TWELVE UNCERTAIN CARDINALITIES OF QUANTUM LATIN SQUARES OF ORDERS NINE AND ELEVEN

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 determined the set of attainable cardinalities for every order $v \geq 8$ with $v \notin \{9, 11, 23\}$ and tabulated what is known at the orders their argument leaves open. We settle twelve of the entries that table records as uncertain: cardinality 34 at order nine, the only gap in the otherwise complete attainable interval $[9, 59]$ of that row, and $13, \ldots, 19$, 21, 48, 50 and 54 at order eleven, among them the three isolated gaps of $[20, 53]$ and the first value of the uncertain interval $[54, 115]$. Every witness has integer coordinates. They are obtained from a classical Latin square by replacing each member of a family of pairwise cell-disjoint subsquares with an orthogonal frame; the content is the packing, not the replacement, and we record the counting ceiling that limits it. We also delimit the method: a search over order-seven Latin squares never packed more than seven pairwise disjoint intercalates, which puts the uncertain block $[24, 27]$ at order seven out of reach of this construction; and for the Fourier matrix at a prime order p the competing Butson mixed-Schur construction has cardinality the size of a sumset of two cosets of one cyclic subgroup, hence only p or p^2. All existence statements below are machine-checked in Lean 4, with no floating point and no square roots entering any certificate.

1. Introduction

Let $n \geq 1$. A *quantum Latin square* of order n, introduced by Musto and Vicary [1] as the datum from which a family of unitary error bases is built, is an $n \times n$ array

$$\Phi = (\varphi_{ij})_{0 \leq i,j < n}, \qquad \varphi_{ij} \in \mathbb{C}^n, \quad \|\varphi_{ij}\| = 1,$$

such that each row $(\varphi_{i0}, \ldots, \varphi_{i,n-1})$ and each column $(\varphi_{0j}, \ldots, \varphi_{n-1,j})$ is an orthonormal basis of $\mathbb{C}^n$. A classical Latin square gives one: read its symbols as the standard basis vectors. Two entries are identified when they differ by a global phase $e^{i\theta}$, equivalently when they span the same complex line, and the *cardinality* $\mathrm{card}(\Phi)$ is the number of classes among the n^2 entries. Classical squares realise the smallest possible cardinality, namely n, and the *cardinality spectrum problem* asks which values

$$\mathrm{Spec}\big(\mathrm{QLS}(n)\big) \;:=\; \{\, \mathrm{card}(\Phi) \;:\; \Phi \text{ a quantum Latin square of order } n \,\}$$

contains. Always $n \leq \mathrm{card}(\Phi) \leq n^2$, both endpoints occur, and $n+1$ never does ([7, Theorem 1.1(1)], attributed there to [4, 5]).

Zhang, Lv and Cao [7] proved that for every $v \geq 8$ with $v \notin \{9, 11, 23\}$ and every $c \in [v, v^2] \setminus \{v+1\}$ there is a quantum Latin square of order v and cardinality c, so the spectrum is completely known outside the five orders $6, 7, 9, 11, 23$. Their concluding table — rendered as Table 6 of [7] — lists, for each of those five orders, the cardinalities they can attain and the cardinalities they cannot decide. Written out, the uncertain entries are

order v	cardinalities recorded as uncertain in [7], Table 6
6	$\{23, 25, 27, 29, 32, 35\}$
7	$[24, 27] \cup [29, 42] \cup \{45\}$
9	$[60, 62] \cup [65, 71] \cup \{34, 73, 74\}$
11	$[13, 19] \cup [54, 115] \cup \{21, 48, 50, 105, 111, 112, 119\}$
23	$\{528\}$

The order-six row was closed within weeks of its publication: Xu [6, 8] constructed squares of cardinalities $13, 15, 17$ and then $19, 21, 23, 25, 27, 32, 35$, and Das and Kumar [9] supplied the last value 29, so that $\mathrm{Spec}(\mathrm{QLS}(6)) = [6, 36] \setminus \{7\}$. The other four rows were untouched.

This paper settles twelve of their entries, all at orders nine and eleven.

- **Order nine, cardinality** 34 (Theorem 5.1). The order-nine row of Table 6 records $[9, 59] \setminus \{10, 34\}$ as attainable, so 34 is its single interior gap ($10 = 9 + 1$ is impossible at every order).
- **Order eleven, cardinalities** 21**,** 48**,** 50 (Theorem 5.2). These are the three interior gaps of the attainable interval $[20, 53]$ of the order-eleven row.
- **Order eleven, cardinality** 54 (Theorem 5.3). This is the first value of the uncertain interval $[54, 115]$ of that row.
- **Order eleven, cardinalities** $13, \ldots, 19$ (Proposition 5.4). The whole block $[13, 19]$ is recorded as uncertain, and we realise all of it. We stress that these seven values are *elementary*: $11 + 2$ is one intercalate and $11 + 3$ is one 3×3 subsquare, which is precisely what the two worked examples [7, Examples 2.14 and 2.15] do at orders six and seven. They are absent from the literature's attainable list only because the order-eleven row of Table 6 is generated by product constructions and 11 does not factor. We record them because the table cell is empty, not because the argument is new.

The construction behind all twelve is one move, applied many times at once. If a classical Latin square L of order n contains a $d \times d$ subsquare — rows R, columns C, symbols S, all of size d, with $L(R \times C) = S$ — then replacing, *inside* $R \times C$ *only*, each symbol $s \in S$ by the s-th member of an orthogonal frame of $\mathrm{span}\{e_s : s \in S\}$ again yields a quantum Latin square, and turns the d^2 cells of the block into exactly d new rays (Lemma 4.1). Applied to t pairwise cell-disjoint subsquares of orders $d_1, \ldots, d_t$, each of whose symbols retains at least one cell outside every block, it produces cardinality $n + \sum_i d_i$. The move itself is not new. What decides which values are reachable is the *packing*: how large $\sum_i d_i$ can be made subject to cell-disjointness and to symbol survival. Cardinality 34 at order nine needs twelve pairwise cell-disjoint subsquares of a single square of order nine, and cardinality 54 at order eleven needs twenty-one; both configurations are exhibited in §5.

