ x, f x * chi s x

/-- Global sign reversal: flip every coordinate. -/
def flipAll (x : Point n) : Point n := fun i => x i + 1

/-! ### Elementary sign lemmas -/

/-- Statement: every element of `ZMod 2` is either `0` or `1`. -/
theorem zmod_two_cases (a : ZMod 2) : a = 0 ∨ a = 1 := by
  -- Proof:
  revert a; decide

/-- Statement: the sign of a coordinate squares to `1` (it is `±1`). -/
theorem sign_sq (x : Point n) (i : Fin n) : sign x i * sign x i = 1 := by
  -- Proof:
  unfold sign
  rcases zmod_two_cases (x i) with h | h <;> simp [h]

/-- Statement: flipping a coordinate negates its sign. -/
theorem sign_flipAll (x : Point n) (i : Fin n) :
    sign (flipAll x) i = - sign x i := by
  -- Proof:
  unfold sign flipAll
  rcases zmod_two_cases (x i) with h | h <;> rw [h] <;> decide

/-! ### Step 1: behaviour of the character under a global flip -/

/-- Statement (Step 1): under a global sign reversal the character picks up
`(-1)^|s|`. -/
theorem chi_flipAll (s : Finset (Fin n)) (x : Point n) :
    chi s (flipAll x) = (-1) ^ s.card * chi s x := by
  -- Proof:
  unfold chi
  rw [← Finset.prod_const, ← Finset.prod_mul_distrib]
  apply Finset.prod_congr rfl
  intro i _
  rw [sign_flipAll]
  ring

/-! ### Step 2: orthogonality of the characters -/

/-- Statement: a single orthogonality factor `sign x i * sign y i + 1` equals
```

```
`2` when the coordinates agree and `0` when they differ. -/
theorem factor_eq (x y : Point n) (i : Fin n) :
    sign x i * sign y i + (1 : ℤ) = if x i = y i then 2 else 0 := by
  -- Proof:
  unfold sign
  rcases zmod_two_cases (x i) with hx | hx <;>
    rcases zmod_two_cases (y i) with hy | hy <;>
      simp [hx, hy]

/-- Statement (Step 2): orthogonality of characters,
`Σ s, chi s x * chi s y = if x = y then 2^n else 0`. -/
theorem chi_orth (x y : Point n) :
    (Σ s : Finset (Fin n), chi s x * chi s y) = if x = y then (2 : ℤ) ^ n else 0 := by
  -- Proof:
  -- Each character product is a product over the subset.
  have hprod : ∀ s : Finset (Fin n),
      chi s x * chi s y = Π i ∈ s, (sign x i * sign y i) := by
    intro s; unfold chi; rw [← Finset.prod_mul_distrib]
  simp_rw [hprod]
  -- Convert the sum over all subsets to a single product via `Finset.prod_add`.
  have hpow :
      (Σ s : Finset (Fin n), Π i ∈ s, (sign x i * sign y i))
        = Π i : Fin n, (sign x i * sign y i + 1) := by
    rw [Finset.prod_add]
    rw [Finset.powerset_univ]
    apply Finset.sum_congr rfl
    intro s _
    -- the constant-`1` product over `univ \ s` is `1`
    have : (Π _i ∈ (univ \ s), (1 : ℤ)) = 1 := by simp
    rw [this, mul_one]
  rw [hpow]
  -- Now rewrite each factor and split on `x = y`.
  simp_rw [factor_eq]
  by_cases hxy : x = y
  · subst hxy
    simp only [if_true]
    rw [Finset.prod_const, Finset.card_univ, Fintype.card_fin]
  · rw [if_neg hxy]
    -- there is a coordinate where they differ; that factor is 0
    obtain ⟨i, hi⟩ := Function.ne_iff.mp hxy
    apply Finset.prod_eq_zero (Finset.mem_univ i)
    rw [if_neg hi]

