REACHABLE CARDINALITIES OF THE BUTSON MIXED SCHUR CONSTRUCTION, AND A QUANTUM LATIN SQUARE OF ORDER SEVEN WITH CARDINALITY 45

KOREA SUPERINTELLIGENCE LABS

Abstract. A *quantum Latin square* of order n is an $n \times n$ array of unit vectors of $\mathbb{C}^n$ every row and every column of which is an orthonormal basis; its *cardinality* is the number of entries once vectors differing by a global phase are identified. Zhang, Lv and Cao tabulate, at the orders their determination of the spectrum leaves open, which cardinalities are known to occur and which are uncertain; the order-seven row of that table prints 45 as uncertain. We exhibit a quantum Latin square of order seven whose cardinality is exactly 45. The witness is a mixed Schur product $\Phi(H,K)_{ij} = 7^{-1/2}(h_i \odot k_j)$ of two Butson Hadamard matrices $H, K \in \mathrm{BH}(7,6)$, presented by explicit exponent matrices over $\mathbb{Z}/6$, and the certificate is exact and integral: for a Butson pair the cardinality is the size of a sumset $|S+T|$ of two n-element subsets of $(\mathbb{Z}/m)^n$ modulo constants, and at $m = 6$ the Butson condition is *equivalent* to two integer equations on each column difference profile. The sufficient shift criterion previously used to assemble such witnesses certifies none of the 84 ordered pairs of distinct columns of ours, and it is the equivalence that replaces it. We also record, general in n and m, the ceiling $\operatorname{card}\Phi(H,H) \le n(n+1)/2$ for the symmetric construction — sharp at $n = 7$, where it gives the value 28 that the same table lists as attainable and isolated — and the bracket $n \le \operatorname{card}\Phi(H,K) \le n^2$. In particular the dichotomy $|S+T| \in \{p, p^2\}$, which holds at a prime order p for matrices monomially equivalent to the Fourier matrix F_p, fails once the modulus is allowed to differ from the order. Every theorem below is machine-checked in Lean 4; the exhaustive enumerations reported alongside them are stated as measurements and are marked as such.

1. Introduction

Let $n \ge 1$. A *quantum Latin square* of order n, introduced by Musto and Vicary [5] as the datum from which a family of unitary error bases is built, is an $n \times n$ array $\Phi = (\varphi_{ij})_{0 \le i,j < n}$ of unit vectors $\varphi_{ij} \in \mathbb{C}^n$ such that each row $(\varphi_{i0}, \dots, \varphi_{i,n-1})$ and each column $(\varphi_{0j}, \dots, \varphi_{n-1,j})$ is an orthonormal basis of $\mathbb{C}^n$. Two entries are identified when they span the same complex line, and the *cardinality* $\operatorname{card}\Phi$ is the number of lines so obtained. A classical Latin square, read as an array of standard basis vectors, has cardinality n; an array whose n^2 entries are pairwise non-proportional has cardinality n^2. The problem is to decide which of the values in between occur:

$$\mathrm{Spec}(n) \;:=\; \{\operatorname{card}\Phi \;:\; \Phi \text{ a quantum Latin square of order } n\} \;\subseteq\; \{n, n+1, \dots, n^2\}.$$

Zhang, Lv and Cao [11] survey the state of this question and tabulate, order by order, the values known to be attainable against those whose status is uncertain. Their Table 6, captioned "Attainable and uncertain cardinalities of a QLS(v) for $v = 6, 7, 9, 11, 23$", carries one row for each of those five orders and no other; its order-seven row reads

$$\text{(1)} \qquad \text{attainable: } [7,23] \setminus \{8\} \cup \{28, 43, 44, 46, 47, 48, 49\}, \qquad \text{uncertain: } [24,27] \cup [29,42] \cup \{45\},$$

where $[a,b]$ denotes the integer interval. (Row and caption are transcribed from the LaTeX source of the current version, arXiv:2607.19969v2 of 23 July 2026; the copy read here is byte-identical to the e-print served by arXiv on 30 August 2026, and the table is numbered 6 in that version.) The single isolated uncertain value of (1) is 45: it is wedged between the attainable values 44 and 46, and every other uncertain value of the row belongs to a block. The present paper settles it.

Theorem 1.1 (Theorem 5.1 below). *There is a quantum Latin square of order seven whose cardinality is exactly* 45.

Date: August 30, 2026.

The route is a construction of Xu [8]. Given two complex Hadamard matrices H and K of order n, written by their *columns* $H = (h_0, \ldots, h_{n-1})$, $K = (k_0, \ldots, k_{n-1})$, the array

$$\Phi(H,K)_{ij} \;=\; n^{-1/2}\,(h_i \odot k_j), \qquad 0 \le i,j < n, \tag{2}$$

formed with the entrywise (Schur) product $\odot$, is a quantum Latin square of order n (Proposition 1, “Mixed Hadamard products”, of [8]), and it is the source of the order-six cardinalities 27, 32 and 35 of that paper. When both matrices are *Butson* — all entries are m-th roots of unity, so $H = \zeta_m^A$ and $K = \zeta_m^B$ for exponent matrices A, B over $\mathbb{Z}/m$ — the line spanned by the cell (i,j) is determined by the class of the exponent vector $A_{\cdot i} + B_{\cdot j}$ modulo the constant vectors, whence