We are equally explicit about where the method stops, since a negative measurement is worth recording once it has been made (§6). At order seven the cell budget would permit $\sum_i d_i \leq 20$ and hence cardinality up to 27, the top of the uncertain block $[24, 27]$; a search over annealed Latin squares of order seven, including squares with the maximum possible 42 intercalates, never found more than *seven* pairwise disjoint ones, so this method reaches only cardinality 21, which is already attainable. At orders nine and eleven the high uncertain cells would need blocks of order four or five filled with a quantum Latin square of large cardinality rather than with a frame; a census of two hundred random Latin squares of each of those orders contained no such subsquare at all, and a single order-four block caps order nine at cardinality 53, below the uncertain interval $[60, 62]$. Finally the other classical source of witnesses — mixed Schur products of two Butson matrices, which is how the order-six values $19, 21, 27, 32, 35$ arise [8] — is structurally silent at prime orders: its cardinality is the size of a sumset $S + T$ in $(\mathbb{Z}/m)^n$ modulo constants, and for the Fourier matrix at a prime order p both S and T are cosets of one cyclic subgroup, so the sumset has size p or p^2.

Everything is certified exactly. The two facts that make this possible are that the quantum Latin square property and the cardinality are both invariant under rescaling each entry by a nonzero scalar, and that "two vectors span the same line" is the vanishing of all 2×2 minors. A witness may therefore be presented projectively — nonzero vectors with pairwise orthogonal rows and columns, no normalisation — and then every condition it must satisfy is a polynomial identity over $\mathbb{Z}$. All twelve witnesses here have integer coordinates; the normalising factors $\|v\|^{-1}$ are supplied once, abstractly, inside a single bridge lemma (§3). The statements are machine-checked in Lean 4 (§8).

Remark 1.1. The order-eleven row of Table 6 in [7] is internally inconsistent as printed: the values 105, 111, 112 appear in *both* the attainable and the uncertain entry, and they moreover lie inside the interval $[54, 115]$ that the same uncertain entry lists. We read the table from the LaTeX source of [7], so this is not an artefact of an HTML rendering: it is the sixth and last table of that source, printed as Table 6 although its internal label reads `tab:5`, and it stands unchanged in v2, which is the current version. Nothing in this paper depends on those three values, and the entries we do use — the interior gaps $21, 48, 50$ of [20, 53], the block [13, 19], the interval [54, 115], and the order-nine row — are unaffected.

2. Quantum Latin squares, rays and cardinality

Throughout, $n \geq 1$ and indices run over $\{0, 1, \ldots, n-1\}$; $e_0, \ldots, e_{n-1}$ is the standard basis of $\mathbb{C}^n$ and $\langle u, v\rangle = \sum_r \overline{u_r} v_r$.

Definition 2.1. An array $\Phi = (\varphi_{ij})$ of vectors of $\mathbb{C}^n$ is a *quantum Latin square of order n* if

$$\langle \varphi_{ij}, \varphi_{ij'}\rangle = \delta_{jj'} \quad \text{and} \quad \langle \varphi_{ij}, \varphi_{i'j}\rangle = \delta_{ii'} \qquad \text{for all } i, i', j, j'.$$

Taking $j = j'$ gives $\|\varphi_{ij}\| = 1$, so an orthonormal family of n vectors in the n-dimensional space $\mathbb{C}^n$ is what each row and column is, and that is an orthonormal basis. The next statement is the check that Definition 2.1 is the definition of [1] and not a weakening of it.

Proposition 2.2. *Let Φ be a quantum Latin square of order $n \geq 1$. Then for each i the family $(\varphi_{ij})_j$ is an orthonormal basis of $\mathbb{C}^n$, and for each j the family $(\varphi_{ij})_i$ is orthonormal.*

Definition 2.3. For $u, v \in \mathbb{C}^n$ write $u \sim v$ when $v = cu$ for some $c \in \mathbb{C}^\times$, i.e. when u and v span the same complex line, or *ray*. The *cardinality* of Φ is

$$\operatorname{card}(\Phi) \ := \ \big|\{\, (i,j) \,\}/{\sim}\big|,$$

the number of rays among the n^2 entries.

Proposition 2.4. *For unit vectors $u, v \in \mathbb{C}^n$ one has $u \sim v$ if and only if $v = e^{i\theta}u$ for some $\theta \in \mathbb{R}$. Consequently* $\operatorname{card}(\Phi)$ *is the number of entries of Φ modulo global phase, which is the invariant of* [1, 7, 8, 9].

The cardinality is never computed here by choosing representatives. It is the number of classes of an explicit equivalence relation, and the only route to a value is the following counting lemma, which is what every certificate below instantiates.

Lemma 2.5. *Let Φ be an array of vectors of $\mathbb{C}^n$, let $k \geq 0$ and let $\lambda : \{0, \ldots, n-1\}^2 \to \{0, \ldots, k-1\}$ be surjective and satisfy*

$$\varphi_{ij} \sim \varphi_{i'j'} \iff \lambda(i,j) = \lambda(i',j') \qquad \textit{for all } i, j, i', j'.$$

Then $\operatorname{card}(\Phi) = k$.

