COMPLETE MAPPINGS OF NON-CYCLIC ABELIAN GROUPS AND DIAGONAL QUANTUM LATIN SQUARES OF MAXIMUM CARDINALITY: TEN NEW ORDERS, AND THE EXACT REACH OF THE CONSTRUCTION

KOREA SUPERINTELLIGENCE LABS

ABSTRACT. A quantum Latin square of order n is an $n \times n$ array of unit vectors of $\mathbb{C}^n$ each of whose rows and columns is an orthonormal basis; its cardinality is the number of entries up to a global phase, and it has maximum cardinality when that number is n^2. Huang and Li recently proved that a maximum-cardinality *diagonal* quantum Latin square, MCDQLS(n), exists for every $n \geq 6$ outside an explicit list $P_1 \cup P_2$ of 35 orders, and that an idempotent MCQLS(n) exists for every $n \geq 6$ outside the 13-element list P_1. Their engine is a single construction driven by a complete mapping of the cyclic group $\mathbb{Z}_v$ and the Fourier kernel ω^{ts}. We observe that no step of that construction uses cyclicity, and run it over an arbitrary finite abelian group G of order v with the Fourier kernel replaced by a bi-additive nondegenerate pairing $B\colon G \times G \to \mathbb{Z}_L$. The generalisation settles ten (order, property) cells of the two exception lists: an MCDQLS(v) exists for $v = 9, 20, 27, 32, 40, 63$, and an idempotent MCQLS(v) exists for $v = 12, 20, 24, 32$; three of these orders carry two witnesses over two different groups. We then determine the reach of the generalised construction exactly: of the 35 orders of $P_1 \cup P_2$, precisely those six are reachable, and each of the remaining 29 is out of reach over *every* abelian group of that order — twenty-six by two counting obstructions, and the last three, 7, 8 and 11, by exhaustive enumeration. At orders 7 and 11 the enumeration proves something stronger and pairing-free, namely that every strong complete mapping of a group of that order is affine, whence Huang and Li's own condition $(*)$ fails for all of them; at order 8 the statement is for the canonical pairing. Every theorem below is machine-checked in Lean 4; the one step left to standard mathematics is the classification of finite abelian groups, which is what turns finitely many named groups into *every* group of an order.

1. INTRODUCTION

The objects. Fix $n \geq 1$ and write $\mathbb{C}^n$ for the standard Hermitian space. A *quantum Latin square* of order n, QLS(n), is an $n \times n$ array $\Phi = (|\varphi_{i,j}\rangle)_{0 \leq i,j < n}$ of vectors of $\mathbb{C}^n$ such that every row $(|\varphi_{i,0}\rangle, \ldots, |\varphi_{i,n-1}\rangle)$ and every column $(|\varphi_{0,j}\rangle, \ldots, |\varphi_{n-1,j}\rangle)$ is an orthonormal basis of $\mathbb{C}^n$. The notion is due to Musto and Vicary [2], who introduce it in order to build unitary error bases from it; the cardinality invariant recalled next is not theirs. Two entries are identified when they differ by a global phase; the number of classes is the *cardinality* $\mathrm{card}(\Phi)$, and $n \leq \mathrm{card}(\Phi) \leq n^2$. The array has *maximum cardinality* when $\mathrm{card}(\Phi) = n^2$, that is, when its n^2 entries are pairwise non-proportional; we then write MCQLS(n).

A *transversal* of Φ is a set of n cells, no two in a common row and no two in a common column, whose vectors form an orthonormal basis of $\mathbb{C}^n$. An array is *idempotent* when its main diagonal $\{(i,i)\}$ is a transversal, and *diagonal* when both the main diagonal and the anti-diagonal $\{(i, n-1-i)\}$ are. Attaching the maximum-cardinality requirement gives the two objects this paper is about: the idempotent MCQLS(n) and the diagonal MCDQLS(n).