$$\operatorname{card}\Phi(H,K) \;=\; |S+T|, \qquad S = \{[A_{\cdot i}]\}_i, \quad T = \{[B_{\cdot j}]\}_j \quad \text{in } V := (\mathbb{Z}/m)^n/\text{constants}, \tag{3}$$

the size of a sumset of two n-element subsets of an abelian group. The reformulation (3) is Xu’s. It is stated, for a single Butson matrix, in the Discussion section of the first version [9] of [8]: “For a Butson matrix $H_{rs} = \zeta^{A_{rs}}$, the collision problem becomes an exact sumset problem for the column vectors of the exponent matrix.” The same section names the mixed construction (2) with two different matrices as future work at order six — “Further cardinalities above 23 may be sought either by refining direct-sum incidence patterns or by using two possibly different Hadamard matrices, $w_{ij} = \frac{1}{\sqrt{6}}(h_i \odot g_j)$, which retain the row and column orthogonality argument but no longer impose symmetry.” Both sentences are present only in v1; they do not appear in v2 or in the current v3, whose Discussion section was rewritten, and (2) is a proposition there rather than a proposal.

Formula (3) makes the cardinality of a Butson mixed Schur product a finite, integral quantity, and it turns the spectrum question into a question about the map

$$(n,m) \;\longmapsto\; \operatorname{Reach}(n,m) \;:=\; \{\, |S+T| \;:\; H,K \in \mathrm{BH}(n,m)\,\} \;\subseteq\; \operatorname{Spec}(n), \tag{4}$$

which we call the *reach* of the construction at (n,m). What has to be supplied to move from a reachable value to a theorem is a certificate that the two matrices really are Butson. The assembly used previously discharges this with a sufficient test — the difference profile of two columns is invariant under a nonzero shift of $\mathbb{Z}/m$, which forces the corresponding sum of roots of unity to vanish — and that test is silent for our witness: it holds for *none* of the 84 ordered pairs of distinct columns of the two matrices (Theorem 5.2). What discharges it instead is a *complete* criterion at $m = 6$, Proposition 3.1: since ζ_6 has degree two over $\mathbb{Q}$, the vanishing of an integer combination of sixth roots of unity is exactly the vanishing of two integer coordinates. Being an equivalence, that criterion also refutes, and Theorem 5.4 uses it to reject a one-entry perturbation of the witness — a separation a merely sufficient test could not exhibit.

Two structural facts frame the answer at order seven. The symmetric construction $K = H$ obeys the ceiling $\operatorname{card}\Phi(H,H) \le n(n+1)/2$ at every order and every modulus (Theorem 4.1), because $\Phi(H,H)_{ij}$ and $\Phi(H,H)_{ji}$ span the same line; Xu states this at $n = 6$, where it gives $\binom{7}{2} = 21$ (Proposition 2 of [8]), with a proof that does not use the six. At $n = 7$ the ceiling is $\binom{8}{2} = 28$, it is attained (Theorem 4.3), and 28 is precisely the isolated attainable value that sits immediately below the uncertain block $[29, 42]$ of (1). The mixed construction, on the other hand, steps over that block: in the exhaustive computations reported in §8 — computations that are outside the formal development — the values it reaches at order seven are 28 and $43, \ldots, 49$, at each of the moduli 6, 12 and 18, so 45 is the only uncertain value of (1) any of them reaches.

Finally, (3) has a clean consequence for the Fourier matrix F_p at a prime p, and for every matrix monomially equivalent to it: the column classes form a coset of a cyclic subgroup of order p, a sumset of two cosets is a coset of the subgroup they generate, and hence $|S+T| \in \{p, p^2\}$. Theorem 7.1 records that this dichotomy does not survive the passage to $m \ne n$: at $(n,m) = (7,6)$ the value 45 is reached, and $45 \notin \{7, 49\}$.

What is not claimed. Nothing here touches the blocks $[24, 27]$ and $[29, 42]$ of (1), nor any order other than seven; the equality $\operatorname{Reach}(7,6) = \{28\} \cup [43, 49]$ is a computation reported in §8, not a theorem; and neither the construction (2) nor the reformulation (3) is ours. What is new is the value: the objects $\mathrm{BH}(7,6)$ are classified, the construction is published, and we have not found the cardinality they produce at order seven on record. The order-six constructions of [7, 8], the most recent order-six witness [2] and the parallel treatment of the cardinality question in [10] contain no order-seven cardinality obtained this way. The searches behind that sentence, re-run on 30 August 2026, are these. The arXiv metadata query `all:"quantum Latin square"` returns 23 records in total — the whole literature is enumerable, and was enumerated; the most recent is [2] of 12 August 2026, and none of the 23 treats order seven. `all:"Butson" AND all:"quantum Latin"` returns exactly one record, namely [8]; `all:"Butson" AND all:"sumset"` and `abs:"quantum Latin square" AND abs:"cardinalit"` return none (a positive control returns 45). In the Semantic Scholar citation graph [11] has exactly two citing papers, [8] and [2], both about order six. Of the 23 records the ones with a general construction settle intervals at orders $4m$, $6m$ and 8, or treat mutually orthogonal or diagonal squares, and [10] in particular has no order-seven content, no Hadamard construction, and mentions 45 only as an open value at order *eight*. Since [11] appeared after all of these and prints 45 as uncertain at order seven, the negative rests ultimately on that table.