Proposition 2.6. *Let Φ be a quantum Latin square of order $n \geq 1$. Two distinct cells of the same row never span the same ray, and consequently*

$$n \ \leq \ \operatorname{card}(\Phi) \ \leq \ n^2.$$

Moreover for every $n \geq 1$ the cyclic Latin square $L(i,j) = i + j \bmod n$, read as $\varphi_{ij} = e_{i+j}$, is a quantum Latin square with $\operatorname{card}(\Phi) = n$ *exactly.*

Proof sketch. If $\varphi_{ij} = c\,\varphi_{ij'}$ with $j \neq j'$ then $0 = \langle \varphi_{ij}, \varphi_{ij'}\rangle = \bar{c}\,\|\varphi_{ij'}\|^2 = \bar{c}$, contradicting $c \neq 0$. Hence the n cells of a single row already give n distinct classes; the upper bound is that there are n^2 cells. For the cyclic square, two cells carry the same ray exactly when they carry the same symbol. No enumeration is involved, and the statement holds for every n. □

Proposition 2.6 settles a convention: the degenerate cardinality is n, not n^2, and a claimed witness of cardinality below its order is refuted outright.

3. Exact certificates

Both defining conditions of Definition 2.1 and the ray relation are invariant under rescaling each entry by a nonzero scalar. This is what allows a witness to be presented *projectively*, with no unit-norm condition anywhere. For vectors u, v over a commutative ring write

$$P(u,v) \ :\iff \ u_r v_s = u_s v_r \quad \text{for all } r, s,$$

the division-free test for spanning the same line.

Theorem 3.1 (Exact bridge)**.** *Let $n, k \geq 1$ and let $v_{ij} \in \mathbb{R}^n$ be nonzero vectors with*

$$\sum_r v_{ij}(r)\, v_{ij'}(r) = 0 \quad (j \neq j'), \qquad \sum_r v_{ij}(r)\, v_{i'j}(r) = 0 \quad (i \neq i').$$

Suppose $\lambda : \{0,\dots,n-1\}^2 \to \{0,\dots,k-1\}$ is surjective and satisfies $P(v_{ij}, v_{i'j'}) \iff \lambda(i,j) = \lambda(i',j')$. Then there is a quantum Latin square Φ of order n with $\operatorname{card}(\Phi) = k$*. The same holds with $\mathbb{R}$ replaced by $\mathbb{C}$ and the bilinear form by the hermitian one, and with $\mathbb{R}^n$ replaced by $(\mathbb{Z}[\sqrt{d}])^n$ for any $d \geq 0$ that is not a perfect square.*

Proof sketch. Put $\Phi_{ij} = \|v_{ij}\|^{-1} v_{ij}$. Orthogonality is preserved and the diagonal entries become 1; ray equality is unchanged by the rescaling, so Lemma 2.5 applies to λ. Over $\mathbb{Z}[\sqrt{d}]$ one transports along the injective ring homomorphism $\mathbb{Z}[\sqrt{d}] \to \mathbb{R}$, injectivity being exactly the hypothesis that d is not a square. ☐

The only square root of the whole development occurs inside this proof, through the identity $(\sqrt{x})^{-1}(\sqrt{x})^{-1}x = 1$, valid for $x > 0$. No witness mentions a norm, and no numerical approximation occurs anywhere.

For the order-six witnesses of §7 the array is written out cell by cell and the ray test is then decided for all n^4 pairs of cells, i.e. n^6 minor comparisons. That is affordable at $n = 6$ and is 1.77×10^6 at $n = 11$. The witnesses of §5 therefore use a more economical shape in which the labelling is the ray relation by construction.

Theorem 3.2 (Integer palette certificate)**.** *Let $n, k \geq 1$, let $p_0, \dots, p_{k-1} \in \mathbb{Z}^n$ be nonzero (the* palette*) and let $\lambda : \{0,\dots,n-1\}^2 \to \{0,\dots,k-1\}$ be surjective (the* labelling*). Put $v_{ij} := p_{\lambda(i,j)}$. If*

(i) *$\sum_r v_{ij}(r) v_{ij'}(r) = 0$ for $j \neq j'$ and $\sum_r v_{ij}(r) v_{i'j}(r) = 0$ for $i \neq i'$, and*
(ii) *$P(p_a, p_b) \iff a = b$ for all $a, b < k$,*

then there is a quantum Latin square of order n with cardinality exactly k.

Condition (ii) is k^2 ray tests instead of n^4, and it is what makes the labelling tautologically the ray relation: two cells carry the same ray precisely when they name the same palette vector. Condition (i) is $2n^2(n-1)$ inner products of length n. Both are exact integer computations.

4. Block replacement and packing

We now describe the construction that produced the witnesses. Let L be a classical Latin square of order n on the symbols $\{0,\dots,n-1\}$, read as the quantum Latin square $\varphi_{ij} = e_{L(i,j)}$ of cardinality n. A $d \times d$ *subsquare* of L is a triple (R, C, S) of d-element sets of rows, columns and symbols with $L(R \times C) = S$; a 2×2 subsquare is an *intercalate.*

Lemma 4.1 (Block replacement)**.** *Let $(R_1, C_1, S_1), \dots, (R_t, C_t, S_t)$ be subsquares of L of orders $d_1, \dots, d_t$ whose cell sets $R_i \times C_i$ are pairwise disjoint. For each i choose an orthogonal basis $(w_s^{(i)})_{s \in S_i}$ of the space* $\operatorname{span}\{e_s : s \in S_i\}$*, consisting of nonzero vectors, and define*

$$v_{ab} \ := \ \begin{cases} w^{(i)}_{L(a,b)}, & (a,b) \in R_i \times C_i \text{ for some } i, \\ e_{L(a,b)}, & \text{otherwise.} \end{cases}$$

Then the rows and the columns of (v_{ab}) are pairwise orthogonal, so after normalisation (v_{ab}) is a quantum Latin square of order n; and

$$\mathrm{card} \;=\; \#\{\textit{symbols occurring outside every block}\} \;+\; \sum_{i=1}^{t} d_i \;=\; n + \sum_{i=1}^{t} d_i$$

as soon as every symbol keeps at least one cell outside every block, and the vectors $w_s^{(i)}$ are chosen pairwise non-proportional across different blocks.