The source, and what it leaves open. Huang and Li [1] prove that no MCDQLS(n) exists for $n \in \{2, 3, 4, 5\}$, and that for every $n \geq 6$ an MCDQLS(n) exists *except possibly* when $n \in P_1 \cup P_2$, where

$$P_1 = \{6, 8, 10, 12, 14, 18, 20, 24, 26, 30, 32, 38, 62\},$$
$$P_2 = \{7, 9, 11, 15, 21, 22, 27, 33, 34, 39, 40, 46, 48, 50, 51, 58, 63, 74, 75, 82, 94, 122\};$$

separately, they prove that an idempotent MCQLS(n) exists for every $n \geq 6$ except possibly $n \in P_1$. So 35 orders are left open on the diagonal side and 13 on the idempotent side: 48 open cells in all, the orders of P_1 counting on both sides.

Their engine is a single construction. Let μ be a *complete mapping* of $\mathbb{Z}_v$, meaning that μ and $t \mapsto t + \mu(t)$ are both permutations, and let $\omega = e^{2\pi i/v}$. Setting

$$|\varphi_{i,j}\rangle \;=\; v^{-1/2}\big(\omega^{\,tj+i\mu(t)}\big)_{t\in\mathbb{Z}_v}, \tag{1}$$

they show that Φ is an idempotent MCQLS(v) as soon as μ satisfies a coprimality condition ($*$) recalled in Section 2, and an MCDQLS(v) if moreover μ is *strong*, i.e. $t \mapsto \mu(t) - t$ is a permutation too. Each step of the proof is one character-sum identity: the rows are orthonormal because $\sum_t \omega^{t(j'-j)} = 0$ for $j \neq j'$, the columns because μ is a permutation, the main diagonal because $\mu + \mathrm{id}$ is, and the anti-diagonal because $\mu - \mathrm{id}$ is. The shape of the exception lists follows. $\mathbb{Z}_v$ has a complete mapping if and only if v is odd — take $\mu = \mathrm{id}$ for v odd, and see Proposition 5.1 below for v even — so P_1 is entirely even; and $\mathbb{Z}_v$ has a strong complete mapping if and only if $\gcd(v, 6) = 1$ ([9, Theorem 15]; for the easy direction take $\mu(t) = 2t$), so P_2 collects the odd multiples of 3, some even leftovers, and 7 and 11.

What is settled here. Nothing in that argument uses cyclicity. Section 3 runs it over an arbitrary finite abelian group G with $|G| = v$, replacing the Fourier kernel ω^{ts} by $\zeta_L^{B(t,s)}$ for a bi-additive nondegenerate pairing $B\colon G \times G \to \mathbb{Z}_L$ and $\zeta_L = e^{2\pi i/L}$. The substitution is routine once stated; what is not routine is that it walks straight into the exception lists, because for several $v \in P_1 \cup P_2$ there are *non-cyclic* abelian groups of order v carrying complete or strong complete mappings where $\mathbb{Z}_v$ carries none.

object	order	group(s)	list
MCDQLS	9	$\mathbb{Z}_3^2$	P_2
	20	$\mathbb{Z}_2^2 \times \mathbb{Z}_5$	P_1
	27	$\mathbb{Z}_3^3$ *and* $\mathbb{Z}_9 \times \mathbb{Z}_3$	P_2
	32	$\mathbb{Z}_2^5$	P_1
	40	$\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_5$ *and* $\mathbb{Z}_2^3 \times \mathbb{Z}_5$	P_2
	63	$\mathbb{Z}_3^2 \times \mathbb{Z}_7$	P_2
idempotent MCQLS	12	$\mathbb{Z}_2^2 \times \mathbb{Z}_3$	P_1
	20, 32	from the MCDQLS witnesses	P_1
	24	$\mathbb{Z}_2^3 \times \mathbb{Z}_3$ *and* $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3$	P_1

This settles ten (order, property) cells, over the eight distinct orders $9, 12, 20, 24, 27, 32, 40, 63$ (Theorems 4.1, 4.2 and 4.3): $P_1 \cup P_2$ shrinks from 35 orders to 29 for MCDQLS, and P_1 from 13 to 9 for the idempotent variant.