2. Preliminaries

Throughout, $m \geq 1$ and $n \geq 1$ are integers, $\zeta_m = e^{2\pi i/m}$, and μ_m is the group of m-th roots of unity. For $a \in \mathbb{Z}/m$ we write ζ_m^a for ζ_m raised to any integer representative of a; this is well defined. Indices i, j, r, s run over $\{0, 1, \ldots, n-1\}$, and we identify that set with $\mathbb{Z}/n$ only for indexing, never algebraically.

Definition 2.1 (Butson matrix)**.** $\mathrm{BH}(n, m)$ is the set of $n \times n$ matrices H with all entries in μ_m and $HH^* = nI_n$. Every such H is ζ_m^A, meaning $H_{ri} = \zeta_m^{A_{ri}}$, for a unique exponent matrix $A \in M_n(\mathbb{Z}/m)$.

Definition 2.2 (column orthogonality and difference profiles)**.** Let $A \in M_n(\mathbb{Z}/m)$ and let $a_i = (A_{ri})_{0 \leq r < n} \in (\mathbb{Z}/m)^n$ be its i-th column. Call A *column-orthogonal* if

$$\sum_{r=0}^{n-1} \overline{\zeta_m^{A_{ri}}}\, \zeta_m^{A_{ri'}} = 0 \qquad \text{for all } i \neq i'. \tag{5}$$

For $i \neq i'$ the *difference profile* is the function $d^A_{ii'} \colon \mathbb{Z}/m \to \mathbb{Z}_{\geq 0}$,

$$d^A_{ii'}(a) = \#\{\, r \;:\; A_{ri'} - A_{ri} = a \,\}, \qquad \text{so} \qquad \sum_{a \in \mathbb{Z}/m} d^A_{ii'}(a) = n \quad \text{and} \quad \sum_r \overline{\zeta_m^{A_{ri}}}\, \zeta_m^{A_{ri'}} = \sum_a d^A_{ii'}(a)\, \zeta_m^a.$$

Condition (5) says that the columns of ζ_m^A are pairwise orthogonal, i.e. that $(\zeta_m^A)^* \zeta_m^A = nI_n$; for a square matrix this is equivalent to $\zeta_m^A \in \mathrm{BH}(n, m)$, and we use the two descriptions interchangeably. All the certificates below are stated on columns, which is the side the construction (2) consumes.

Definition 2.3 (mixed Schur product)**.** For $A, B \in M_n(\mathbb{Z}/m)$ put $\sigma_{ij}(r) = A_{ri} + B_{rj} \in \mathbb{Z}/m$ and

$$\Phi(A, B)_{ij} \;:=\; n^{-1/2} \big(\zeta_m^{\sigma_{ij}(0)}, \ldots, \zeta_m^{\sigma_{ij}(n-1)} \big) \;\in\; \mathbb{C}^n.$$

This is (2) for $H = \zeta_m^A$, $K = \zeta_m^B$.

Lemma 2.4 (proportionality is an identity of exponents)**.** *Two vectors $(\zeta_m^{u_r})_r$ and $(\zeta_m^{w_r})_r$ span the same complex line if and only if $u_r + w_s = u_s + w_r$ for all r, s, i.e. if and only if $u - w$ is a constant vector of $(\mathbb{Z}/m)^n$.*

Proof. Both vectors have nonvanishing coordinates, so they are proportional if and only if $\zeta_m^{u_r} \zeta_m^{w_s} = \zeta_m^{u_s} \zeta_m^{w_r}$ for all r, s, and $\zeta_m^x = \zeta_m^y$ for $x, y \in \mathbb{Z}/m$ if and only if $x = y$. □

Accordingly we call two cells *collinear*, written $(i, j) \sim (i', j')$, when

$$\sigma_{ij}(r) + \sigma_{i'j'}(s) = \sigma_{ij}(s) + \sigma_{i'j'}(r) \qquad \text{for all } r, s. \tag{6}$$

By Lemma 2.4 this is exactly the statement that $\Phi(A, B)_{ij}$ and $\Phi(A, B)_{i'j'}$ span the same line, and (3) is the observation that the equivalence classes of $\sim$ are indexed by the sums $[a_i] + [b_j]$ in V.

Definition 2.5 (the reach)**.** Let $k \geq 0$. Say that *k is reachable at* (n, m), written $k \in \mathrm{Reach}(n, m)$, if there are column-orthogonal $A, B \in M_n(\mathbb{Z}/m)$ and a labelling $\lambda \colon \{0, \ldots, n-1\}^2 \to \mathbb{Z}_{\geq 0}$ such that

(i) $(i,j) \sim (i',j')$ *if and only if* $\lambda(i,j) = \lambda(i',j')$;
(ii) $\lambda(i,j) < k$ for all i,j; and
(iii) every $t \in \{0,\dots,k-1\}$ equals $\lambda(i,j)$ for some i,j.

Write $k \in \mathrm{Reach}^{\mathrm{s}}(n,m)$ for the same with $B = A$.

Conditions (ii) and (iii) say that λ maps onto $\{0,\dots,k-1\}$; with (i) they say that λ induces a bijection from the collinearity classes onto $\{0,\dots,k-1\}$, so k is pinned from both sides. Requiring (i) to be an equivalence, and not merely the implication from collinearity to equality of labels, is what forbids a labelling that merges two classes or splits one; both perturbations are carried out on the order-seven witness in §6, and both are refuted.