Proof. Fix a row a. If $a \in R_i$ then the cells of that row inside C_i carry the d_i pairwise orthogonal vectors $w_s^{(i)}$, $s \in S_i$; every other cell of the row carries some e_u with $u \notin S_i$, because L restricted to $R_i \times C_i$ already uses all of S_i in row a and L is a Latin square, and such e_u is orthogonal to every $w_s^{(i)}$ since the latter lies in $\mathrm{span}\{e_s : s \in S_i\}$. Blocks meeting the row in disjoint column sets contribute vectors supported on disjoint symbol sets, again orthogonal. Rows disjoint from every R_i are untouched. Columns are the transposed argument, using that outside R_i the columns of C_i never carry a symbol of S_i. For the count: the d_i^2 cells of the i-th block carry exactly the d_i rays of $w_s^{(i)}$, and a symbol s retains its own ray $[e_s]$ exactly when one of its n cells lies outside all blocks. □

Lemma 4.1 is not a new idea: the two worked examples [7, Examples 2.14 and 2.15] are the cases $t = 1$, $d \in \{2, 3\}$ at orders six and seven, giving cardinalities $8, 9$ and $9, 10$. What is not automatic is how large $\sum_i d_i$ can be made. The following ceiling is what a search has to work against.

Proposition 4.2. *With the notation of Lemma 4.1, if every symbol keeps a cell outside every block then*

$$\sum_{i=1}^{t} d_i^2 \;\le\; n(n-1).$$

Consequently $\sum_i d_i \le \frac{1}{2}n(n-1)$, with the sharper bounds: if all blocks are intercalates then $t \le \lfloor n\lfloor n/2\rfloor/2\rfloor$, and if some block has order $d \ge 3$ then $\sum_i d_i \le \frac{1}{2}n(n-1) - \frac{3}{2}$. At $n = 7, 9, 11$ this caps $\sum_i d_i$ at 20, 36 and 54 respectively, i.e. the construction of Lemma 4.1 cannot pass cardinality 27, 45 and 65 at those orders.

Proof. The i-th block absorbs exactly d_i of the n cells of each of its d_i symbols, and the blocks are cell-disjoint, so a symbol s loses $\sum_{i:\, s \in S_i} d_i \le n-1$ of its cells. Summing over the n symbols gives $\sum_i d_i^2 \le n(n-1)$. Since $d_i \ge 2$ we have $\sum_i d_i = \sum_i d_i^2/d_i \le \frac{1}{2}\sum_i d_i^2$, and a single block of order $d \ge 3$ costs $\frac{1}{2}(d^2 - 2d) \ge \frac{3}{2}$ of that. An intercalate occupies two cells of each of its two rows, so a row of n cells meets at most $\lfloor n/2\rfloor$ of them, and counting row incidences gives $2t \le n\lfloor n/2\rfloor$. At $n = 11$, for instance, an all-intercalate packing has $t \le 27$ and $\sum_i d_i \le 54$, while a packing using a block of order at least three has $\sum_i d_i \le \lfloor 55 - \frac{3}{2}\rfloor = 53$; the maximum is therefore 54. The cases $n = 7$ and $n = 9$ are identical, with 20 against 19 and 36 against 34. □

Lemma 4.1 and Proposition 4.2 are stated and proved here at the level of ordinary mathematics; they are the design principle behind the witnesses and are not part of the formal development, which verifies each finished witness directly and does not go through them (§8).

How the packings were found. Latin squares were generated by simulated annealing, starting from the Jacobson–Matthews random Latin square procedure [11] and moving by row cycles, with objective the size of the largest cell-disjoint block packing; for each square produced, that packing was then solved exactly by branch and bound under the symbol-survival constraint of Proposition 4.2. At order nine the best value found was $\sum_i d_i = 28$; at order eleven, 43, hit twice in about 150 annealed squares and never beaten. The two packings displayed in §5 come from this search.

5. Twelve cardinalities at orders nine and eleven

5.1. Order nine. The Latin square is

$$L_9 = \begin{matrix} 3 & 2 & 0 & 4 & 7 & 1 & 5 & 8 & 6 \\ 1 & 3 & 2 & 6 & 8 & 4 & 7 & 5 & 0 \\ 8 & 0 & 3 & 7 & 1 & 5 & 6 & 4 & 2 \\ 0 & 6 & 4 & 3 & 5 & 2 & 8 & 7 & 1 \\ 6 & 8 & 5 & 1 & 4 & 7 & 0 & 2 & 3 \\ 4 & 1 & 7 & 8 & 6 & 3 & 2 & 0 & 5 \\ 7 & 5 & 8 & 0 & 2 & 6 & 1 & 3 & 4 \\ 2 & 7 & 1 & 5 & 3 & 0 & 4 & 6 & 8 \\ 5 & 4 & 6 & 2 & 0 & 8 & 3 & 1 & 7 \end{matrix}$$

and it carries twelve pairwise cell-disjoint subsquares, one of order three and eleven intercalates, with $\sum_i d_i = 3 + 22 = 25$:

rows	columns	symbols	rows	columns	symbols
$0,1,3$	$4,6,7$	$5,7,8$	$1,3$	$2,5$	$2,4$
$0,4$	$0,8$	$3,6$	$2,7$	$0,8$	$2,8$
$0,7$	$2,5$	$0,1$	$2,7$	$6,7$	$4,6$
$0,8$	$1,3$	$2,4$	$4,5$	$1,3$	$1,8$
$1,3$	$0,8$	$0,1$	$4,5$	$6,7$	$0,2$
$1,3$	$1,3$	$3,6$	$6,8$	$6,7$	$1,3$

Each intercalate on symbols $\{s, s'\}$ is filled with the orthogonal pair $a\,e_s + b\,e_{s'}$, $-b\,e_s + a\,e_{s'}$ for a small integer pair (a, b) varied from block to block; the 3×3 block is filled with $(1, 2, 2)$, $(2, 1, -2)$, $(2, -2, 1)$ in its symbol coordinates. That the resulting 34 vectors are pairwise non-proportional is part of what the certificate checks. Every symbol keeps a cell outside every block, so Lemma 4.1 predicts cardinality $9 + 25 = 34$, and the certificate confirms it.