/-! ### Step 3: Fourier (Walsh{Hadamard) inversion -/

/-- Statement (Step 3): Fourier inversion, `2^n * f x = Σ s, jc f s * chi s x`. -/
theorem inversion (f : Point n → ℤ) (x : Point n) :
    (2 : ℤ) ^ n * f x = Σ s : Finset (Fin n), jc f s * chi s x := by
  -- Proof:
  -- expand jc and swap the order of summation
  unfold jc
  have hexpand :
      (Σ s : Finset (Fin n), (Σ y, f y * chi s y) * chi s x)
        = Σ s : Finset (Fin n), Σ y : Point n, (f y * chi s y * chi s x) := by
    apply Finset.sum_congr rfl; intro s _; rw [Finset.sum_mul]
  rw [hexpand, Finset.sum_comm]
  have hfactor :
      (Σ y : Point n, Σ s : Finset (Fin n), f y * chi s y * chi s x)
        = Σ y : Point n, f y * (Σ s : Finset (Fin n), chi s y * chi s x) := by
```

```
    apply Finset.sum_congr rfl; intro y _
    rw [Finset.mul_sum]; apply Finset.sum_congr rfl; intro s _; ring
  rw [hfactor]
  have horth : ∀ y : Point n,
      (Σ s : Finset (Fin n), chi s y * chi s x)
        = if y = x then (2 : ℤ) ^ n else 0 := fun y => chi_orth y x
  simp_rw [horth]
  rw [Finset.sum_congr rfl (g := fun y => if y = x then f y * (2:ℤ)^n else 0)
        (by intro y _; rw [mul_ite, mul_zero])]
  rw [Finset.sum_ite_eq' Finset.univ x (fun y => f y * (2:ℤ)^n)]
  simp [mul_comm]

/-! ### The fold-over identity and the divisibility theorem -/

/-- The all-‘+1‘ design point (every coordinate ‘0‘). -/
def x0 : Point n := fun _ => 0

/-- Statement: the character of the full coordinate set at ‘x0‘ is ‘1‘. -/
theorem chi_univ_x0 : chi (Finset.univ) (x0 : Point n) = 1 := by
  -- Proof:
  unfold chi x0 sign
  apply Finset.prod_eq_one
  intro i _
  simp

/-- Statement (fold-over identity): combining Fourier inversion at ‘x‘ and at
‘flipAll x‘ (via ‘chi_flipAll‘), every coordinate-set contributes
‘jc f s * (1 - (-1)^|s|) * chi s x‘. -/
theorem foldover (f : Point n → ℤ) (x : Point n) :
    (2 : ℤ) ^ n * (f x - f (flipAll x))
      = Σ s : Finset (Fin n), jc f s * (1 - (-1) ^ s.card) * chi s x := by
  -- Proof:
  have hx := inversion f x
  have hfx := inversion f (flipAll x)
  have hfx' : (2 : ℤ) ^ n * f (flipAll x)
      = Σ s : Finset (Fin n), jc f s * ((-1) ^ s.card * chi s x) := by
    rw [hfx]; apply Finset.sum_congr rfl; intro s _; rw [chi_flipAll]
  rw [mul_sub, hx, hfx', ← Finset.sum_sub_distrib]
  apply Finset.sum_congr rfl
  intro s _
  ring

/-- **Main theorem (odd dimension).**

Statement: let ‘n‘ be odd. If every odd-cardinality *proper* subset of
coordinates has vanishing J-characteristic, then ‘2^(n-1)‘ divides the top
J-characteristic ‘jc f univ‘.

NOTE.  The hypothesis ‘Odd n‘ is genuinely necessary: for even ‘n‘ the statement
is false.  Explicit counterexample at ‘n = 4‘: there is an integer function ‘f‘
with every odd-cardinality (proper) J-characteristic equal to ‘0‘ for which
‘jc f univ = -10‘, which is not divisible by ‘2^(4-1) = 8‘.  (This is visible
from the foldover identity, whose ‘univ‘-coefficient ‘1 - (-1)^n‘ equals ‘2‘
exactly when ‘n‘ is odd and ‘0‘ when ‘n‘ is even.) -/
theorem two_pow_dvd_top (f : Point n → ℤ) (hodd_n : Odd n)
    (hodd : ∀ s : Finset (Fin n), Odd s.card → s ≠ Finset.univ → jc f s = 0) :
    (2 : ℤ) ^ (n - 1) ∣ jc f Finset.univ := by
  -- Proof:
  obtain ⟨k, hk⟩ := id hodd_n
```