3. The complete criterion, the bridge, and the bracket

The three statements of this section are the working layer. They are proved for all n and m (respectively all n, at $m = 6$), with no enumeration.

Proposition 3.1 (complete Butson criterion at $m = 6$)**.** *Let $A \in M_n(\mathbb{Z}/6)$ and abbreviate $d_a = d^A_{ii'}(a)$. Then A is column-orthogonal if and only if for every ordered pair $i \neq i'$ the two integer equations*

$$d_0 - d_2 - d_3 + d_5 = 0 \qquad \textit{and} \qquad d_1 + d_2 - d_4 - d_5 = 0 \tag{7}$$

hold.

Proof. Since ζ_6 has degree two over $\mathbb{Q}$, the pair $1, \zeta_6$ is a $\mathbb{Z}$-basis of $\mathbb{Z}[\zeta_6]$, and $\zeta_6^2 = \zeta_6 - 1$, $\zeta_6^3 = -1$, $\zeta_6^4 = -\zeta_6$, $\zeta_6^5 = 1 - \zeta_6$. Hence

$$\sum_{a \in \mathbb{Z}/6} d_a \zeta_6^a = (d_0 - d_2 - d_3 + d_5) + (d_1 + d_2 - d_4 - d_5)\,\zeta_6,$$

and an integer combination of a $\mathbb{Z}$-basis vanishes if and only if both coordinates do. Now apply Definition 2.2. □

Two remarks on Proposition 3.1. First, 6 is the smallest modulus with two distinct prime divisors, so the counting obstruction available at prime-power moduli — a vanishing sum of N roots of unity of order p^k forces $p \mid N$, because the p^k-th cyclotomic polynomial takes the value p at 1 — is vacuous here, which is exactly why the $\mathrm{BH}(n,6)$ row of the classification tables is the awkward one. Second, (7) is an *equivalence*: it certifies a Butson matrix and refutes a non-Butson one with the same computation. The general structure theory of vanishing sums of roots of unity behind such criteria is Lam and Leung's [3].

Proposition 3.2 (collinearity at a base point)**.** *Fix $t \in \{0,\dots,n-1\}$. Then* (6) *holds if and only if*

$$\sigma_{ij}(r) - \sigma_{i'j'}(r) = \sigma_{ij}(t) - \sigma_{i'j'}(t) \qquad \textit{for all } r. \tag{8}$$

Proof. (6) at (r,t) is (8) at r; conversely (8) at r minus (8) at s is (6) at (r,s). □

Proposition 3.2 is what makes the order-seven certificate cheap: testing (6) for one quadruple costs n^2 comparisons, testing (8) costs n, and there are n^4 quadruples.

Theorem 3.3 (from a reachable value to a quantum Latin square)**.** *If $k \in \mathrm{Reach}(n,m)$, then there is a quantum Latin square Φ of order n with* $\operatorname{card}\Phi = k$.

Proof sketch. Take A, B, λ as in Definition 2.5 and $\Phi = \Phi(A,B)$. For two cells in the same row i, the factor $\zeta_m^{A_{ri}}$ cancels against its conjugate coordinatewise, so

$$\sum_r \overline{\Phi_{ij}(r)}\,\Phi_{ij'}(r) = \tfrac{1}{n} \sum_r \overline{\zeta_m^{B_{rj}}}\,\zeta_m^{B_{rj'}},$$

which vanishes for $j \neq j'$ because B is column-orthogonal; symmetrically, two cells in the same column produce the corresponding sum for A. Every entry has norm one by construction. Hence Φ is a quantum Latin square. Its cardinality is the number of classes of the relation $\sim$, and by Lemma 2.4 that relation is (6); conditions (i)–(iii) of Definition 2.5 say that λ induces a bijection from the classes onto $\{0,\dots,k-1\}$, so $\operatorname{card}\Phi = k$. □

Proposition 3.4 (the bracket)**.** *Let $n \geq 1$. If $k \in \mathrm{Reach}(n,m)$ then $n \leq k \leq n^2$.*

Proof. For the upper bound, (iii) exhibits k distinct cells among the n^2 available. For the lower bound, fix a row i and suppose $(i,j) \sim (i,j')$. By (6) the vector $(B_{rj'} - B_{rj})_r$ is a constant c, so

$$\sum_r \overline{\zeta_m^{B_{rj}}}\, \zeta_m^{B_{rj'}} = n\, \zeta_m^c \neq 0,$$

contradicting column-orthogonality of B unless $j = j'$. So the n cells of a row lie in n distinct classes, and λ is injective on them; with (ii) this gives $n \leq k$. □

The lower bound is where column-orthogonality of the *second* matrix is load-bearing: for an arbitrary pair of exponent matrices an entire row can collapse into one class.