Theorem 5.1. *There is a quantum Latin square of order nine with cardinality* 34*. Equivalently,* $34 \in \mathrm{Spec}(\mathrm{QLS}(9))$*, a value recorded as uncertain in* [7, Table 6] *and the only gap in the attainable interval* $[9, 59]$ *of that row.*

Proof sketch. The witness is the palette of 34 integer vectors of $\mathbb{Z}^9$ described above — the nine standard basis vectors together with the 25 vectors introduced by the twelve blocks — together with the labelling that assigns to each of the 81 cells the palette index of its entry. Theorem 3.2 then applies, and its three hypotheses are verified by exhaustive exact computation: $9 \cdot 9 \cdot 8 = 648$ row inner products and 648 column inner products of length nine, all of which vanish; and $34^2 = 1156$ pairwise ray tests among palette vectors, each a conjunction of 81 integer identities $p_a(r)p_b(s) = p_a(s)p_b(r)$, which hold exactly on the diagonal. Surjectivity of the labelling and nonvanishing of the palette vectors are two further finite checks. Nothing else is used: the theorem does not go through Lemma 4.1, which served only to find the array. $\square$

5.2. **Order eleven.** All eleven order-eleven witnesses come from one Latin square and one packing; they differ only in how many blocks are switched on. The square is

$$L_{11} = \begin{array}{ccccccccccc} 10 & 9 & 8 & 2 & 7 & 1 & 5 & 4 & 6 & 3 & 0 \\ 8 & 0 & 10 & 7 & 2 & 4 & 3 & 6 & 9 & 1 & 5 \\ 9 & 2 & 0 & 5 & 3 & 6 & 10 & 8 & 1 & 4 & 7 \\ 3 & 7 & 1 & 4 & 9 & 8 & 2 & 5 & 0 & 10 & 6 \\ 0 & 8 & 9 & 10 & 6 & 3 & 4 & 2 & 7 & 5 & 1 \\ 6 & 5 & 4 & 1 & 0 & 10 & 9 & 7 & 2 & 8 & 3 \\ 4 & 6 & 5 & 0 & 1 & 7 & 8 & 10 & 3 & 9 & 2 \\ 7 & 3 & 2 & 8 & 10 & 5 & 0 & 1 & 4 & 6 & 9 \\ 2 & 10 & 3 & 6 & 8 & 9 & 1 & 0 & 5 & 7 & 4 \\ 1 & 4 & 6 & 3 & 5 & 0 & 7 & 9 & 8 & 2 & 10 \\ 5 & 1 & 7 & 9 & 4 & 2 & 6 & 3 & 10 & 0 & 8 \end{array}$$

and the packing consists of twenty-one pairwise cell-disjoint subsquares, one of order three and twenty intercalates, with $\sum_i d_i = 3 + 40 = 43$:

rows	columns	symbols	rows	columns	symbols
$1, 4, 10$	$2, 3, 8$	$7, 9, 10$	$2, 9$	$3, 4$	$3, 5$
$0, 2$	$5, 8$	$1, 6$	$3, 5$	$2, 3$	$1, 4$
$0, 3$	$0, 9$	$3, 10$	$3, 9$	$5, 8$	$0, 8$
$0, 3$	$1, 4$	$7, 9$	$4, 10$	$0, 9$	$0, 5$
$0, 6$	$2, 6$	$5, 8$	$4, 10$	$1, 10$	$1, 8$
$0, 6$	$3, 10$	$0, 2$	$4, 10$	$4, 6$	$4, 6$
$1, 3$	$7, 10$	$5, 6$	$4, 10$	$5, 7$	$2, 3$
$1, 7$	$1, 6$	$0, 3$	$5, 9$	$6, 7$	$7, 9$
$1, 8$	$0, 4$	$2, 8$	$6, 7$	$4, 7$	$1, 10$
$2, 6$	$0, 9$	$4, 9$	$7, 9$	$2, 9$	$2, 6$
			$8, 9$	$1, 10$	$4, 10$

Theorem 5.2. *There are quantum Latin squares of order eleven with cardinalities* 21, 48 *and* 50*. These are the three interior gaps of the attainable interval* $[20, 53]$ *of the order-eleven row of* [7, Table 6]*, where all three are recorded as uncertain.*

Theorem 5.3. *There is a quantum Latin square of order eleven with cardinality* 54*, the first value of the uncertain interval* $[54, 115]$ *of the order-eleven row of* [7, Table 6].

Proposition 5.4. *For every* c *with* $13 \le c \le 19$ *there is a quantum Latin square of order eleven with cardinality* c*. The whole block* $[13, 19]$ *is recorded as uncertain in* [7, Table 6].

Remark 5.5. Proposition 5.4 is elementary and we claim no novelty for its argument. Switching on a single intercalate gives $11 + 2 = 13$ and switching on the single 3×3 block gives $11 + 3 = 14$; the remaining five values use between two and four blocks. This is exactly the worked example [7, Examples 2.14 and 2.15], read at order eleven instead of at orders six and seven. The values are missing from the attainable entry of Table 6 because that row is produced by the product constructions of [7, §3–§4], which require v to factor.