The second half of the paper determines how much further this engine can possibly go, and the answer is: no further. Section 5 proves two counting obstructions — a complete mapping of a finite abelian group forces $\sum_{g\in G} g = 0$, and a strong complete mapping of a group surjecting onto $\mathbb{Z}_3$ forces $9 \mid |G|$ — which between them rule out 26 of the 29 surviving orders over every abelian group of that order. Section 6 settles the last three, 7, 8 and 11, by exhaustive enumeration inside the proof kernel. At orders 7 and 11 the enumeration returns more than a count: *every* strong complete mapping of *every* group of order 7 or 11 is affine, $\mu(t) = k \cdot t + b$, and an affine μ can satisfy neither the maximum-cardinality condition for any pairing whatsoever nor Huang and Li's own condition ($*$) (Theorem 6.2). This explains two entries that [1] leaves in P_2 without comment: their odd-prime lemma is stated for primes $p \geq 13$, and the reason 7 and 11 are not covered is that there is nothing there to find. Section 7 collects the result (Theorem 7.1): every one of the 35 orders of $P_1 \cup P_2$ is either settled by a witness above or provably out of reach of the construction, and the same holds for the 13 orders of P_1.

We emphasise what is *not* claimed. The unreachability statements say that this construction — Huang and Li's, generalised as far as an arbitrary finite abelian group and an arbitrary pairing —

produces nothing at those orders. They say nothing about the existence of an MCDQLS(v) by other means, and the corresponding cells of $P_1 \cup P_2$ remain open questions.

Relation to the literature. Four papers in this line [3, 5, 6, 7] settle neighbouring existence problems, all for the plain invariant with no transversal condition attached. What we were able to establish about each, and on what evidence: [3] is the paper [1] builds on, and [1] describes its construction as having "employed Fourier matrix to construct an MCQLS(v) for any order $v \geq 4$"; its companion preprint [4], by the same four authors and cited alongside it by [1], we did read in full — its kernel is the discrete Fourier matrix $v^{-1/2}\omega^{kl}$ of $\mathbb{Z}_v$ with $\omega = e^{2\pi i/v}$, and the words *abelian*, *character*, *cyclic*, *complete mapping*, *transversal*, *diagonal* and *pandiagonal* do not occur in it at all. [6] states in its own abstract that it proceeds "by extending the classical singular direct product construction to the quantum setting". [5] we could not characterise from any source we could read; what we can report is its reference list, all 25 entries of which we did obtain, and which contains no character theory, no finite fields and no complete mappings. [7] is on arXiv and was read in full: it glues sub-QLS(4) blocks and contains no character theory. The decisive point does not depend on any of that. [1] is the most recent paper of the line, it cites all four, and it still lists the orders settled here as undetermined; had any of them settled MCDQLS(9), the concluding theorem of [1] would be false.

One caveat, stated because it is real: the body text of [3], [5] and [6] was not obtained. All three are paywalled with no repository copy, and no abstract of the first two is deposited with any indexing service we could reach. Everything said about those three above is what a source we could read says about them, not what we have read in them.

2. Preliminaries

Throughout, $n, v \geq 1$ are integers and G is a finite abelian group, written additively.

Definition 2.1. A family $\psi_0, \ldots, \psi_{n-1} \in \mathbb{C}^n$ is *orthonormal* when $\langle \psi_i, \psi_{i'} \rangle = \delta_{i,i'}$. An array $\Phi\colon \{0, \ldots, n-1\}^2 \to \mathbb{C}^n$ is a QLS(n) when each of its rows and each of its columns is an orthonormal family. For σ an injection of $\{0, \ldots, n-1\}$ into itself, the cell set $\{(i, \sigma(i))\}$ is a *transversal* of Φ when $(\Phi(i, \sigma(i)))_i$ is an orthonormal family. Two vectors are *ray-equivalent* when each is a nonzero scalar multiple of the other; $\mathrm{card}(\Phi)$ is the number of ray-equivalence classes among the n^2 entries. Finally Φ is an idempotent MCQLS(n) when it is a QLS(n), the main diagonal $\sigma = \mathrm{id}$ is a transversal and $\mathrm{card}(\Phi) = n^2$; it is an MCDQLS($n$) when in addition the anti-diagonal $\sigma(i) = n-1-i$ is a transversal.