4. The symmetric ceiling

Theorem 4.1 (symmetric ceiling, general in n and m)**.** *If $k \in \mathrm{Reach}^{\mathrm{s}}(n,m)$ then $2k \leq n(n+1)$.*

Proof. With $B = A$ we have $\sigma_{ij}(r) = A_{ri} + A_{rj} = \sigma_{ji}(r)$, so (6) holds for the pair of cells (i,j) and (j,i), and $\lambda(i,j) = \lambda(j,i)$ by Definition 2.5(i). Every value of λ is therefore attained on the closed upper triangle $U = \{(i,j) : i \leq j\}$, so $k \leq |U|$ by (i)–(iii). Writing $L = \{(i,j) : j \leq i\}$ we have $U \cup L$ the full grid, $U \cap L$ the diagonal, and $|L| = |U|$ by the coordinate swap; hence $2|U| = |U| + |L| = |U \cup L| + |U \cap L| = n^2 + n$ and $2k \leq n(n+1)$. □

The count is carried out without dividing by two, which is why the statement is phrased as $2k \leq n(n+1)$. Xu [8] states this bound at $n = 6$, in the form $\mathrm{card}\,\Phi(H) \leq \binom{7}{2} = 21$ and with the same proof — the symmetry $\Phi(H,H)_{ij} = \Phi(H,H)_{ji}$ leaves at most one class per unordered pair $\{i,j\}$ — and that proof nowhere uses the value of n; the content of Theorem 4.1 is only that it is written down for all n and m.

Corollary 4.2. $29 \notin \mathrm{Reach}^{\mathrm{s}}(7,6)$*, since* $2 \cdot 29 = 58 > 56 = 7 \cdot 8$*. By Theorem 4.1 the same holds for every* $k \geq 29$ *and every modulus* m*, so the whole uncertain block* $[29,42]$ *of* (1) *lies above the symmetric ceiling at order seven.*

The ceiling at $n = 7$ is $\binom{8}{2} = 28$, and it is attained.

Theorem 4.3 (the ceiling is sharp at order seven)**.** $28 \in \mathrm{Reach}^{\mathrm{s}}(7,6)$*, witnessed by* $H = \zeta_6^A$ *for the matrix* A *of* (9) *below with the labelling*

$$\Lambda^{\mathrm{s}} = \begin{pmatrix} 0 & 4 & 5 & 9 & 18 & 20 & 21 \\ 4 & 7 & 10 & 16 & 26 & 22 & 24 \\ 5 & 10 & 11 & 17 & 27 & 23 & 25 \\ 9 & 16 & 17 & 19 & 2 & 3 & 1 \\ 18 & 26 & 27 & 2 & 12 & 15 & 6 \\ 20 & 22 & 23 & 3 & 15 & 8 & 13 \\ 21 & 24 & 25 & 1 & 6 & 13 & 14 \end{pmatrix}.$$

Consequently $2 \cdot 28 = 7 \cdot 8$ *realises the bound of Theorem 4.1 with equality, and there is a quantum Latin square of order seven with cardinality* 28.

The value 28 is listed as attainable in (1), so Theorem 4.3 is a reproduction of published data rather than a new value; we record it because of where 28 sits. It is an isolated attainable value directly below the uncertain block $[29,42]$, and Theorem 4.1 identifies it as exactly the roof of the symmetric construction. The mixed construction of the next section is what steps over that block.

5. A quantum Latin square of order seven with cardinality 45

Fix $m = 6$ and $n = 7$ and let $A, B \in M_7(\mathbb{Z}/6)$ be

$$A = \begin{pmatrix} 0&0&0&0&0&0&0\\ 0&1&1&2&4&4&4\\ 0&3&4&1&1&3&5\\ 0&4&1&4&2&1&4\\ 0&0&3&4&1&4&2\\ 0&2&5&4&4&2&1\\ 0&4&3&1&4&0&2 \end{pmatrix}, \qquad B = \begin{pmatrix} 0&0&0&0&0&0&0\\ 0&1&2&3&3&5&5\\ 0&2&5&0&3&2&4\\ 0&2&5&3&0&4&2\\ 0&5&1&4&4&2&2\\ 0&4&3&0&2&4&1\\ 0&4&3&2&0&1&4 \end{pmatrix}, \tag{9}$$

whose columns are, read downwards,

$$A:\ 0000000,\ 0134024,\ 0141353,\ 0214441,\ 0412144,\ 0431420,\ 0454212,$$

$$B:\ 0000000,\ 0122544,\ 0255133,\ 0303402,\ 0330420,\ 0524241,\ 0542214.$$

Both are dephased: the first row and the first column vanish. $\mathrm{BH}(7,6)$ is known to be nonempty, and to consist of exactly two matrices up to monomial equivalence: this is the $(n,q) = (7,6)$ entry of Table 2 of [4], reproduced as the $n = 7$ entry of the $\mathrm{BH}(n,6)$ row $1, 1, 1, 2, 0, 4, 2, 36, 17, 34, 0, 8703$ of Table 4.5 of [6]. The examples themselves are older: [4] attributes them to Brock [1] and, "independently but slightly later", to Petrescu. So the objects are not new; what is new is the cardinality the pair produces.

Theorem 5.1. *Let A, B be as in (9). Then ζ_6^A and ζ_6^B lie in $\mathrm{BH}(7,6)$; $45 \in \mathrm{Reach}(7,6)$, witnessed by the labelling*

$$\Lambda = \begin{pmatrix} 0&10&22&23&28&40&42\\ 13&21&26&35&32&7&3\\ 15&19&28&36&33&2&5\\ 20&27&31&39&43&12&17\\ 34&41&1&9&16&27&29\\ 35&44&4&14&8&30&25\\ 37&38&6&18&11&24&28 \end{pmatrix}; \tag{10}$$

and consequently there is a quantum Latin square of order seven whose cardinality is exactly 45.

Proof sketch. That $\zeta_6^A, \zeta_6^B \in \mathrm{BH}(7,6)$ is Proposition 3.1 applied to each matrix: the two integer equations (7) are evaluated on each of the $7 \cdot 6 = 42$ ordered pairs of distinct columns, each evaluation being a tally of the seven row differences into the six residues. That Λ is the collinearity relation is Proposition 3.2 at the base point $t = 0$, evaluated on all $7^4 = 2401$ quadruples (i, j, i', j') at a cost of seven exponent differences each, i.e. 16 807 comparisons in $\mathbb{Z}/6$; conditions (ii) and (iii) of Definition 2.5 are read off the 49 entries of (10) and the 45 values $0, \ldots, 44$. Definition 2.5 is then satisfied and Theorem 3.3 produces the quantum Latin square. All four searches are exhaustive and finite, and no step uses floating-point arithmetic. $\square$

The 45 classes of (10) are 42 singletons, the two pairs $\{(1,3), (5,0)\}$ and $\{(3,1), (4,5)\}$, and the single triple $\{(0,4), (2,2), (6,6)\}$; in particular $49 = 42 + 2 \cdot 2 + 3$ and $45 = 42 + 2 + 1$.

Theorem 5.2 (the shift test is empty on this witness)**.** *Call an ordered pair (i, i') of distinct columns of an exponent matrix C* shifted *if there is $t \neq 0$ in $\mathbb{Z}/m$ with $d^C_{ii'}(a + t) = d^C_{ii'}(a)$ for all a; a shifted pair is automatically orthogonal. Not one of the 42 ordered pairs of distinct columns of A, and not one of the 42 of B, is shifted.*

The profiles occurring in (9) have nonzero multiplicities of the two shapes $1 + 1 + 1 + 2 + 2$ and $1 + 1 + 2 + 3$, and neither is invariant under a nonzero rotation of $\mathbb{Z}/6$. So Theorem 5.2 is not a defect of the particular witness: the sufficient criterion is structurally unavailable here, and Proposition 3.1 — an equivalence — is what the certificate needs. In fact nothing about (9) is used:

Remark 5.3 (the shift test is vacuous at $(7,6)$)*.* Let C be any 7×7 exponent matrix over $\mathbb{Z}/6$ and $i \neq i'$. If $d^C_{ii'}(a+t) = d^C_{ii'}(a)$ for all a and some $t \neq 0$, then $d^C_{ii'}$ is constant on each coset of the subgroup $\langle t\rangle$, so $7 = \sum_a d^C_{ii'}(a)$ is divisible by $|\langle t\rangle| \in \{2,3,6\}$, which is absurd. Hence no ordered pair of distinct columns of any $\mathrm{BH}(7,6)$ is shifted, and the sufficient test certifies no order-seven witness at modulus six whatsoever. This elementary observation is ordinary mathematics recorded here for orientation, and is *not* part of the formal development; what is formalised is Theorem 5.2, the finite check on (9). Neither statement is used in the proof of Theorem 5.1, or anywhere else below.

That the complete criterion is genuinely discriminating, and not a test everything passes, is the content of:

Theorem 5.4 (separation)**.** *Let A' be A with the single entry $A_{11} = 1$ replaced by 2. Then A' is not column-orthogonal.*

The refutation runs through (7) and nothing else: the criterion is applied to A' exactly as it was applied to A and B, and it fails. Where it fails is a count outside the formal development, which certifies only that some ordered pair of distinct columns breaks (7); recomputing, twelve of the 42 ordered pairs do.

6. Controls

The certificate of Theorem 5.1 would be worthless if the labelling (10) could be perturbed and still pass, so we record that it cannot, in both directions, and that the bracket of Proposition 3.4 refutes.

Proposition 6.1 (the labelling is pinned from both sides)**.** *Let Λ^- be* (10) *with the entry $\Lambda_{51} = 44$ replaced by 43, so that the two classes 43 and 44 are merged and Λ^- takes exactly the 44 values $0,\dots,43$; and let Λ^+ be* (10) *with Λ_{22} replaced by 45 and Λ_{66} by 46, so that the unique three-cell class is split into singletons and Λ^+ takes exactly the 47 values $0,\dots,46$. Neither Λ^- nor Λ^+ satisfies condition (i) of Definition 2.5 for the pair* (9)*.*

Proposition 6.2 (the bracket refutes)**.** $6 \notin \mathrm{Reach}(7,6)$ *and* $50 \notin \mathrm{Reach}(7,6)$*.*

Proof. Proposition 3.4 with $n = 7$: $6 < 7$ and $50 > 49$. □

Together with Corollary 4.2 these are three refutations of three different shapes: a value below the order, a value above n^2, and a symmetric value above the ceiling. Each is a general bound instantiated at $(7,6)$, so Definition 2.5 is not satisfiable by a misplaced quantifier: it excludes as well as it certifies.