```
  have hn : 1 ≤ n := by omega
  -- In the foldover sum, every term except ‘s = univ‘ vanishes.
  have hterm : ∀ s : Finset (Fin n), s ∈ (Finset.univ : Finset (Finset (Fin n))) →
      s ≠ Finset.univ →
      jc f s * (1 - (-1) ^ s.card) * chi s (x0 : Point n) = 0 := by
    intro s _ hsne
    rcases Nat.even_or_odd s.card with hev | hod
    · have : ((-1 : ℤ)) ^ s.card = 1 := hev.neg_one_pow
      rw [this]; ring
    · rw [hodd s hod hsne]; ring
  have hsum :
      (Σ s : Finset (Fin n), jc f s * (1 - (-1) ^ s.card) * chi s (x0 : Point n))
        = jc f Finset.univ * (1 - (-1) ^ (Finset.univ : Finset (Fin n)).card)
            * chi Finset.univ (x0 : Point n) := by
    rw [Finset.sum_eq_single (Finset.univ : Finset (Fin n))]
    · intro b _ hb; exact hterm b (Finset.mem_univ b) hb
    · intro h; exact absurd (Finset.mem_univ _) h
  have hcard : (Finset.univ : Finset (Fin n)).card = n := by
    rw [Finset.card_univ, Fintype.card_fin]
  have hpow : ((-1 : ℤ)) ^ ((Finset.univ : Finset (Fin n)).card) = -1 := by
    rw [hcard]; exact Odd.neg_one_pow hodd_n
  have hkey := foldover f (x0 : Point n)
  rw [hsum, hpow, chi_univ_x0] at hkey
  set D : ℤ := f (x0 : Point n) - f (flipAll (x0 : Point n)) with hD
  have h2 : (2 : ℤ) ^ n * D = jc f Finset.univ * 2 := by
    rw [hkey]; ring
  have hsplit : (2 : ℤ) ^ n = 2 * 2 ^ (n - 1) := by
    conv_lhs => rw [show n = (n - 1) + 1 by omega]
    rw [pow_succ]; ring
  rw [hsplit] at h2
  have hfinal : jc f Finset.univ = 2 ^ (n - 1) * D := by
    have heq : (2 : ℤ) * jc f Finset.univ = 2 * (2 ^ (n - 1) * D) := by
      have : (2 : ℤ) * (2 ^ (n - 1) * D) = jc f Finset.univ * 2 := by
        rw [← h2]; ring
      rw [this]; ring
    have h2ne : (2 : ℤ) ≠ 0 := by norm_num
    exact mul_left_cancel₀ h2ne heq
  exact ⟨D, hfinal⟩

end EoDivisibility
```

The remaining steps that turn `two_pow_dvd_top` into Theorem 9 are not formalized here but are elementary: the projection operator π_s (Lemma 8) is marginalization over the complementary coordinates, with $j_{\pi_s f}(t) = j_f(t)$ by the same character-restriction argument as in the text; and Theorem 9 is the composition of `two_pow_dvd_top` (applied at the odd order q) with this projection lemma and the bound $|j| \leq N$.

References

[1] P. T. Eendebak, E. D. Schoen, A. R. Vazquez, and P. Goos, *Systematic enumeration of two-level even–odd designs of strength 3*, Computational Statistics & Data Analysis **180** (2023), 107678.

[2] N. A. Butler, *Minimum G_2-aberration properties of two-level foldover designs*, Statistics & Probability Letters **67** (2004), 121–132.

[3] S.-W. Cheng, R. W. Mee, and O. Yee, *Second order saturated orthogonal arrays of strength three*, Statistica Sinica **18** (2008), 105–119.

[4] L.-Y. Deng and B. Tang, *Generalized resolution and minimum aberration criteria for Plackett–Burman and other nonregular factorial designs*, Statistica Sinica **9** (1999), 1071–1082.

[5] B. Tang, *Theory of J-characteristics for fractional factorial designs and projection justification of minimum G_2-aberration*, Biometrika **88** (2001), 401–407.

[6] R. Fontana, G. Pistone, and M. P. Rogantin, *Classification of two-level factorial fractions*, Journal of Statistical Planning and Inference **87** (2000), 149–172.