Proof sketch for Theorems 5.2, 5.3 and Proposition 5.4. Each of the eleven witnesses is a sub-packing of the packing displayed above: cardinality $11 + \sum_i d_i$ with $\sum_i d_i = 2, 3, 4, 5, 6, 7, 8$ for $c = 13, \ldots, 19$; $\sum_i d_i = 10$ (five intercalates) for $c = 21$; 37 (the 3×3 block and seventeen intercalates) for $c = 48$; 39 (the 3×3 block and eighteen intercalates) for $c = 50$; and the whole packing, $\sum_i d_i = 43$, for $c = 54$. Each witness is then presented as an integer palette of c vectors of $\mathbb{Z}^{11}$ with its labelling of the 121 cells, and Theorem 3.2 is applied. As in Theorem 5.1 the hypotheses are exhaustive finite checks: $11 \cdot 11 \cdot 10 = 1210$ row inner products and 1210 column inner products of length eleven per witness, and c^2 pairwise ray tests among palette vectors, each a conjunction of 121 integer identities — so $54^2 = 2916$ ray tests for the largest witness. No hypothesis of Lemma 4.1 is invoked in the verification. $\square$

Theorem 5.6. *Every one of the twelve cardinalities*

$$34 \textit{ at order nine}, \qquad 13, 14, 15, 16, 17, 18, 19,\ 21,\ 48,\ 50,\ 54 \textit{ at order eleven}$$

is realised by a quantum Latin square, and every one of them is recorded as uncertain in [7, Table 6]*. Seven of the twelve, the block* $[13, 19]$*, are elementary (Proposition 5.4); the other five require the packing.*

5.3. **Negative controls.** A certificate that a labelling has k classes is only as good as the guarantee that the labelling is neither too coarse nor too fine, and an orthogonality test is only meaningful if it can fail. Both are checked.

Proposition 5.7. *For the order-nine witness of cardinality* 34 *and the order-eleven witness of cardinality* 54*:*

- (i) *merging two of the ray classes, which produces a labelling with one class fewer, yields a relation that is refuted as the ray relation;*
- (ii) *splitting one ray class according to the row index, which produces a labelling with one class more, is likewise refuted;*
- (iii) *increasing a single coordinate of a single palette vector by* 1 *makes the row orthogonality test fail, while the unmodified palette passes it.*

Together with Proposition 2.6, which gives $9 \le 34 \le 81$ *and* $11 \le 54 \le 121$ *for structural reasons, the values are pinned from both sides and the tests are not vacuous.*

Items (i)–(iii) are again exhaustive computations over the same finite data: (i) and (ii) each inspect all n^4 ordered pairs of cells and exhibit a pair on which the modified labelling and the ray relation disagree; (iii) inspects the $2n^2(n-1)$ inner products.

6. What the method does not reach

The remaining uncertain entries of Table 6 are not accessible to this construction, and the reasons are worth recording, since each of them was measured rather than guessed. The statements in this section are computational observations and counting arguments, not machine-checked theorems, and we mark them as such.

6.1. **Order seven.** The uncertain block at order seven begins at 24, and Proposition 4.2 caps $\sum_i d_i$ at 20 there, i.e. cardinality at 27 — exactly the top of $[24, 27]$. The construction nevertheless does not get there. Every annealed Latin square of order seven that we examined — more than two hundred, including squares attaining 42 intercalates — packs at most *seven* pairwise cell-disjoint intercalates. That gives $\sum_i d_i \le 14$ and cardinality at most 21, which is inside the attainable interval $[7, 23] \setminus \{8\}$ of that row and therefore of no help. The uncertain block at order seven needs a different construction.

Here 42 is the largest number of intercalates an order-seven Latin square can have, so the squares just described are the most favourable input the method admits. The upper bound is a count: the intercalates lying in a fixed pair of rows are the transpositions of the derangement carrying one row to the other, a derangement of seven points has at most two transpositions (three would consume six points and leave the seventh fixed), and there are $\binom{7}{2} = 21$ pairs of rows. Attainment is what our search records, and 42 is also the order-seven term of the tabulated maxima $0, 1, 0, 12, 4, 27, 42, 112, 72$ for orders $1, \ldots, 9$ [12].

6.2. **The high cells at orders nine and eleven.** Reaching $[60, 62] \cup [65, 71] \cup \{73, 74\}$ at order nine or $[55, 115]$ at order eleven would require the natural strengthening of Lemma 4.1 in which a $d \times d$ block is filled not with an orthogonal frame but with an arbitrary quantum Latin square of order d written in the basis $\{e_s : s \in S\}$, so that the block contributes up to d^2 rays instead of d. For that one needs subsquares of order four or five. Two obstructions were found. First, a census of two hundred random Latin squares of each of the orders nine and eleven contained *no* subsquare of order four at all, and none of order five at order eleven (order five requires $n \ge 10$). Second, even granting such blocks the arithmetic is tight: filling a single order-four block with a quantum Latin square of cardinality 16 and spending the remaining cell budget of Proposition 4.2 on intercalates gives at order nine

$$\operatorname{card} \;\le\; 9+16+2\cdot\left\lfloor \tfrac{72-16}{4}\right\rfloor \;=\; 9+16+28 \;=\; 53,$$

below the uncertain interval $[60,62]$, so at least two order-four blocks would be needed. A count also rules out two order-k subsquares that share neither a row nor a column at $(n,k)=(9,4)$ and $(11,5)$: their symbol sets must then be disjoint in the untouched columns, so $|S_A \cup S_B| = 2k = n-1$, and the single leftover row is forced to carry the same leftover symbol in all k of those columns. The cases where the two subsquares share rows or columns are limited by the same count to at most one shared column, respectively one shared row; that is not a contradiction, so it is a search not yet run rather than a theorem.

6.3. **Order eleven stops at $\sum_i d_i = 43$.** The packing displayed in §5 has $\sum_i d_i = 43$ against the ceiling 54 of Proposition 4.2, and 43 was the best value found over roughly 150 annealed Latin squares of order eleven, attained twice. Every additional unit of $\sum_i d_i$ would settle one more uncertain cell of the interval $[54,115]$, which makes "improve the packing" a well-posed and cheap follow-up question rather than a vague one.