7. The prime-order dichotomy does not survive $m \neq n$

For the Fourier matrix $F_p = (\,\zeta_p^{ri}\,)_{r,i}$ at a prime p the column classes $[a_i] \in V = (\mathbb{Z}/p)^p/\text{constants}$ form the cyclic subgroup generated by $[(0,1,\dots,p-1)]$, of order p; more generally, any matrix obtained from F_p by rescaling rows and columns by phases has for its column-class set a coset of such a subgroup. A sumset of a coset of P_1 and a coset of P_2 is a coset of P_1+P_2, which has order p or p^2 when P_1 and P_2 have order p; so (3) gives $|S+T| \in \{p,p^2\}$ for any two such matrices, and nothing strictly between. The argument uses the order and the modulus through the same prime, and it does not extend:

Theorem 7.1. $45 \in \mathrm{Reach}(7,6)$ *and* $45 \notin \{7,49\}$*. Hence at the prime order $n = 7$ the reach of the Butson mixed Schur construction is not contained in $\{n,n^2\}$ once the modulus is allowed to differ from the order.*

Proof. Theorem 5.1 and $45 \neq 7$, $45 \neq 7^2$. □

The point is that a prime *order* says nothing on its own: the coset picture is a statement about matrices monomially equivalent to F_p, whereas $\mathrm{BH}(7,6)$ is nonempty [6], and Theorem 7.1 forces its column-class sets to escape the picture — were the two sets of (9) cosets of subgroups of order 7 of V, their sumset would have size 7 or 49, not 45. This is the precise sense in which composite moduli, and not only composite orders, give the construction room.

8. Computations outside the formal development

The statements of this section were obtained by enumeration in a separate program. They are *not* part of the formal development and are recorded as measurements: none of the theorems above depends on them, and they are reported here because they locate the witness of §5 inside the construction and because they delimit what the construction can do at order seven. The program enumerates all fully dephased $\mathrm{BH}(n,m)$ as cliques of pairwise orthogonal balanced dephased rows, collects the column-class sets of (3) up to translation, closes them under the $n!$ row permutations, and sweeps all ordered pairs; the vanishing of a sum of m-th roots of unity is decided completely, by dividing the multiplicity polynomial by the m-th cyclotomic polynomial over $\mathbb{Z}$, so the enumeration is exact at every modulus.

Remark 8.1 (the measured reach at seven cells). With "rows" the balanced dephased rows over $\mathbb{Z}/m$ of length n, "matrices" the fully dephased Butson matrices they form, and "class sets" the distinct column-class sets up to translation — before and after closing under row permutations — the enumeration gives:

(n,m)	rows	matrices	class sets	closed	$\mathrm{Reach}(n,m)$	symmetric
$(7,6)$	1 680	5 880	153	840	$\{28\}\cup[43,49]$	$\{28\}$
$(7,7)$	720	120	1	120	$\{7,49\}$	$\{7\}$
$(7,10)$	2 520	0	0	—	$\emptyset$	—
$(7,12)$	15 540	23 520	435	3 360	$\{28\}\cup[43,49]$	$\{28\}$
$(7,14)$	720	120	1	120	$\{7,49\}$	$\{7\}$
$(7,18)$	44 520	41 160	717	5 880	$\{28\}\cup[43,49]$	$\{28\}$
$(9,3)$	560	7 560	20	3 080	$\{9,18,21,27,36,54,63,72,81\}$	$\{9,18\}$

At order seven the only uncertain value of (1) that any of these moduli reaches is 45: the blocks $[24,27]$ and $[29,42]$ are untouched at $m=6,12,18$, and $m=7,14$ collapse to $\{7,49\}$. At $(7,14)$ there is a single column-class set up to translation and its entries are all even, so every $\mathrm{BH}(7,14)$ is a $\mathrm{BH}(7,7)$ in disguise — the picture predicted by the structure theory of vanishing sums of roots of unity [3]. At order nine every value of $\mathrm{Reach}(9,3)$ already lies in the attainable column of the corresponding row of [11], a clean negative. The row $(7,10)$ records that no two of the 2 520 balanced dephased rows are orthogonal, so $\mathrm{BH}(7,10)$ has no two rows and is empty — a reproduction, not a new fact: the $(n,q)=(7,10)$ entry of Table 2 of [4] is 0, and by the legend of that table a displayed number is the exact count of $\mathrm{BH}(n,q)$ matrices up to monomial equivalence.

Remark 8.2 (how hard 45 is to hit). At $(7,6)$ the $153\times 840 = 128\,520$ ordered pairs of class sets distribute over the reachable values as

$$28:153,\quad 43:612,\quad 44:2\,295,\quad 45:2\,295,\quad 46:459,\quad 47:6\,426,\quad 48:20\,196,\quad 49:96\,084.$$

So 45 is produced by 1.8% of the pairs: the obstruction was never the size of the search, it was the certificate. The value 28 occurs exactly once per class set, that is only for $K=H$: the enumeration finds cardinality 28 for *every* one of the 5 880 symmetric products at $(7,6)$, so there the ceiling of Theorem 4.1 is not merely attained but forced, and no mixed pair falls back to it.

Remark 8.3 (numerical confirmation of the witness). Independently of the exact certificate, the matrices (9) were evaluated in floating-point: $\zeta_6^A(\zeta_6^A)^*$ and $\zeta_6^B(\zeta_6^B)^*$ agree with $7I_7$ to 1.4×10^{-15}, the assembled array $\Phi_{ij}=7^{-1/2}(h_i\odot k_j)$ has every row and every column an orthonormal basis to 4.5×10^{-16}, and counting the 49 entries up to proportionality gives 45. This is a check on the transcription of (9) only; it plays no part in any proof.