Definition 2.1 transcribes [1, §1]. Two points are worth making explicit, since the constructions below are checked against these predicates and a weakening of them would make the witnesses worthless.

Proposition 2.2 (Faithfulness)**.** *Let $n \geq 1$. An orthonormal family of n vectors of $\mathbb{C}^n$ is an orthonormal* basis *of $\mathbb{C}^n$; in particular each row and each column of a* QLS(n)*, and each of its transversals, really is a basis of $\mathbb{C}^n$. Moreover, for unit vectors u, v, ray-equivalence holds if and only if $v = e^{i\theta}u$ for some $\theta \in \mathbb{R}$, which is the identification used in* [1]*; and if no two distinct cells of Φ are ray-equivalent then* $\mathrm{card}(\Phi) = n^2$.

Proof sketch. Orthonormality gives linear independence, and n independent vectors in a space of dimension n form a basis. For the phase statement, if $v = cu$ with $c \neq 0$ and u, v of norm 1, then $|c| = 1$, so $c = e^{i \arg c}$; the converse is immediate. For the last statement, ray-equivalence is an equivalence relation on the cell set and the quotient map is a bijection under the hypothesis. □

Proposition 2.3 (The two bounds)**.** *For every array Φ of order n one has* $\mathrm{card}(\Phi) \leq n^2$*, and for every* QLS($n$) *with $n \geq 1$ one has $n \leq \mathrm{card}(\Phi)$.*

Proof. The quotient map from the n^2 cells onto the set of rays is surjective, which gives the upper bound. For the lower bound, two distinct cells of one row of a QLS(n) carry orthogonal unit vectors, hence are not ray-equivalent, so a single row already contributes n classes. □

These are the two brackets around the claim $\operatorname{card}(\Phi) = n^2$: it is a claim *at* the ceiling, and it is not vacuous.

Definition 2.4. A map $\mu\colon G \to G$ is a *complete mapping* when μ and $t \mapsto t+\mu(t)$ are both bijections, and a *strong complete mapping* when in addition $t \mapsto \mu(t) - t$ is a bijection.

Definition 2.5 ([1, condition $(*)$])**.** A permutation μ of $\mathbb{Z}_v$ satisfies $(*)$ when there are distinct $s, t, r \in \mathbb{Z}_v$ with

$$\gcd\big((t-s)(\mu(r)-\mu(s)) - (r-s)(\mu(t)-\mu(s)),\, v\big) = 1,$$

equivalently, when the displayed determinant is a unit of $\mathbb{Z}_v$.

3. The construction over an arbitrary finite abelian group

Definition 3.1. Let $L \geq 1$. A *pairing* on G with values in $\mathbb{Z}_L$ is a map $B\colon G \times G \to \mathbb{Z}_L$ that is additive in each slot,

$$B(s+t, x) = B(s, x) + B(t, x), \qquad B(t, x+y) = B(t, x) + B(t, y),$$

and *nondegenerate* in its second slot: for every $d \in G \setminus \{0\}$ there is $t \in G$ with $B(t, d) \neq 0$.

For $G = \mathbb{Z}_v$, $L = v$ and $B(x, y) = xy$ this is exactly the kernel of (1). Two constructions supply all the pairings used below: on a cyclic factor $\mathbb{Z}_m$ inside $\mathbb{Z}_L$ with $m \mid L$ one takes $B_m(x, y) = (L/m)\,\bar{x}\bar{y}$, where $\bar{x} \in \{0, \dots, m-1\}$ denotes the representative of x; and pairings on G and H with values in the same $\mathbb{Z}_L$ add to a pairing on $G \times H$. Applying both to a primary decomposition $G \cong \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$ with $L = \operatorname{lcm}(n_1, \dots, n_k)$ gives what we call the *canonical* pairing of that decomposition; it is the direct generalisation of ω^{ts}.