6.4. **Butson matrices are silent at prime orders.** The other construction available for sporadic cardinalities is the mixed Schur product: given two $n\times n$ Butson matrices $H=\zeta_m^A$ and $K=\zeta_m^B$ with entries m-th roots of unity and pairwise orthogonal columns, the array $\Phi_{ij} = n^{-1/2}(h_i \odot k_j)$ formed from the columns h_i of H and k_j of K is a quantum Latin square. This is how the order-six cardinalities $19, 21, 27, 32, 35$ arise [8], and it is available at every order.

Theorem 6.1. *Let $m,n\ge 1$, let A,B be $n\times n$ matrices over $\mathbb{Z}/m$ and put $\Phi_{ij}(r) = \zeta_m^{A_{ri}+B_{rj}}$. Then the inner product of two entries in one row of Φ equals that of the corresponding two columns of ζ_m^B, the inner product of two entries in one column equals that of the corresponding two columns of ζ_m^A, and $\Phi_{ij}\sim\Phi_{i'j'}$ if and only if $A_{ri}+B_{rj}+A_{si'}+B_{sj'} = A_{si}+B_{sj}+A_{ri'}+B_{rj'}$ for all r,s. Hence if the columns of ζ_m^A and those of ζ_m^B are pairwise orthogonal, and λ is a surjective labelling onto $\{0,\dots,k-1\}$ agreeing with that criterion, then after normalisation Φ is a quantum Latin square of order n with cardinality k. In particular there is a quantum Latin square of order four with cardinality* 16, *obtained from two* BH$(4,4)$ *matrices.*

Cardinality 16 at order four is a known value — $\operatorname{Spec}(\mathrm{QLS}(4)) = \{4,6,8,16\}$ is quoted in [7, §1] and attributed there to Paczos, Wierzbiński, Rajchel-Mieldzioć, Burchardt and Życzkowski [2] and to Zhang and Cao [3] — and is recorded here only because it exercises Theorem 6.1 at an order other than six.

Remark 6.2 (The sumset obstruction). Dephasing sends the ray class of the cell (i,j) of $\Phi(H,K)$ to $[A_{\cdot i}]+[B_{\cdot j}]$ in $V=(\mathbb{Z}/m)^n/\text{constants}$, so that

$$\operatorname{card}\Phi(H,K) \;=\; |S+T|, \qquad S=\{[A_{\cdot i}]\},\ T=\{[B_{\cdot j}]\},$$

the size of a sumset of two n-element subsets of an abelian group. For the Fourier matrix F_p at a prime order p the column classes form a coset of a cyclic subgroup of order p, and a sumset of two cosets is a coset of the subgroup they generate; hence $|S+T|\in\{p,p^2\}$, and both values are attainable for trivial reasons. This is confirmed by exhaustive enumeration at $p=5$ and $p=7$. There are 144 dephased BH$(5,5)$ and 86 400 dephased BH$(7,7)$ exponent matrices; among them the column-class set S takes only 6 respectively 120 distinct values, each one a subgroup of order p, and over *all* ordered pairs of those values $|S+T|$ is 5 or 25 respectively 7 or 49, both occurring. This covers every ordered pair of BH$(5,5)$, respectively BH$(7,7)$, matrices, dephased or not: rescaling the rows and columns of a Butson matrix by phases translates its column-class set by a fixed class of V, which leaves $|S+T|$ unchanged. What this does *not* settle is whether BH(p,m) exists for other moduli m; nothing here forbids, say, a BH$(7,6)$. The composite orders are where the construction has room, which is why the order-six witnesses of [8] exist while no order-seven analogue is known.

7. Order six, independently re-derived

For completeness we record that the whole of the recent order-six literature was re-derived exactly by the same machinery before the present work, since it is what calibrates the certificates. Nothing in this section is new.

Proposition 7.1. *The arrays printed in* [6] *(Sections 2–4), in* [8] *(equation (11) at the parameter values* $(1/\sqrt{2}, 1/\sqrt{2})$ *and* $(4/5, 3/5)$*) and in* [9] *(equation (1) with the diagonal extension of its Proposition 2.3) are, after clearing denominators inside* $\mathbb{Z}[\sqrt{2}]$ *respectively* $\mathbb{Z}[\sqrt{481}]$*, quantum Latin squares of order six of cardinalities* $13, 15, 17$*;* $23, 25$*; and* 29*.*

The quadratic field is forced in the last case: the normalising factors of [9] are not themselves in $\mathbb{Q}(\sqrt{481})$, which is precisely why the projective presentation of Theorem 3.1 is needed rather than the paper's normalised one. The largest integer coefficient occurring after clearing denominators is 162 260 322 588.

Lemma 7.2 (Shift criterion)**.** *Let* $m \geq 1$*,* $\zeta_m = e^{2\pi i/m}$*, and let* $c : \mathbb{Z}/m \to \mathbb{Z}$ *satisfy* $c(a+t) = c(a)$ *for all* a *and some* $t \neq 0$*. Then* $\sum_a c(a)\zeta_m^a = 0$*. Consequently two columns of a Butson matrix are orthogonal as soon as the multiplicity vector of their exponent differences is invariant under a nonzero shift.*

Proof. Multiplying $S = \sum_a c(a)\zeta_m^a$ by ζ_m^t reindexes the sum to itself, so $(\zeta_m^t - 1)S = 0$, and $\zeta_m^t \neq 1$ because $t \neq 0$ in $\mathbb{Z}/m$. □

The criterion verifies and cannot refute — it is strictly weaker than the Lam–Leung theorem on vanishing sums of roots of unity [10] — but it suffices for every column pair of all five of Xu's Butson matrices, with $t = 4$ at $m = 8$, $t = 6$ at $m = 12$, $t = 1$ at $m = 3$ and $t \in \{2, 3\}$ at $m = 6$.

Proposition 7.3. *The exponent matrices printed in* [8] *(equations (2), (7), (19), (23), (27) and (29)) define complex Hadamard matrices, and the corresponding mixed Schur products are quantum Latin squares of order six of cardinalities* 19*,* 21*,* 27*,* 32 *and* 35*.*

Theorem 7.4. *Each of the twelve values* $\{6, 13, 15, 17, 19, 21, 23, 25, 27, 29, 32, 35\}$ *lies in* $\mathrm{Spec}(\mathrm{QLS}(6))$*, by an exact witness.*

This is a strict subset of the published spectrum $[6, 36] \setminus \{7\}$: the remaining attainable values come from earlier constructions, collected without individual attribution in the order-six row of [7, Table 6], that we did not transcribe; and the impossibility of 7 is not a finite witness but the general theorem that no quantum Latin square of order u has cardinality $u + 1$, recorded as [7, Theorem 1.1(1)] and attributed there to Zhang, Wang and Ji [4] and to Zhang and Ji [5].

Proposition 7.5. *For the cardinality-*29 *witness of* [9]*: merging two ray classes (giving* 28 *labels) and splitting one by row (giving* 30*) are both refuted as the ray relation; bumping one coordinate of one entry by* 1 *makes a row orthogonality test fail while the unmodified array passes it; the six diagonal cells share a single ray, the two off-diagonal coincidences* $(0,1) \sim (2,3)$ *and* $(1,4) \sim (5,2)$ *hold, and the cells* $(0,1)$ *and* $(0,2)$ *are confirmed to lie on different rays, so the relation is not the total one.*

Remark 7.6. Every printed matrix, phase-class table, signature table and numerical constant of [6, 8, 9] that bears on order six was recomputed in exact arithmetic before being transcribed, and all of them agreed, including the twenty-eight projective signatures of the table in [9] and the row-permutation tally of [8]. The only discrepancy found in any of the four sources is the printed inconsistency of Remark 1.1, which lies in a row that does not touch order six.

8. Verification

Every existence statement in this paper has been formally verified in Lean 4 against *Mathlib*; the development contains no `sorry`, and each theorem depends on no axioms beyond `propext`, `Classical.choice` and `Quot.sound` — in particular nothing is delegated to compiled evaluation, and every finite search quoted above is re-run inside the kernel. Definition 2.1 is checked to be the definition of [1] rather than a weakening of it by deriving from it Mathlib's `Orthonormal` predicate and a `Module.Basis` (Proposition 2.2), and the cardinality is the number of classes of an explicit quotient, reached only through Lemma 2.5 (Proposition 2.4 identifies that quotient with the global-phase quotient of the literature). The exact bridges of §3 are the only place a square root appears; no witness file mentions a norm, and no floating-point arithmetic occurs anywhere. What rests on exhaustive computation is exactly this: the palette hypotheses of Theorems 5.1, 5.2, 5.3, Proposition 5.4 and Theorem 5.6 (per witness of order n and cardinality c: $2n^2(n-1)$ inner products and c^2 ray tests of n^2 minor identities each), the four control computations of Proposition 5.7 and their order-six counterparts in Proposition 7.5, the orthogonality and ray tests behind Propositions 7.1 and 7.3, and the shift certificates behind Lemma 7.2. Proposition 2.6, Lemma 2.5, Theorems 3.1, 3.2 and 6.1 and Lemma 7.2 are proved in general, with no enumeration. Three things in this paper are *not* part of the formal development and are stated as ordinary mathematics: Lemma 4.1 and Proposition 4.2, which explain how the witnesses were found but are not used to verify them; the annealing and branch-and-bound searches of §4, whose output is the displayed data and whose correctness is irrelevant because the output is verified independently; and the measured negative statements of §6 together with the sumset enumeration of Remark 6.2. Repository reference to be added at submission.

References

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

[2] J. Paczos, M. Wierzbiński, G. Rajchel-Mieldzioć, A. Burchardt and K. Życzkowski, *Genuinely quantum solutions of the game Sudoku and their cardinality*, Phys. Rev. A **104** (2021), no. 4, 042423.

[3] Y. Zhang and H. Cao, *Quantum Latin squares with maximal cardinality*, Discrete Math. **349** (2026), no. 3, article 114863.

[4] Y. Zhang, X. Wang and L. Ji, *Quantum Latin squares with all possible cardinalities*, J. Combin. Des. **34** (2026), no. 8, 378–387; arXiv:2507.05642.

[5] Y. Zhang and L. Ji, *Quantum Latin squares of order* $6m$ *with all possible cardinalities*, arXiv:2601.09132v1.

[6] Z. Xu, *Three quantum Latin squares of order 6 with cardinalities 13, 15, and 17*, arXiv:2605.15540v2.

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

[8] Z. Xu, *New cardinalities for quantum Latin squares of order six*, arXiv:2607.11800v3.

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

[10] T. Y. Lam and K. H. Leung, *On vanishing sums of roots of unity*, J. Algebra **224** (2000), no. 1, 91–109.

[11] M. T. Jacobson and P. Matthews, *Generating uniformly distributed random Latin squares*, J. Combin. Des. **4** (1996), no. 6, 405–437.

[12] OEIS Foundation Inc., *Maximum number of intercalates in a Latin square of order* n, entry A092237 of the On-Line Encyclopedia of Integer Sequences, `https://oeis.org/A092237`.

The four 2026 preprints [6, 7, 8, 9] were read from their LaTeX e-prints; the pinned version numbers are the ones current on 2026-08-28, and none of the four carries a journal reference. The equation numbers quoted from [8] and [9] are those of the pinned versions.