Remark 8.4 (what is out of reach, and at what price). Two computations were attempted and not completed. Establishing $\mathrm{Reach}(7,6)=\{28\}\cup[43,49]$ *as a theorem* would close the blocks $[24,27]\cup[29,42]$ of (1) to this construction at order seven; it requires, besides the finite search, a dephasing lemma — every $\mathrm{BH}(n,m)$ is row- and column-scaling equivalent to a dephased one, and dephasing translates the column-class set — which is not formalised here. And $\mathrm{Reach}(9,6)$, whose uncertain targets are the order-nine blocks of [11], was abandoned: the 48 440 balanced dephased rows and their 25 505 200 compatible pairs are built in minutes, but the 8-clique enumeration ran more than half an hour of processor time without emitting a matrix count, at a peak resident set of 0.3 GB. The obstruction is time, not memory, and the remedy is orderly generation up to the row-permutation group in the manner of [4], since BH$(9,6)$ has only seventeen monomial equivalence classes [6, Table 4.5].

9. Verification

Every lemma, proposition, theorem and corollary of §§2–7 has been formally verified in Lean 4 against *Mathlib*; the remarks have not, and say so where they stand. The development contains no `sorry`, and no statement depends on axioms beyond `propext`, `Classical.choice` and `Quot.sound`; in particular nothing is delegated to compiled evaluation, so every finite check quoted above is re-run inside the kernel, and no floating-point arithmetic occurs anywhere in a proof. Proposition 3.1, Proposition 3.2, Theorem 3.3, Proposition 3.4, Theorem 4.1 and Proposition 6.2 are proved in general, with no enumeration. What rests on exhaustive computation is exactly this: the Butson property of the two matrices (9) and the refutation of the perturbed matrix of Theorem 5.4 (42 ordered pairs of distinct columns each, two integer equations per pair, each equation a tally of seven row differences); the emptiness of the shift test in Theorem 5.2 (84 ordered pairs, five nonzero shifts each); and the three labellings of (10), Λ^{s} and the two perturbations of Proposition 6.1, each tested on all $7^4 = 2401$ quadruples of cells by Proposition 3.2 at the base point $t = 0$, at seven comparisons in $\mathbb{Z}/6$ per quadruple, together with the 49 range checks and the 45 (respectively 28, 44, 47) surjectivity searches. Note that Theorem 5.4 is verified as stated, that is as the failure of (7) on A'; the count of twelve failing pairs quoted after it is not part of the formal development. Four things in all are *not* part of it and are stated above as ordinary mathematics: the enumerations of §8, the numerical evaluation of Remark 8.3, the coset argument opening §7, which motivates Theorem 7.1 but is not used in its proof, and the elementary Remark 5.3, which is used nowhere. Repository reference to be added at submission.

References

[1] B. W. Brock, *Hermitian congruence and the existence and completion of generalized Hadamard matrices*, J. Combin. Theory Ser. A **49** (1988), no. 2, 233–261; DOI 10.1016/0097-3165(88)90054-4.

[2] A. P. Das and D. Kumar, *A quantum Latin square of order six with cardinality 29*, arXiv:2608.12607v1.

[3] T. Y. Lam and K. H. Leung, *On vanishing sums of roots of unity*, J. Algebra **224** (2000), no. 1, 91–109; DOI 10.1006/jabr.1999.8089.

[4] P. H. J. Lampio, P. R. J. Östergård and F. Szöllősi, *Orderly generation of Butson Hadamard matrices*, Math. Comp. **89** (2020), no. 321, 313–331; DOI 10.1090/mcom/3453. Also arXiv:1707.02287, which has one version only; the table numbering cited above is that of the arXiv version, where Table 2 is "The number of BH(n, q) matrices up to monomial equivalence".

[5] B. Musto and J. Vicary, *Quantum Latin squares and unitary error bases*, Quantum Inf. Comput. **16** (2016), no. 15–16, 1318–1332; arXiv:1504.02715v2, DOI 10.26421/QIC16.15-16-4.

[6] G. Nuñez Ponasso, *Combinatorics of Complex Maximal Determinant Matrices*, Ph.D. dissertation, Worcester Polytechnic Institute, 2023; arXiv:2404.09040v2.

[7] Z. Xu, *Three Quantum Latin Squares of Order 6 with Cardinalities 13, 15, and 17*, arXiv:2605.15540v2.

[8] Z. Xu, *New Cardinalities for Quantum Latin Squares of Order Six*, arXiv:2607.11800v3.

[9] Z. Xu, *Quantum Latin Squares of Order Six with Cardinalities Nineteen, Twenty-One, and Twenty-Three*, arXiv:2607.11800v1. This is the first version of [8], under its original title; the two sentences quoted in §1 occur in it and in no later version.

[10] Y. Zang, M. Zheng, Z. Tian and X. Shan, *On the cardinalities of quantum Latin squares*, arXiv:2508.01972v1.

[11] Y. Zhang, M. Lv and H. Cao, *On the possible cardinalities of quantum Latin squares*, arXiv:2607.19969v2.

The preprints [2, 7, 8, 9, 10, 11] were read from their LaTeX e-prints and the pinned version numbers are the ones current on 30 August 2026: v3 is the last of {v1, v2, v3} for [8], v2 the last of two for [7] and for [11], and [2] and [10] have one version each. None of them carries a journal reference. For the two sources cited by table number, [6] is at v2 and [4] has a single arXiv version; the BH$(n, 6)$ row of Table 4.5 of [6] quoted in §5 is unchanged between its two versions.