Given a pairing B, a map $\mu\colon G \to G$ and $v = |G|$, define for $a, b \in G$

$$|\varphi_{a,b}\rangle \;=\; v^{-1/2}\big(\zeta_L^{\,B(t,b)+B(\mu(t),a)}\big)_{t \in G}, \qquad \zeta_L = e^{2\pi i/L}, \tag{2}$$

and read the result as a $v \times v$ array through a bijection $e\colon \{0, \dots, v-1\} \to G$, that is, $\Phi(i, j) = |\varphi_{e(i),e(j)}\rangle$.

Theorem 3.2 (The construction over G)**.** *Let G be a finite abelian group of order $v \geq 1$, let B be a pairing on G with values in $\mathbb{Z}_L$, let $\mu\colon G \to G$, and let $e\colon \{0, \dots, v-1\} \to G$ be a bijection. Assume*

(i) *μ is a bijection;*
(ii) *$t \mapsto t + \mu(t)$ is a bijection;*
(iii) *for every $(d, q) \in G \times G$ with $(d, q) \neq (0, 0)$, the map $t \mapsto B(t, q) + B(\mu(t), d)$ is non-constant on G.*

Then the array (2) *is an idempotent* MCQLS(v)*. If moreover*

(iv) *$t \mapsto \mu(t) - t$ is a bijection, and*
(v) *$e(i) + e(v-1-i) = c$ for all i and some fixed $c \in G$,*

then it is an MCDQLS(v)*.*

Proof sketch. Everything reduces to one vanishing lemma: if $f\colon G \to \mathbb{Z}_L$ is additive and $f(t_0) \neq 0$ for some t_0, then $\sum_{t \in G} \zeta_L^{f(t)} = 0$, because multiplying the sum by $\zeta_L^{f(t_0)}$ reindexes it along $t \mapsto t_0 + t$, so $(\zeta_L^{f(t_0)} - 1)\sum_t \zeta_L^{f(t)} = 0$ while $\zeta_L^{f(t_0)} \neq 1$. The inner product of the cells (a, b) and (a', b') equals $v^{-1}\sum_t \zeta_L^{B(t,b'-b)+B(\mu(t),a'-a)}$, so: rows are orthonormal because $t \mapsto B(t, b'-b)$ is additive and, by nondegeneracy, nonzero somewhere when $b \neq b'$; columns because $t \mapsto B(\mu(t), a'-a)$ reindexes to $s \mapsto B(s, a'-a)$ by (i); the main diagonal (a, a) because $t \mapsto B(t+\mu(t), d)$ reindexes by (ii); and the anti-diagonal, which over G is the cell set $\{(a, c-a)\}$, because $t \mapsto B(\mu(t)-t, d)$ reindexes by (iv), while (v) is exactly what makes $\{(a, c-a)\}$ the anti-diagonal $\{(i, v-1-i)\}$ of the array read through e. Finally, if two cells are ray-equivalent then the quotient of their coordinates is constant in t, which says that $t \mapsto B(t, q) + B(\mu(t), d)$ is constant for $(d, q) = (a'-a, b'-b)$; by (iii) this forces $(d, q) = (0, 0)$, so no two distinct cells share a ray and Proposition 2.2 gives card $= v^2$. □

Two bookkeeping points are hidden by the cyclic case and cost false positives if ignored.

Remark 3.3. (a) Hypothesis (v) is a genuine restriction on the enumeration, not a consequence of bijectivity: Proposition 8.1(d) exhibits a bijection $\{0,\dots,8\} \to \mathbb{Z}_3^2$ for which no constant c works. For the mixed-radix enumeration of $\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$ it holds automatically with $c = (n_1 - 1, \dots, n_k - 1)$, because $v - 1 - i$ has mixed-radix digits $n_l - 1 - i_l$ with no borrow. (b) Condition (iii) must be tested on the whole character, with the single common denominator $L = \mathrm{lcm}(n_i)$. A factor-by-factor test is strictly weaker — a sum of non-integers can be an integer, as in $\frac{1}{3} + \frac{2}{3}$ — and produces false positives; this is a real trap, and it produced them at $v = 8$ and $v = 12$ during an early pass of this work.

4. Ten cells of the exception lists

Theorem 4.1. *An* MCDQLS(v) *exists for*

$$v \in \{9,\ 20,\ 27,\ 32,\ 40,\ 63\},$$

six of the 35 *orders that* [1] *leaves undetermined (*20 *and* 32 *from* P_1*;* 9*,* 27*,* 40 *and* 63 *from* P_2*). A witness is obtained from Theorem 3.2 at, respectively, the groups* $\mathbb{Z}_3^2$*;* $\mathbb{Z}_2^2 \times \mathbb{Z}_5$*;* $\mathbb{Z}_3^3$ *and* $\mathbb{Z}_9 \times \mathbb{Z}_3$*;* $\mathbb{Z}_2^5$*;* $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_5$ *and* $\mathbb{Z}_2^3 \times \mathbb{Z}_5$*;* $\mathbb{Z}_3^2 \times \mathbb{Z}_7$*, each with its canonical pairing and its mixed-radix enumeration.*

Theorem 4.2. *An idempotent* MCQLS(v) *exists for*

$$v \in \{12,\ 20,\ 24,\ 32\},$$

four of the 13 *orders of* P_1*. At* $v = 12$ *and* $v = 24$ *a witness comes from Theorem 3.2 at* $\mathbb{Z}_2^2 \times \mathbb{Z}_3$*, respectively at* $\mathbb{Z}_2^3 \times \mathbb{Z}_3$ *and at* $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3$*; at* $v = 20$ *and* $v = 32$ *it comes from the corresponding witness of Theorem 4.1, since every* MCDQLS *is in particular an idempotent* MCQLS*.*

The two theorems are stated separately because of an asymmetry that is not an artefact of the proof. At orders 12 and 24 the complete mappings used are not strong, and cannot be: by Proposition 5.3 no abelian group of order 12 or 24 has a strong complete mapping at all. So at those orders the idempotent variant is settled by this engine while the diagonal variant is provably beyond it.

Theorem 4.3. *Ten* (*order, property*) *cells of* [1]*'s exception lists are settled at once:* $P_1 \cup P_2$ *loses* $9, 20, 27, 32, 40, 63$ *for* MCDQLS*, and* P_1 *loses* $12, 20, 24, 32$ *for the idempotent variant. Thus for* MCDQLS *the list of possible exceptions shrinks from* 35 *orders to*

$$\{6, 7, 8, 10, 11, 12, 14, 15, 18, 21, 22, 24, 26, 30, 33, 34, 38, 39, 46, 48, 50, 51, 58, 62, 74, 75, 82, 94, 122\},$$

and for the idempotent variant from 13 *orders to* $\{6, 8, 10, 14, 18, 26, 30, 38, 62\}$*. Moreover three of the settled cells carry a second witness over a second group — order* 27 *over* $\mathbb{Z}_3^3$ *and over* $\mathbb{Z}_9 \times \mathbb{Z}_3$*, order* 40 *over* $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_5$ *and over* $\mathbb{Z}_2^3 \times \mathbb{Z}_5$*, and order* 24 *(idempotent) over* $\mathbb{Z}_2^3 \times \mathbb{Z}_3$ *and over* $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3$ *— so the existence results are not accidents of one presentation.*

Proof sketch, and what rests on computation. Each witness is a table: a permutation μ of the group, recorded as a list of v mixed-radix indices. Given the table, hypotheses (i), (ii), (iv) and (v) of Theorem 3.2 are finite injectivity and identity checks over G, and hypothesis (iii) is the finite statement "for all $(d, q) \neq (0, 0)$ there exists t with $B(t, q) + B(\mu(t), d) \neq B(0, q) + B(\mu(0), d)$" — $v^2 - 1$ pairs, each discharged by exhibiting one t. All of these are decided by kernel evaluation, so each existence theorem is a finite verification from its table and nothing else.

The tables themselves were *found* by depth-first search over partial assignments, maintaining the three injectivity constraints incrementally and testing (iii) at each leaf; the whole search campaign cost under 15 minutes of CPU time except at $v = 63$, discussed in Remark 4.4. Search is not part of any proof here: every table was then re-verified twice independently before being used, once at the exact character level in $\mathbb{Z}_L$ and once by rebuilding the whole $v \times v$ complex array in floating point and checking every row, column, diagonal and anti-diagonal inner product and counting rays by $|\langle u, w\rangle| = 1$. The ray counts came out at the ceiling in every case: 81/81, 144/144, 400/400, 576/576, 729/729, 1024/1024, 1600/1600 and 3969/3969. □

Remark 4.4. Order 63 is worth a sentence because the search failed there and a construction replaced it. A randomised depth-first search over $\mathbb{Z}_3^2 \times \mathbb{Z}_7$ ran 4.8×10^9 nodes in about one CPU-hour across twelve restarts without reaching a single leaf, although solutions certainly exist. What produced the table instead was a twisted product: if G and H have coprime orders, μ_G is a strong complete mapping of G satisfying (iii), μ_H is a strong complete mapping of H and $\varphi\colon G \to H$ is any surjective map, then $\mu(g,h) = (\mu_G(g), \mu_H(h) + \varphi(g))$ is a strong complete mapping of $G \times H$ satisfying (iii). The twist is what buys (iii): with φ constant the product fails, precisely because every strong complete mapping of $\mathbb{Z}_7$ is affine (Theorem 6.2). Concretely, μ_G was the order-9 witness of Theorem 4.1, $\mu_H(z) = 2z$ on $\mathbb{Z}_7$, and φ sent the element of $\mathbb{Z}_3^2$ with digits (x_1, x_2) to $3x_1 + x_2 \bmod 7$. The table so obtained was verified exactly like the others; the twisted product is how it was found, not why it is correct, and it is stated here only as a search heuristic — it is not part of the formal development, and the MCDQLS(63) of Theorem 4.1 rests on its table alone.

5. Two obstructions

The witnesses raise the question of how far the engine reaches, and the following two counting arguments answer it for all but three orders. Both are weaker special cases of classical criteria, and we record the relation for orientation only, since nothing below uses either. The 2-obstruction is the abelian case of Hall and Paige's necessary condition [8, Theorem 5]: *a finite group whose Sylow 2-subgroup is cyclic does not have a complete mapping.* The 3-obstruction is a weakening of Evans's characterisation [9, Theorem 15]: *a finite abelian group admits strong complete mappings if and only if neither its Sylow 2-subgroup nor its Sylow 3-subgroup is nontrivial and cyclic.* For general background on complete mappings and orthomorphisms see [10]. We state and prove the forms we need, which are short and self-contained.

Proposition 5.1 (The 2-obstruction)**.** *If a finite abelian group G has a complete mapping, then $\sum_{g \in G} g = 0$. Consequently a group whose element sum is nonzero has neither a complete nor a strong complete mapping, and the character construction produces nothing over it.*

Proof. Write $S = \sum_{g \in G} g$. Since μ is a bijection, $\sum_t \mu(t) = S$. Since $t \mapsto t + \mu(t)$ is a bijection, $\sum_t (t + \mu(t)) = S$ as well; but the left side is $\sum_t t + \sum_t \mu(t) = S + S$. So $S + S = S$, i.e. $S = 0$. □

Corollary 5.2. *Twenty-three explicitly given abelian groups have nonzero element sum and therefore no complete mapping. They are all the abelian groups of the orders*

$$6,\ 10,\ 14,\ 18,\ 22,\ 26,\ 30,\ 34,\ 38,\ 46,\ 50,\ 58,\ 62,\ 74,\ 82,\ 94,\ 122,$$

together with $\mathbb{Z}_8$ (order 8), $\mathbb{Z}_4 \times \mathbb{Z}_3$ (order 12), $\mathbb{Z}_8 \times \mathbb{Z}_3$ (order 24) and $\mathbb{Z}_{16} \times \mathbb{Z}_3$ (order 48).

Proof. Each element sum is a single finite computation in the group, discharged by kernel evaluation, and Proposition 5.1 applies. □

Proposition 5.3 (The 3-obstruction)**.** *Let G be a finite abelian group admitting a surjective homomorphism $\chi\colon G \to \mathbb{Z}_3$ and a strong complete mapping. