hexagon:2611.01381v1

New Hadamard orders via multiplicative functions

Alexander Kolpakov

29 November 2026

Abstract

A fixed system of periodic T-matrices of length 631 gives Hadamard matrices of orders $1262(q+1)q^r$ for prime powers $q \equiv 1 \pmod 4$ and $r \geq 0$, and $631(q+1)$ for prime powers $q \equiv 3 \pmod 4$. We combine these constructions with classical products, using the fixed design only once. We determine the leading interval counts for the two base families and their doublings. Two independent source parameters already give more than any fixed multiple of $N/\log N$ distinct orders in $[N, \lambda N]$, for fixed $\lambda > 1$. Adding Paley factors gives the larger counting scale supplied by Ford's theorem on multiplicative-function values.

1 Introduction

A real Hadamard matrix of order n is an $n \times n$ matrix H with entries in $\{1, -1\}$ such that $HH^{\mathsf{T}} = nI_n$. Write $\mathrm{H}(n)$ when such a matrix exists. Apart from 1 and 2, its order must be divisible by four. The Hadamard conjecture asserts that this necessary condition is sufficient.

Our companion paper [1] constructs periodic T-matrices of length 631 and a full orthogonal design of order 2524 and type $(631, 631, 631, 631)$. Here we ask what further existence statements follow from reusing that structure. We obtain two uniform prime-power families, combine several parameters while using the fixed design only once, and count the resulting distinct orders. We use classical substitution, recurrence and product theorems, attributed as they enter the proofs. We count outputs of these constructions; priority for individual orders is recorded in the companion paper.

For a positive integer t, put

$$\begin{aligned} \mathcal{F}_t &= \{2t(q+1)q^r : q \equiv 1 \pmod 4 \text{ a prime power}, \ r \geq 0\}, \\ \mathcal{G}_t &= \{t(q+1) : q \equiv 3 \pmod 4 \text{ a prime power}\}. \end{aligned} \tag{1}$$

These are sets of integers: repeated parameterizations contribute only one order. Our principal construction statements are as follows.

Theorem 1.1 (Families from the fixed design)**.** *Every order in $\mathcal{F}_{631} \cup \mathcal{G}_{631}$ admits a real Hadamard matrix. More generally, for every $k \geq 1$, prime powers $q_i \equiv 1 \pmod 4$ and integers $r_i \geq 0$, the following two orders admit real Hadamard matrices:*

$$1262 \prod_{i=1}^{k} (q_i + 1) q_i^{r_i}, \tag{2}$$

$$2^{2+\lceil 7(k-1)/11 \rceil - k} \, 631 \prod_{i=1}^{k} (q_i + 1) q_i^{r_i}. \tag{3}$$

The first product preserves a symmetric commuting quadruple before substitution. The second uses the classical products of two, four and twelve Hadamard matrices to reduce the power of two in the final order.

In both products the multiplier 631 occurs only once. The comparison with an ordinary order-2524 Hadamard matrix is also useful. Combining that matrix with k ordinary Williamson inputs sometimes gives the same order as (3); for $k = 4$ and $k = 12$, using the design on one input halves that order. Section 3 gives the precise comparison. This identifies the benefit of the additional structure even when H(2524) is already known.

For the interval counts, let

$$\mathcal{D}_t^+ = \{2^d n : n \in \mathcal{F}_t \cup \mathcal{G}_t,\ d \geq 0\}.$$

Corollary 1.2. *For every fixed $\lambda > 1$, as $N \longrightarrow \infty$,*

$$\#\big(\mathcal{F}_{631} \cap [N, \lambda N]\big) \sim \frac{(\lambda - 1)N}{2524 \log N}, \tag{4}$$

$$\#\big((\mathcal{F}_{631} \cup \mathcal{G}_{631}) \cap [N, \lambda N]\big) \sim \frac{3(\lambda - 1)N}{2524 \log N}, \tag{5}$$

$$\#\big(\mathcal{D}_{631}^+ \cap [N, \lambda N]\big) \sim \frac{3(\lambda - 1)N}{1262 \log N}. \tag{6}$$

Each of these families therefore meets every sufficiently large interval $[N, \lambda N]$. Products give larger sets: even two independent source parameters yield more than any fixed multiple of $N/\log N$ distinct orders. We first prove the two uniform constructions, then explain how to reuse the design in products, and finally count their orders.

For context, de Launey and Gordon [9], using Ford's work [12], obtain the general Hadamard-order lower bound

$$\frac{x}{\log x} \exp\{(C + o(1))(\log\log\log x)^2\}, \qquad C = 0.8178146\ldots.$$

Classical products with Paley matrices give this same scale in each fixed-ratio interval for a family built from any fixed Hadamard seed. We include that consequence to place our order counts in context; it is not a new general density bound. Ford's theorem counts distinct shifted-prime products, resolving the repeated-representation problem. Its application is proved in Appendix D. Appendix E gives a further consequence of the companion paper's rank comparison: families of mutually inequivalent matrices at the doubled orders.

2 Two uniform constructions

The first family uses a full orthogonal design of type (t, t, t, t). The second uses the additional periodic T-matrix structure. Both ingredients are available at $t = 631$.

2.1 The fixed design and substitution

For a positive integer t, suppose that X_0, X_1, X_2, X_3 are matrices of order $4t$, with entries in $\{0, 1, -1\}$, satisfying

$$X_i X_i^{\mathsf{T}} = tI_{4t}, \tag{7}$$

$$X_i X_j^{\mathsf{T}} + X_j X_i^{\mathsf{T}} = 0 \quad (i \neq j). \tag{8}$$

At every position, require exactly one of the four matrices to have a nonzero entry. Equivalently, $\sum_i x_i X_i$ is a full orthogonal design of type (t,t,t,t). The companion paper [1] constructs such a quadruple for $t = 631$ from an explicit periodic T-matrix witness. We use that fixed design throughout; the prime-power parameter below is independent of its construction.

Proposition 2.1 (Cooper–Wallis substitution)**.** *Suppose (7)–(8) and the support partition hold. Let A_0, A_1, A_2, A_3 be symmetric, pairwise commuting sign matrices of order w such that*

$$\sum_{i=0}^{3} A_i^2 = 4wI_w. \tag{9}$$

Then

$$H = \sum_{i=0}^{3} X_i \otimes A_i \tag{10}$$

is a real Hadamard matrix of order $4tw$.

Proof. Each entry has exactly one nonzero summand, which is a product of two signs. For $i \neq j$, symmetry and commutativity give $A_i A_j^{\mathsf{T}} = A_j A_i^{\mathsf{T}}$. The two corresponding terms in HH^{T} therefore cancel by (8). The diagonal terms give

$$HH^{\mathsf{T}} = tI_{4t} \otimes \sum_i A_i A_i^{\mathsf{T}} = 4twI_{4tw}.$$

□

This is the classical substitution of Cooper and Wallis [2, Theorem 3]. For group-developed inputs it can also be read as restriction of scalars from a rational group algebra: multiplication by a group polynomial becomes its regular-action matrix. Formula (10) retains the whole action; the support partition proves that its final entries are signs.

We call a quadruple satisfying the hypotheses on the A_i a *symmetric Williamson-type quadruple* of order w.

2.2 The finite-field core

Fix a prime power $q \equiv 1 \pmod 4$. Let χ be the quadratic character of $\mathbb{F}_q$, extended by $\chi(0) = 0$, and define

$$K_{x,y} = \chi(y - x) \qquad (x, y \in \mathbb{F}_q).$$

Write J for the all-one matrix of order q. The needed identities are

$$K^{\mathsf{T}} = K, \qquad K^2 = qI - J, \qquad KJ = JK = 0, \qquad J^2 = qJ. \tag{11}$$

Here K has zero diagonal and signs elsewhere. Symmetry follows from $\chi(-1) = 1$, and the row sum is zero because exactly half the nonzero field elements are squares.

For completeness, the character sum behind the second identity is

$$\sum_{s \in \mathbb{F}_q} \chi\big(s(s+1)\big) = -1.$$

Indeed the number of solutions of $y^2 = s(s+1)$ is both q plus this sum and $q - 1$: the change of variables $u = 2s + 1 - 2y$, $v = 2s + 1 + 2y$ identifies the solutions with $uv = 1$. Rescaling the summation variable gives inner product -1 for distinct rows of K; a row has squared norm $q - 1$. Hence $KK^{\mathsf{T}} = qI - J$, as required. These calculations use only that the characteristic is odd.

2.3 Strong starters and Spence's recurrence

Turyn's theorem [3], in the form recorded by Seberry and Balonin [4, Theorem 2 and Lemma 1], supplies symmetric commuting circulants R, S of order $w_0 = (q+1)/2$ such that $S, R+I, R-I$ have sign entries and

$$R^2 + S^2 = qI. \tag{12}$$

Begin with the four sign matrices

$$D_0 = E_0 = S, \qquad F_0 = R + I, \qquad G_0 = R - I.$$

They satisfy two identities, stronger than their total Williamson norm:

$$M_0 := (D_0 - E_0)^2 + (F_0 - G_0)^2 = 4I, \tag{13}$$
$$P_0 := (D_0 + E_0)^2 + (F_0 + G_0)^2 = 4qI. \tag{14}$$

These follow at once from (12). Keeping both identities is the point that allows the recurrence to work for every stage.

For a pair (U, V) define

$$\begin{aligned} U' &= \frac{U-V}{2} \otimes J + \frac{U+V}{2} \otimes (K+I), \\ V' &= \frac{U-V}{2} \otimes J + \frac{U+V}{2} \otimes (K-I). \end{aligned} \tag{15}$$

Apply this to (D_r, E_r) and (F_r, G_r) to obtain the next four matrices. This is Spence's recurrence [5, Theorem 4]. Each step multiplies their common order by q, so their order at stage r is

$$w_r = \frac{q+1}{2} q^r. \tag{16}$$

Lemma 2.2. *For every $r \geq 0$, the four matrices are symmetric commuting sign matrices, and*

$$\begin{aligned} M_r &:= (D_r - E_r)^2 + (F_r - G_r)^2 = 4q^r I_{w_r}, \\ P_r &:= (D_r + E_r)^2 + (F_r + G_r)^2 = 4q^{r+1} I_{w_r}. \end{aligned} \tag{17}$$

Consequently their squared matrices sum to $4w_r I_{w_r}$.

Proof. For two corresponding signs u, v, exactly one of $(u-v)/2$ and $(u+v)/2$ is nonzero, and that value is a sign. The matrices $J, K+I, K-I$ all have sign entries. Thus (15) gives signs. The first tensor factors belong to the commutative algebra generated by the old four matrices, and the second factors belong to the commutative algebra generated by I, J, K. Symmetry and commutativity are therefore preserved.

Adding and subtracting (15) gives

$$U' - V' = (U+V) \otimes I, \qquad U' + V' = (U-V) \otimes J + (U+V) \otimes K.$$

The mixed products in the square of the latter expression vanish by $JK = KJ = 0$. Applying (11) to both pairs yields

$$\begin{aligned} M_{r+1} &= P_r \otimes I, \\ P_{r+1} &= qP_r \otimes I + (qM_r - P_r) \otimes J. \end{aligned} \tag{18}$$

Equations (13)–(14) start the induction. Under (17), the coefficient $qM_r - P_r$ is zero, proving the next stage. Finally,

$$D_r^2 + E_r^2 + F_r^2 + G_r^2 = \tfrac{1}{2}(M_r + P_r) = 2(q+1)q^r I_{w_r} = 4w_r I_{w_r}.$$

□

An arbitrary Williamson quadruple cannot replace the starter above: its total norm need not give $P_0 = qM_0$, and the J term in (18) would then remain. The strong starter condition is part of the construction.

Theorem 2.3. *Whenever a full orthogonal design of type (t,t,t,t) exists,*

$$\mathrm{H}\big(2t(q+1)q^r\big) \quad \textit{for all prime powers } q \equiv 1 \pmod 4 \textit{ and } r \geq 0.$$

In particular this holds for $t = 631$.

Proof. Use Lemma 2.2 in Proposition 2.1. By (16), the resulting Hadamard order is $4tw_r = 2t(q+1)q^r$. □

This combines Turyn's starters, Spence's recurrence and the fixed design. For other values of t, the same conclusion holds whenever a full orthogonal design of the stated type is available.

2.4 A second family from the periodic T-matrices

The design at $t = 631$ comes from four periodic T-matrices. We now use this additional structure to obtain the second prime-power family. Let $T_1, \ldots, T_4$ be circulant $\{0, 1, -1\}$-matrices of order t, with disjoint supports partitioning all entries and $\sum_k T_k T_k^{\mathsf{T}} = tI_t$. These conditions hold for the explicit T-matrices at $t = 631$.

A negacyclic matrix is a polynomial in the signed cyclic shift Q_s whose wrap-around entry is -1, so $Q_s^s = -I_s$. This algebra is commutative and closed under transpose. Its reversing permutation J_s satisfies $J_s Q_s J_s = Q_s^{\mathsf{T}}$.

Lemma 2.4 (Block substitution)**.** *If a Hadamard matrix of order $4s$ is a 4×4 array of negacyclic blocks of order s, then periodic T-matrices of order t give* $\mathrm{H}(4st)$.

The classical circulant version is Seberry and Yamada [10, Theorem 4, printed p. 105]. The proof in Appendix A gives the entry and Gram calculation for the negacyclic case, using its transpose-reversing permutation.

Lemma 2.5. *For every prime power $q \equiv 3 \pmod 4$, the Paley matrix of order $q+1$ is equivalent to a 4×4 array of negacyclic blocks of order $(q+1)/4$.*

The required block input is also supplied by the classical negaperiodic Golay-pair route: Balonin and Đoković [11, Propositions 2 and 8] give a Hadamard matrix of order $q+1$ in a two-by-two negacyclic form. Splitting each block's even and odd coordinates gives the four-by-four form needed here. Appendix A records this reindexing and a direct proof for the Paley matrix itself.

Choose a cyclic subgroup of order $(q+1)/2$ in the norm-one group of $\mathbb{F}_{q^2}^{\times}$. Its action on the projective line over $\mathbb{F}_q$ has four orbits, giving the four block rows. The proof in Appendix A includes the sign switching that gives a negative wrap-around sign. This sign is retained in the block algebra throughout the substitution.

Corollary 2.6. *For every t with verified periodic T-matrices,*

$$\mathrm{H}\big(t(q+1)\big) \qquad (q \equiv 3 \pmod 4 \text{ a prime power}).$$

In particular, this holds at $t = 631$.

Proof. Apply Lemma 2.4 to Lemma 2.5. □

3 Reusing the fixed design

3.1 Combine the quadruples before substitution

The fixed design need only be used once. Seberry and Yamada's product for Williamson-type matrices [10, Corollary 25] combines Williamson-type quadruples before substitution. We use its symmetric case:

Proposition 3.1. *A symmetric commuting sign quadruple of order u whose squares sum to $4uI$, together with one of order v whose squares sum to $4vI$, gives such a quadruple of order $2uv$.*

The construction uses four disjoint support blocks from the first quadruple and substitutes the second quadruple into them. Their norm identity gives $8uvI$, and the tensor-factor algebras preserve symmetry and commutativity. The complete blocks and calculation are in Appendix A.

Corollary 3.2. *Suppose the fixed design exists for t. For every $k \geq 1$, choose independently prime powers $q_i \equiv 1 \pmod 4$ and integers $r_i \geq 0$, $1 \leq i \leq k$. Then*

$$\mathrm{H}\left(2t \prod_{i=1}^{k} (q_i+1) q_i^{r_i}\right).$$

Proof. The recurrence supplies source widths $w_i = (q_i+1)q_i^{r_i}/2$. Repeated products in Proposition 3.1 give a symmetric commuting quadruple of width $2^{k-1}\prod_i w_i$. Substituting once gives order $4t\,2^{k-1}\prod_i w_i = 2t\prod_i (q_i+1)q_i^{r_i}$. □

This product preserves a symmetric commuting quadruple for further substitutions, while using the fixed design only once. If only the final Hadamard matrix is needed, the four- and twelve-input products below can give smaller orders.

3.2 Products of Hadamard matrices

The following classical products require only Hadamard matrices as inputs. For positive integer parameters, they give

$$\begin{aligned} \mathrm{H}(4a),\ \mathrm{H}(4b) &\implies \mathrm{H}(8ab), \\ \mathrm{H}(4a_1),\dots,\mathrm{H}(4a_4) &\implies \mathrm{H}(16a_1a_2a_3a_4), \\ \mathrm{H}(4a_1),\dots,\mathrm{H}(4a_{12}) &\implies \mathrm{H}(512\textstyle\prod_{i=1}^{12} a_i). \end{aligned} \tag{19}$$

The first is the Agayan–Sarukhanyan product, as proved in de Launey [8, Section 2]. The second is due to Craigen, Seberry and Zhang [7, Theorem 1]; the third is due to de Launey [8, Section 3]. Repeated inputs are allowed, and there is no coprimality, oddness or symmetry assumption. We also allow ordinary Kronecker products and doubling.

3.3 The exact power-of-two cost

Write an input order as $4a$. Combining s normalized orders by the three rules in (19) gives $4 \cdot 2^d \prod a_i$, where

$$(s, d) = (2, 1),\ (4, 2),\ (12, 7).$$

Each such operation reduces the number of remaining factors by $s - 1$. For $k \geq 1$, let

$$\begin{aligned} c(k) = \min\{u_2 + 2u_4 + 7u_{12} : u_2, u_4, u_{12} \geq 0, \\ u_2 + 3u_4 + 11u_{12} = k - 1\}. \end{aligned} \tag{20}$$

The minimum is over nonnegative integers and exists because binary operations alone suffice. It has a simple closed form:

$$c(k) = \left\lceil \frac{7(k-1)}{11} \right\rceil. \tag{21}$$

To see this, each cost is at least $7/11$ times the corresponding leaf reduction, giving the lower bound. Write $k - 1 = 11s + r$, $0 \leq r \leq 10$. Choose s twelve-input nodes, $\lfloor r/3 \rfloor$ four-input nodes and $r \bmod 3$ binary nodes. Their cost is

$$7s + 2\lfloor r/3 \rfloor + (r \bmod 3) = 7s + \lceil 7r/11 \rceil,$$

where the equality is checked for the eleven possible remainders. This attains the lower bound.

Proposition 3.3. *Given k Hadamard input orders $4a_1, \ldots, 4a_k$, the least output order obtainable using every input once and the rules in (19), Kronecker products and doubling is*

$$2^{2+c(k)} \prod_{i=1}^{k} a_i = 2^{2+\lceil 7(k-1)/11 \rceil} \prod_{i=1}^{k} a_i. \tag{22}$$

All its doublings are also obtainable. The minimum is taken over these products of Hadamard matrices; products of structured quadruples are considered separately in Proposition 3.1.

Proof. A tree with k leaves and the indicated internal arities satisfies $\sum (s-1)u_s = k - 1$. Its powers of two multiply, giving the cost in (20). Conversely any such internal-node counts can be realized: begin with one leaf and repeatedly replace a leaf by a node with its prescribed number of children. Labels can then be assigned to the resulting k leaves in any order. This proves attainability of the minimum. A Kronecker operation on two normalized inputs has cost two; replacing it by the binary rule of cost one and a doubling gives the same order. Kronecker nodes and extra doublings therefore cannot improve the minimum. □

For example,

k	1	2	3	4	12	64
$2 + c(k)$	2	3	4	4	9	43

The table gives the minimum cost within the stated product rules.

3.4 Use the fixed design once in the product

A symmetric Williamson-type quadruple of order $w_i = (q_i + 1)q_i^{r_i}/2$ already gives $\mathrm{H}(4w_i)$ by the classical Williamson array, before the fixed design is used. Equivalently, use Proposition 2.1 with the standard orthogonal design of order four, so $t = 1$. We may therefore apply the design to one quadruple and use the other $k - 1$ Hadamard matrices directly.

Corollary 3.4. *Suppose the fixed design exists for t. Choose independently prime powers $q_i \equiv 1 \pmod 4$ and integers $r_i \geq 0$, for $1 \leq i \leq k$. Then*

$$\mathrm{H}\left(2^{2+c(k)-k} t \prod_{i=1}^{k} (q_i+1) q_i^{r_i}\right). \tag{23}$$

In particular, four inputs give order $t\prod_{i=1}^{4}(q_i+1)q_i^{r_i}$, and twelve give $(t/8)\prod_{i=1}^{12}(q_i+1)q_i^{r_i}$.

Proof. Apply the optimal product tree to the k input orders $4tw_1, 4w_2, \ldots, 4w_k$. Their normalized product is $t\prod_i w_i$, giving $4 \cdot 2^{c(k)} t \prod_i w_i$. □

To compare with an ordinary Hadamard input, set all variables of the design equal to one, giving $\mathrm{H}(4t)$. Combining this matrix with all k ordinary Williamson inputs gives $\mathrm{H}(4 \cdot 2^{c(k+1)} t \prod_i w_i)$. Formula (23) halves this order when $c(k+1) = c(k)+1$ and agrees with it when $c(k+1) = c(k)$. The orders agree for $k = 3$; using the design on one input saves a factor of two for $k = 4$ and $k = 12$. At $t = 631$, $\mathrm{H}(2524)$ was already known independently, so this comparison isolates the benefit of its additional T-matrix structure.

Applying the design to every input instead gives an order larger by t^{k-1}. The single-use formula avoids those repeated factors without changing the classical multiplication rules.

4 Counting distinct orders

The constructions may give the same integer from different parameters. We count distinct orders throughout. All logarithms are natural; $\log_j x$ denotes the j-fold iterated logarithm. All interval estimates below hold for each fixed ratio $\lambda > 1$.

4.1 The first prime-power family

The arithmetic count for $\mathcal{F}_t$ makes sense for every fixed positive integer t. Its interpretation as a family of Hadamard orders uses the design hypothesis in Theorem 2.3.

Proposition 4.1. *For every fixed $t \geq 1$ and $\lambda > 1$,*

$$\#\big(\mathcal{F}_t \cap [N, \lambda N]\big) \sim \frac{(\lambda-1)N}{4t \log N}.$$

Proof. First take $r = 0$ and $q = p$ prime. The map $p \mapsto 2t(p+1)$ is injective. The prime number theorem in the fixed progression $1 \pmod 4$ [6, Theorem 5.10] says

$$\pi(x; 4, 1) \sim \frac{x}{2 \log x}.$$

Its difference at $\lambda N/(2t) - 1$ and $N/(2t) - 1$ is $(\lambda-1)N/(4t \log N)$ asymptotically. Subtraction is valid here because the two arguments have a fixed ratio greater than one and each error is $o(N/\log N)$.

We bound all remaining parameter choices up to $X = \lambda N$. The number of nonprime prime powers $q \leq X$ is at most

$$\sum_{2 \leq e \leq \log X/\log 2} X^{1/e} = O(\sqrt{X} \log X).$$

This covers the remaining $r = 0$ choices, after harmless changes of the constant depending on t. If $r \geq 1$, then $q^{r+1} \leq X/(2t)$. Since $q \geq 5$, there are only $O(\log X)$ possible stages, and the number of ordered pairs (q, r) is at most

$$\sum_{1 \leq r \leq O(\log X)} (X/(2t))^{1/(r+1)} = O_t(\sqrt{X} \log X).$$

These are upper bounds on parameter choices, so they remain valid when two choices give the same order. The prime, stage-zero subset supplies the lower bound; adding all other orders changes its count by $o(N/\log N)$. This proves the assertion for distinct orders. □

Repeated parameterizations really occur: $(q, r) = (5, 1)$ and $(29, 0)$ both give $60t$. They do not affect the asymptotic, because at least one parameterization lies in the error term just estimated.

The leading constant comes from the prime number theorem in the progression $1 \pmod 4$. Higher prime powers and positive recurrence stages contribute only to the error term.

Every member of $\mathcal{F}_t$ has $v_2(n) = 2 + v_2(t)$, because $q + 1 \equiv 2 \pmod 4$ and q is odd. Thus the construction supplies orders within a single two-adic stratum for each fixed t; for $t = 631$ they are all congruent to 4 modulo 8.

4.2 The second family and the union

Prime counting in the progression $3 \pmod 4$ gives, for each fixed $\lambda > 1$,

$$\#(\mathcal{G}_t \cap [N, \lambda N]) \sim \frac{(\lambda - 1)N}{2t \log N}.$$

Nonprime prime powers contribute only $O_{t,\lambda}(\sqrt{N} \log N)$. For the prime parts of $\mathcal{F}_t$ and $\mathcal{G}_t$, an intersection requires $2t(p + 1) = t(\ell + 1)$, or $\ell = 2p + 1$. The two-linear-form upper-bound sieve [13, Theorem 5] gives $O_{t,\lambda}(N/\log^2 N)$ such pairs; all remaining intersections lie in the previously bounded error terms. Hence

$$\#\big((\mathcal{F}_t \cup \mathcal{G}_t) \cap [N, \lambda N]\big) \sim \frac{3(\lambda - 1)N}{4t \log N}. \tag{24}$$

4.3 Including every doubling

Put $\mathcal{D}_t = \{2^d n : n \in \mathcal{F}_t,\ d \geq 0\}$. This set consists of all Sylvester doublings of orders in the first family. Since all orders in $\mathcal{F}_t$ have the same exact two-adic exponent, the sets $2^d \mathcal{F}_t$ are disjoint as d varies.

Corollary 4.2. *For every fixed $t \geq 1$ and $\lambda > 1$,*

$$\#(\mathcal{D}_t \cap [N, \lambda N]) \sim \frac{(\lambda - 1)N}{2t \log N}.$$

If the design for t is supplied, these are Hadamard existence orders.

Each fixed doubling contributes its scaled prime count. The geometric sum doubles the leading constant. Appendix B justifies the uniform tail estimate needed to sum over every doubling.

Corollary 4.3. *If periodic T-matrices exist at t, then $\mathcal{D}_t^+$ consists of Hadamard orders and satisfies*

$$\#(\mathcal{D}_t^+ \cap [N, \lambda N]) \sim \frac{3(\lambda - 1)N}{2t \log N}$$

for each fixed $\lambda > 1$.

Unlike the single-family doublings, these output sets can overlap. Appendix B bounds the overlaps before summing the geometric series. At $t = 631$, the leading constant is six times that of the original undoubled $\mathcal{F}_{631}$ count.

Theorem 1.1 follows from Theorem 2.3 and Corollaries 2.6, 3.2 and 3.4. Proposition 4.1, (24) and Corollary 4.3 give Corollary 1.2.

4.4 Distinct orders from two source parameters

Let $\mathcal{S}_{t,2}$ be the orders obtained by combining two quadruples before substitution:

$$\mathcal{S}_{t,2} = \{2t(p+1)(q+1) : p, q \equiv 1 \pmod 4 \text{ prime}\}.$$

Corollary 3.2 gives every member from two independently chosen sources. Two parameters do not automatically mean more distinct orders, because such products can have repeated representations. Nevertheless the following improvement holds.

Proposition 4.4. *For every fixed $t \geq 1$ and $\lambda > 1$,*

$$\frac{\#(\mathcal{S}_{t,2} \cap [N, \lambda N])}{N/\log N} \longrightarrow \infty.$$

This conclusion already holds among the displayed prime-input orders, which have exact two-adic exponent $3 + v_2(t)$.

The proof fixes finitely many first inputs and uses a two-linear-form sieve to bound overlaps between their output sets. Each input contributes a leading constant proportional to the reciprocal of $(p+1)/2$. These reciprocals have a divergent sum, so larger fixed collections give arbitrarily large lower constants. Appendix B gives the argument, with the collection fixed before N tends to infinity.

4.5 Products with Paley orders

To count products of arbitrarily many shifted primes, we use Ford's theorem on distinct values of multiplicative functions. De Launey and Gordon [9] used this theorem to obtain their general Hadamard-order bound. The same argument counts an explicit family built from any fixed Hadamard seed.

Let

$$\mathcal{M}_+ = \left\{ \prod_{j=1}^{k} (p_j + 1) : k \geq 0, \quad p_j \text{ odd primes} \right\},$$

where primes may repeat and the empty product is one. Fix a Hadamard order h divisible by four, and put $\mathcal{E}_h = h\mathcal{M}_+$. The fixed design gives $h = 4t$ by setting its variables equal to one; at $t = 631$ this permits $h = 2524$. The companion paper also supplies $h = 7572$.

Theorem 4.5. *Every order in $\mathcal{E}_h$ admits a real Hadamard matrix. For every fixed $\lambda > 1$,*

$$\#\big(\mathcal{E}_h \cap [N, \lambda N]\big) = \frac{N}{\log N} \exp\big\{(C + o(1))(\log\log\log N)^2\big\}, \qquad C = 0.8178146\ldots.$$

Proof. For every odd prime p, the Paley constructions give $\mathrm{H}(2(p+1))$: use the second construction when $p \equiv 1 \pmod 4$, and double the first when $p \equiv 3 \pmod 4$. Write a current order as $h' = 4a$. Combining $\mathrm{H}(h')$ with $\mathrm{H}(2(p+1)) = \mathrm{H}(4 \cdot (p+1)/2)$ by the binary rule in (19) gives

$$\mathrm{H}\big(8a(p+1)/2\big) = \mathrm{H}\big(h'(p+1)\big).$$

Induction proves existence for every member of $\mathcal{E}_h$. Ford's local value-distribution theorem gives the interval count; Appendix D verifies its hypotheses and proves the more precise estimate there. □

The displayed expression specifies the leading logarithmic factor, rather than an asymptotic with a determined multiplicative constant. It grows faster than $N/\log N$. Thus $\mathcal{E}_{4t}$ supplies asymptotically more orders than the two base formulas together: removing $\mathcal{F}_t \cup \mathcal{G}_t$, whose interval count is $O_{t,\lambda}(N/\log N)$, leaves the same leading logarithmic scale.

5 Further ingredients and questions

Any further full orthogonal design of type (t,t,t,t) gives the first prime-power family and its mixed products. When the design comes from periodic T-matrices, the second Paley-based family is available as well. The roles of the two ingredients are separate: a different fixed design changes t, while a different family of symmetric Williamson-type quadruples supplies new widths for substitution.

The substitution requires symmetry, commutativity and the norm identity (9). Turyn's starters and Spence's recurrence provide one uniform supply. A natural next problem is to find further families of quadruples satisfying those identities, or products that exploit more of their structure. Appendix C analyzes the coverage of the present completed-matrix products under their stated source assumptions.

A The structured products

A.1 The symmetric Williamson-type product

Proof of Proposition 3.1. Here is the block construction, including the properties needed for iteration. For the first quadruple A, B, C, D, put

$$E = (A+B)/2, \quad F = (A-B)/2, \quad G = (C+D)/2, \quad K = (C-D)/2,$$

and define

$$T_1 = \begin{pmatrix} E & 0 \\ 0 & E \end{pmatrix}, \quad T_2 = \begin{pmatrix} F & 0 \\ 0 & F \end{pmatrix}, \quad T_3 = \begin{pmatrix} 0 & G \\ G & 0 \end{pmatrix}, \quad T_4 = \begin{pmatrix} 0 & K \\ K & 0 \end{pmatrix}.$$

The T_i have disjoint supports partitioning all positions and satisfy $\sum_i T_i T_i^{\mathsf{T}} = 2uI$. For the second quadruple X, Y, Z, W, form

$$\begin{aligned} L &= T_1 \otimes X + T_2 \otimes Y + T_3 \otimes Z + T_4 \otimes W, \\ M &= -T_1 \otimes Y + T_2 \otimes X + T_3 \otimes W - T_4 \otimes Z, \\ N &= -T_1 \otimes Z - T_2 \otimes W + T_3 \otimes X + T_4 \otimes Y, \\ P &= -T_1 \otimes W + T_2 \otimes Z - T_3 \otimes Y + T_4 \otimes X. \end{aligned}$$

Their entries are signs by the support partition. Expanding their Gram products, symmetry and commutativity in each tensor factor cancel the cross terms, giving

$$LL^{\mathsf{T}} + MM^{\mathsf{T}} + NN^{\mathsf{T}} + PP^{\mathsf{T}} = \Big(\sum_i T_i T_i^{\mathsf{T}}\Big) \otimes (XX^{\mathsf{T}} + YY^{\mathsf{T}} + ZZ^{\mathsf{T}} + WW^{\mathsf{T}}) = 8uvI.$$

All four T_i belong to the algebra generated by the old symmetric commuting matrices and the two-by-two swap matrix. Thus they are symmetric and commute. The four outputs belong to the tensor product of this algebra with the algebra generated by X, Y, Z, W, so they too are symmetric and commute. This proves the form of the classical product used here.

□

A.2 T-matrices and negacyclic blocks

Proof of Lemma 2.4. Write the given Hadamard matrix as $(N_{kj})_{k,j=1}^{4}$. Set $A_j = \sum_k T_k \otimes N_{kj}$. Each entry is a sign, since the supports of the T_k partition the entries. Orthogonality of the block rows gives

$$\sum_j N_{kj} N_{\ell j}^{\mathsf{T}} = 4s\delta_{k\ell} I_s,$$

so

$$\sum_j A_j A_j^{\mathsf{T}} = \sum_{k,\ell} T_k T_\ell^{\mathsf{T}} \otimes \sum_j N_{kj} N_{\ell j}^{\mathsf{T}} = 4stI_{st}.$$

The A_j lie in the commutative, transpose-closed algebra generated by $P_t \otimes I_s$ and $I_t \otimes Q_s$, where P_t is the ordinary cyclic shift. Let R_t send an index x of C_t to $-x$ and let J_s be the back-diagonal permutation. Then $R = R_t \otimes J_s$ is a symmetric permutation involution, and

$$R_t P_t R_t = P_t^{\mathsf{T}}, \quad J_s Q_s J_s = Q_s^{\mathsf{T}}, \quad R A_j^{\mathsf{T}} = A_j R.$$

For $A = A_1, B = A_2, C = A_3, D = A_4$, use the Goethals–Seidel array

$$\begin{pmatrix} A & BR & CR & DR \\ -BR & A & D^{\mathsf{T}}R & -C^{\mathsf{T}}R \\ -CR & -D^{\mathsf{T}}R & A & B^{\mathsf{T}}R \\ -DR & C^{\mathsf{T}}R & -B^{\mathsf{T}}R & A \end{pmatrix}.$$

All its entries are signs. Its diagonal Gram blocks equal $\sum_j A_j A_j^{\mathsf{T}} = 4stI$; its off-diagonal blocks cancel by commutativity and the displayed reflection identity. Thus its order and Gram scale are both $4st$. □

A.3 The four-block form of the Paley matrix

The block input can alternatively be obtained from a negaperiodic Golay pair of length $2s = (q+1)/2$, whose existence is proved in [11, Proposition 8]. Proposition 2 there gives

$$H = \begin{pmatrix} A & B \\ -B^{\mathsf{T}} & A^{\mathsf{T}} \end{pmatrix}, \qquad A, B \in \mathbb{R}[Q_{2s}].$$

This matrix commutes with $\mathrm{diag}(Q_{2s}^2, Q_{2s}^2)$. Ordering the even and odd coordinates separately inside each block conjugates Q_{2s}^2 to $\mathrm{diag}(Q_s, Q_s)$. The reordered H therefore has sixteen blocks in $\mathbb{R}[Q_s]$, which is sufficient for Lemma 2.4. The following proof also identifies the block form directly in the Paley matrix.

Proof of Lemma 2.5. Put $s = (q+1)/4$. Choose an element h of order $2s$ in the norm-one subgroup of $\mathbb{F}_{q^2}^{\times}$. Multiplication by h is an element g of $\mathrm{SL}_2(\mathbb{F}_q)$ and satisfies $g^s = -I$. Its action on the projective line has four orbits of length s. Indeed, if $h^j v = \lambda v$ for a nonzero $v \in \mathbb{F}_{q^2}$ and $\lambda \in \mathbb{F}_q$, division by v gives $h^j = \lambda$. The norm-one subgroup meets $\mathbb{F}_q^{\times}$ only in $\{1, -1\}$, so the smallest positive projective period is s.

Choose representatives v_x for the projective points and let χ be the quadratic character of $\mathbb{F}_q$. Set $S_{xx} = 0$ and $S_{xy} = \chi(\det(v_x, v_y))$ for $x \neq y$. Because $\chi(-1) = -1$, S is skew-symmetric. Each row has squared norm q; for two distinct rows use their lines as coordinate axes to see that the cross sum is $\sum_{z \in \mathbb{F}_q} \chi(-z) = 0$. Thus $SS^{\mathsf{T}} = qI$ and $H = I + S$ is the Paley Hadamard matrix. Changing representatives switches the corresponding rows and columns.

Write $gv_x = c_x v_{gx}$. Determinant preservation gives

$$S_{xy} = \chi(c_x)\chi(c_y)S_{gx,gy}.$$

Hence g induces a signed permutation preserving H by simultaneous row and column action. Its sign product around each orbit is $\chi(-1) = -1$, since $g^s = -I$. A diagonal sign switch makes the first $s-1$ steps positive and the final step negative on every orbit. After this switch and ordering by the four orbits, the automorphism is $\mathrm{diag}(Q_s, Q_s, Q_s, Q_s)$. Every matrix block commutes with Q_s. The signed shift is a companion matrix with cyclic vector and minimal polynomial $x^s + 1$, so its centralizer is $\mathbb{R}[Q_s]$. All sixteen blocks are therefore negacyclic, as required. □

B Counting doublings and two-source products

B.1 The doubling constant

Proof of Corollary 4.2. Every member of $\mathcal{F}_t$ has exact two-adic exponent $2 + v_2(t)$. Thus the sets $2^d\mathcal{F}_t$ are disjoint. The nonprime prime powers and positive recurrence stages contribute at most

$$\sum_{d\geq 0} O_t\left(\sqrt{\lambda N/2^d}\log(2+\lambda N/2^d)\right) = O_{t,\lambda}(\sqrt{N}\log N).$$

The sum stops when the scaled cutoff falls below the smallest source order. It remains to count the prime, stage-zero members. For each fixed d, their count is asymptotic to $2^{-d}(\lambda-1)N/(4t\log N)$ by the prime number theorem in the progression $1 \pmod 4$.

To justify summation, fix D. For $D < d \leq \frac{\log N}{2\log 2}$, the standard prime-counting upper bound gives $O_{t,\lambda}(N/(2^d \log N))$ terms, uniformly in this range. For larger d, even counting all positive integers below $\lambda N/2^d$ gives $O_\lambda(\sqrt{N})$ in total. Consequently the omitted tail, divided by $N/\log N$, has limiting upper bound $O_{t,\lambda}(2^{-D})$. First let N tend to infinity, then let D tend to infinity. The geometric sum $\sum_{d\geq 0} 2^{-d} = 2$ gives the asserted constant. □

B.2 Doubling both base families

Proof of Corollary 4.3. For the prime parts, fix a finite doubling range $0 \leq d \leq D$. Each scaled $\mathcal{F}_t$ part contributes leading constant $2^{-d}(\lambda-1)/(4t)$, and each scaled $\mathcal{G}_t$ part contributes $2^{-d}(\lambda-1)/(2t)$. Two pieces with distinct scale coefficients intersect only when two nonproportional fixed linear forms are prime. Their intersection has size $O_{D,t,\lambda}(N/\log^2 N)$ by the upper-bound sieve. If the coefficients are equal across the two types of piece, their primes lie in the disjoint progressions 1 and 3 modulo four, so the intersection is empty. The finite union therefore has the sum of the leading constants.

The nonprime prime powers and positive recurrence stages contribute $O_{t,\lambda}(\sqrt{N}\log N)$ after summing over all doublings, as in Corollary 4.2. The remaining prime tail with $D < d \leq \frac{\log N}{2\log 2}$ contributes at most $O_{t,\lambda}(2^{-D}N/\log N)$, uniformly in N; larger d contribute $O_{t,\lambda}(\sqrt{N})$ even if every integer is counted. First let N tend to infinity, then let D grow. The finite sum tends to twice the constant $3(\lambda-1)/(4t)$ in (24). □

B.3 The two-source lower bound

Proof of Proposition 4.4. For each prime $p \equiv 1 \pmod 4$ put $a_p = (p+1)/2$. Fix any finite set B of distinct such values. For $a \in B$ let

$$E_a = \{4ta(q+1) : q \equiv 1 \pmod 4 \text{ prime}\}.$$

Corollary 3.2, with the first prime fixed, gives these orders. For each fixed a,

$$\#(E_a \cap [N, \lambda N]) \sim \frac{\lambda - 1}{8ta} \frac{N}{\log N}.$$

If $a \neq b$, write $a = ga'$, $b = gb'$ with $(a', b') = 1$. An intersection requires $q = b'h - 1$ and $q' = a'h - 1$ for an integer $h = O_{a,b,t,\lambda}(N)$. The two distinct linear forms have nonzero determinant. The classical two-linear-form upper-bound sieve therefore gives

$$\#(E_a \cap E_b \cap [N, \lambda N]) = O_{a,b,t,\lambda}(N/\log^2 N).$$

Only fixed coefficients are used here. The upper and lower finite-union bounds imply

$$\liminf_{N\to\infty} \frac{\#(\mathcal{S}_{t,2} \cap [N, \lambda N])}{N/\log N} \geq \frac{\lambda - 1}{8t} \sum_{a\in B} \frac{1}{a}.$$

Partial summation of the prime number theorem in the progression $1 \pmod 4$ gives

$$\sum_{\substack{p\leq Y \\ p\equiv 1 \pmod 4}} \frac{1}{a_p} \sim \log\log Y,$$

so these finite reciprocal sums are unbounded. Given any desired lower constant, choose B first and then take N sufficiently large for that fixed choice. This proves convergence to infinity, without any uniform estimate in a growing set B. Finally a_p and a_q are odd, so $v_2(8ta_pa_q) = 3 + v_2(t)$ for every displayed order. □

The sieve input in the two-source proof is the classical upper bound for two distinct linear forms with fixed integer coefficients. A precise statement is reproduced as Theorem 5 of [13], with its reference to Halberstam and Richert. This proof supplies no explicit rate for the diverging factor, and it does not assume that the full two-parameter map is injective.

C A density bound for the stated product closure

This appendix concerns the completed-matrix product grammar defined below, starting with the stated seed sets. The grammar concerns orders of completed matrices; it does not describe every intermediate structured object or arbitrary iteration of other constructions. It makes no assertion that a Hadamard matrix fails to exist at any other admissible order. All logarithms are natural.

There are $(\lambda - 1)N/4 + O(1)$ admissible multiples of four in $[N, \lambda N]$. By Corollary 1.2, the proportion supplied by $\mathcal{F}_{631}$ alone is asymptotic to $1/(631 \log N)$. This tends to zero, although the number supplied tends to infinity. We now examine the larger set obtained by combining its orders with the stated products.

Small gaps and positive density must also be distinguished. A recent preprint of Mark [15], using sparse multi-base representations and Golay constructions, gives exact Hadamard gaps of size $x^{o(1)}$. That is an existing result about the full known existence set, not a consequence of the family studied here. A set with such gaps can still have density zero. We make no claim to improve the best general gap or density bounds.

C.1 A bound on the number of sources

Let $\mathcal{A} \subseteq \mathbb{N}$ contain 1, and suppose H($4a$) has been established for each $a \in \mathcal{A}$. Write

$$A(x) = \#\{a \in \mathcal{A} : a \le x\}.$$

Our assumption will be

$$A(x) = O\big(x/\log(2x)\big). \tag{25}$$

It holds if the source orders consist of the plain source family $\mathcal{F}_1$, the two base families $\mathcal{F}_{631}$ and $\mathcal{G}_{631}$, any finite list of completed orders, and all Paley orders. Indeed Proposition 4.1, or its proof with an upper cutoff, gives the required estimate for both $\mathcal{F}_1$ and $\mathcal{F}_{631}$. The normalized Paley parameters are $(q+1)/4$ for prime powers $q \equiv 3 \pmod 4$ and $(q+1)/2$ for prime powers $q \equiv 1 \pmod 4$. Prime counting and the elementary bound for nonprime prime powers give (25) for each. The same elementary bound applies to $\mathcal{G}_{631}$. A finite set adds $O(1)$ to the count. A fixed finite collection of geometric families, such as an additional family $u\,3^r$, adds only $O(\log x)$ terms and can be included as well.

The normalization uses the full integer $a = n/4$, not just the odd part of the order. Removing unbounded powers of two from the inputs would change the set to which the counting hypothesis applies.

C.2 Powers of two bound the number of leaves

Let $\mathcal{C}(\mathcal{A})$ be the smallest set of orders containing all $4a$, $a \in \mathcal{A}$, and closed under (19), Kronecker products, and doubling. Factors of orders 1 and 2 are absorbed by the identity operation and doubling.

Lemma C.1. *Every construction expression with k source leaves has the form*

$$n = 4 \cdot 2^b \prod_{i=1}^{k} a_i, \qquad a_i \in \mathcal{A}, \qquad b \ge \frac{7}{11}(k-1). \tag{26}$$

Consequently, if $v_2(n) = j \ge 2$, then

$$k \le 1 + \left\lfloor \frac{11(j-2)}{7} \right\rfloor. \tag{27}$$

Proof. The ratios of cost to leaf reduction for the three rules are 1, 2/3, and 7/11. The Kronecker ratio is 2; doubling adds cost without adding leaves. Summing over the tree gives (26). Since every a_i is an integer, $b \le j-2$, which proves (27). □

The leaf bound is sharp for this arithmetic model. Given an integer budget $B = 7s + r$, $0 \le r \le 6$, use s twelve-input nodes, $\lfloor r/2 \rfloor$ four-input nodes and $r \bmod 2$ binary nodes. Their leaf reduction is

$$11s + 3\lfloor r/2 \rfloor + (r \bmod 2) = \lfloor 11B/7 \rfloor.$$

The last equality follows by checking $r = 0, \dots, 6$. Assigning the known source H(4) to every leaf realizes equality with odd normalized inputs. Extra factors of two in an input consume part of the same budget.

C.3 A fixed number of factors remains sparse

Lemma C.2. *Under (25), for every fixed $k \geq 1$ and $\lambda > 1$,*

$$\#\{a_1 \cdots a_k \in [N, \lambda N] : a_i \in \mathcal{A}\} = O_{\mathcal{A},k,\lambda}\left(\frac{N}{\log N}(\log\log N)^{k-1}\right).$$

Proof. Partial summation in (25) gives

$$S(X) := \sum_{\substack{a \in \mathcal{A} \\ a \leq X}} \frac{1}{a} = O_{\mathcal{A}}(\log\log(3X)).$$

It suffices to count ordered tuples. A tuple with product at least N has a largest factor at least $N^{1/k}$. Choose its position in at most k ways and denote the product of the other factors by B. Then $B \leq \lambda N^{1-1/k}$, so the largest factor has at most

$$A(\lambda N/B) \leq O_{\mathcal{A},\lambda}\left(\frac{kN}{B\log N}\right)$$

possibilities. Sum this bound over the other factors. Enlarging each of their ranges to $[1, \lambda N]$ bounds the sum of their reciprocal products by $S(\lambda N)^{k-1}$. Thus the number of tuples is at most $O_{\mathcal{A},\lambda}(k^2 N S(\lambda N)^{k-1}/\log N)$, which proves the assertion for fixed k. Ties for the largest factor only overcount. □

Theorem C.3. *If (25) holds, then for every fixed $\lambda > 1$,*

$$\#\big(\mathcal{C}(\mathcal{A}) \cap [N, \lambda N]\big) = o(N).$$

Equivalently, the fraction of admissible multiples of four certified by this closure tends to zero in every such interval.

Proof. First fix $j \geq 2$ and count outputs for which $v_2(n) = j$. By Lemma C.1, both b and k in (26) range over finite sets depending only on j. For each choice, the product of the a_i lies in

$$\left[\frac{N}{4 \cdot 2^b}, \frac{\lambda N}{4 \cdot 2^b}\right].$$

Lemma C.2 gives $o(N)$ possibilities. Summing over these finite choices proves the same bound in each fixed j stratum.

Now fix $J \geq 3$. The finitely many strata $2 \leq j < J$ contribute $o(N)$ in total. Every remaining order is divisible by 2^J, so there are at most $(\lambda - 1)N/2^J + O(1)$ of them in the interval. Divide by $(\lambda - 1)N/4 + O(1)$, the number of admissible multiples of four. The limiting upper fraction is at most 2^{2-J}. Letting J tend to infinity gives zero. □

In particular, Theorem C.3 allows all generic Paley seeds, the plain source family and the two base families. The mixed products in Corollary 3.4 use exactly these inputs. Their orders can be doubled $k - 1 - c(k)$ times to give the Hadamard orders in Corollary 3.2, because $c(k) \leq k - 1$. Thus this expanded order grammar also contains those orders from structured products, without asserting closure of the structured quadruples under arbitrary operations. The proof uses the source count and the positive power-of-two cost of combining more inputs. Construction monoids of Hadamard orders are studied in [9].

The theorem shows that iterating the specified completed-matrix products from these seed sets cannot establish an almost-all theorem. A route past this obstruction must change a hypothesis, for example by providing a source set with a larger counting function, or a composition law without a fixed positive two-adic cost per added source. Either change would require a separate proof of what it covers.

D The precise count for products with Paley orders

We give the detailed application of Ford's theorem used in Theorem 4.5. In addition to its displayed leading scale, the argument gives bounds within fixed multiplicative constants of the function

$$\mathfrak{B}(x) = \frac{x}{\log x} \exp\bigl\{C(\log_3 x - \log_4 x)^2 + D\log_3 x - (D + \tfrac{1}{2} - 2C)\log_4 x\bigr\},$$

where $C = 0.8178146464\ldots$ and $D = 2.1769687436\ldots$ are Ford's constants [12, Theorem 1]. More precisely, for every fixed $\lambda > 1$ and Hadamard order h divisible by four,

$$\#\bigl(\mathcal{E}_h \cap [N, \lambda N]\bigr) \asymp_{\lambda,h} \mathfrak{B}(N). \tag{28}$$

Proof of the counting assertion in Theorem 4.5. Define a multiplicative function f by

$$f(2^a) = 4^a, \qquad f(p^a) = (p+1)^a \quad (p \text{ odd prime},\ a \geq 1), \qquad f(1) = 1.$$

Its range is exactly $\mathcal{M}_+$. One inclusion follows because the factor $4 = f(2)$ is already the generator $3 + 1$. For the reverse inclusion, map a product $\prod_{p \text{ odd}} (p+1)^{a_p}$ to the integer $\prod_{p \text{ odd}} p^{a_p}$. Thus equality of the ranges requires no injectivity of the prime-product parameterization.

The function meets Ford's hypotheses [12, Theorem 14]. The set $\{f(p) - p : p \text{ prime}\}$ equals $\{1, 2\}$. Also $f(n) \geq n$, so for any fixed $0 < \delta < 1/2$,

$$\sum_{n \text{ square-full}} \frac{n^\delta}{f(n)} \leq \sum_{n \text{ square-full}} n^{-(1-\delta)} < \infty.$$

The last series converges by its Euler product: the nonconstant term at p is $\sum_{a \geq 2} p^{-a(1-\delta)} = O_\delta(p^{-2(1-\delta)})$, and $2(1-\delta) > 1$.

Let $V_f(x)$ count the distinct values of f up to x. Ford's Theorems 1 and 14 give $V_f(x) \asymp \mathfrak{B}(x)$. His Theorems 4 and 14 give the local estimate

$$V_f(x+y) - V_f(x) \asymp \frac{y}{x+y} V_f(x+y)$$

when $y \geq x^\theta$ and $\theta < 1$ is admissible in the prime-interval estimate stated there. For example, one may use $\theta = 0.525$. For fixed $\lambda > 1$, take $x = N/h$ and $y = (\lambda - 1)N/h$; the required inequality holds for all sufficiently large N. Multiplication by h is injective, so the left side counts $\mathcal{E}_h \cap (N, \lambda N]$. Inclusion of the lower endpoint changes the count by at most one. Finally, $\mathfrak{B}(\lambda N/h) \asymp_{\lambda,h} \mathfrak{B}(N)$, which proves (28). Expanding the exponent and absorbing bounded multiplicative constants into $o((\log_3 N)^2)$ gives the shorter expression in Theorem 4.5. □

E A further consequence for inequivalent matrices

The same finite constructions also give families of mutually inequivalent matrices at a fixed order. The companion paper [1] supplies two matrices at order $h = 885924$: the scalar-restriction representative A has rank $r_A = 246090$ over $\mathbb{F}_3$, while the standard Paley-I representative B has rank $r_B = 442962$.

For $m = 2^\ell$ let $W_{u,v} = (-1)^{u \cdot v}$ be the Sylvester matrix, indexed by $u, v \in \mathbb{F}_2^\ell$. Choose an order-$h$ Hadamard block K_v independently for each v and define

$$H_{(u,i),(v,j)} = W_{u,v}(K_v)_{i,j}.$$

This classical block construction also appears in research notes on Hadamard permanents in Davis's repository [14]. That exposition suggested applying it to the two matrices above.

Proposition E.1. *For every $\ell \geq 0$, the block construction gives at least $2^\ell + 1$ pairwise inequivalent real Hadamard matrices of order $885924 \cdot 2^\ell$. Their ranks over $\mathbb{F}_3$ are*

$$2^\ell \cdot 246090 + k \cdot 196872, \qquad 0 \leq k \leq 2^\ell.$$

Equivalence may include independent signed row and column permutations and transposition.

Proof. There is an exact factorization $H = (W \otimes I_h)\,\mathrm{diag}(K_v)$. Its entries are signs and its Gram matrix is $(W \otimes I_h)(hI)(W^\mathsf{T} \otimes I_h) = mhI$. Since $WW^\mathsf{T} = mI$ and $3 \nmid m$, W is invertible over $\mathbb{F}_3$, so the rank of H is the sum of the ranks of the K_v. Choose k copies of B and $m - k$ copies of A. The displayed ranks are distinct, and signed permutations and transposition preserve rank. □

For example, at order 1771848 the three resulting ranks are 492180, 689052 and 885924. One explicit choice puts B in the first k column blocks and A in the rest. Only the two seed ranks enter the calculation.

Thus the construction gives $m + 1$ distinct equivalence classes at orders already obtained by doubling 885924. The rank argument certifies $m + 1$ classes among the 2^m block assignments; comparison with other published representatives is a separate question.

F Reproduction and proof scope

The source package accompanying this article includes a self-contained finite replay bundle in `anc/replay/`. After extracting the package, use Python 3.11 or later and run

```
cd anc/replay
python -m pip install "numpy>=1.26" "sympy>=1.12" "pytest>=8"
python run_replays.py --tests
```

The runner executes the four finite checks below and the theory tests. To run the arithmetic check separately, use

```
python -m theory.code.density_checks \
  --ledger certificates/scalar-lift/completed-order-inventory-v3.json \
  --output /tmp/hadamard-interval-counts.json
```

The default parameters are $t = 631$ and maximum order 10^9. The program counts distinct orders, records collisions, checks their exact powers of two, and independently verifies the leaf budget through 128 and the minimum-cost formula through 256 leaves. Passing a different `-t` changes the conditional arithmetic family; it does not verify a design at that parameter. To compile the manuscript, return to the root of the extracted source package and run

```
latexmk -pdf -interaction=nonstopmode -halt-on-error main.tex
```

From `anc/replay/`, the other finite controls run with:

```
python -m theory.code.structured_sources \
  --output /tmp/structured-source-controls.json
python -m theory.code.paley_t_product --prime 43 \
  --output /tmp/paley-t-product.json
python -m theory.code.block_bootstrap \
  --output /tmp/block-bootstrap.json
```

The first checks small structured source products, the mixed-input orders for three, four and twelve sources, and their comparison with using the ordinary order-2524 matrix as a separate input. The second checks a prime-field Paley block construction and uses the explicit periodic T-matrices, with an implicit final matrix. The all-prime-power theorem is proved mathematically; this finite command does not enumerate general extension fields. The third checks full Gram matrices and modular ranks for small examples, and derives the large block-family ranks from the exact order-885924 rank certificate. These commands use implicit entry formulas for large matrices and do not allocate their full arrays or repeat a dense rank calculation at that order.

The all-parameter induction and the analytic counting consequences are proved in the text, using the stated prime-counting, sieve and Ford theorems. The finite programs check the stated examples and arithmetic identities. The general counting results use the cited analytic theorems. The fixed design at $t = 631$ and its exact verification are given in [1]. The completed-order ledger and the original Lean formalization belong to that companion work; the present paper adds mathematical consequences and finite executable controls.

References

[1] A. Kolpakov, *Butson towers and high-rank Hadamard matrices*, companion manuscript, Hexagon-Math 2611.01070, 2026. https://hexagonmath.org/2611.01070.

[2] J. Cooper and J. Wallis, *A construction for Hadamard arrays*, Bull. Austral. Math. Soc. **7** (1972), 269–277. https://doi.org/10.1017/S0004972700045019.

[3] R. J. Turyn, *An infinite class of Williamson matrices*, J. Combin. Theory Ser. A **12** (1972), 319–321. https://doi.org/10.1016/0097-3165(72)90095-7.

[4] J. Seberry and N. A. Balonin, *Two infinite families of symmetric Hadamard matrices*, Australas. J. Combin. **69** (2017), 349–357. https://ajc.maths.uq.edu.au/pdf/69/ajc_v69_p349.pdf.

[5] E. Spence, *An infinite family of Williamson matrices*, J. Austral. Math. Soc. Ser. A **24** (1977), 252–256. https://doi.org/10.1017/S1446788700020255.

[6] K. S. Kedlaya, *Analytic Number Theory*, Chapter 5, Theorem 5.10, online lecture notes, consulted 29 November 2026. https://kskedlaya.org/ant/chapter-5.html.

[7] R. Craigen, J. Seberry and X.-M. Zhang, *Product of four Hadamard matrices*, J. Combin. Theory Ser. A **59** (1992), 318–320. https://documents.uow.edu.au/~jennie/WEBPDF/168_1992.pdf.

[8] W. de Launey, *A product for twelve Hadamard matrices*, Australas. J. Combin. **7** (1993), 123–127. https://ajc.maths.uq.edu.au/pdf/7/ocr-ajc-v7-p123.pdf.

[9] W. de Launey and D. M. Gordon, *On the density of the set of known Hadamard orders*, Cryptogr. Commun. **2** (2010), 233–246. https://arxiv.org/abs/1004.4872v1.

[10] J. Seberry and M. Yamada, *On the products of Hadamard matrices, Williamson matrices and other orthogonal matrices using M-structures*, J. Combin. Math. Combin. Comput. **7** (1990), 97–137, Theorem 4 and Corollary 25. https://documents.uow.edu.au/~jennie/WEBPDF/139_1990.pdf.

[11] N. A. Balonin and D. Ž. Đoković, *Negaperiodic Golay pairs and Hadamard matrices*, arXiv:1508.00640v1, 4 August 2015, Propositions 2 and 8. https://arxiv.org/abs/1508.00640v1.

[12] K. Ford, *The distribution of totients*, Ramanujan J. **2** (1998), 67–151. Revised version arXiv:1104.3264v2, 14 July 2013, Theorems 1, 4 and 14. https://arxiv.org/abs/1104.3264v2.

[13] F. Luca, J. Ouaknine and J. Worrell, *A universal Skolem set of positive lower density*, LIPIcs **241** (MFCS 2022), 73:1–73:12, Theorem 5. https://doi.org/10.4230/LIPIcs.MFCS.2022.73.

[14] C. Davis (repository curator), *Vanishing Hadamard permanents*, research note in *Solved conjectures*, consulted 29 November 2026. Pinned research note, commit 959a0e7.

[15] J. Mark, *Sparse multi-base representations and asymptotic existence of Hadamard matrices*, aiXiv/Hexagon 2611.00465v1, 5 November 2026, Theorems 4.2 and 6.1. https://aixiv.online/abs/2611.00465v1. Author repository, checked at commit 971eea9.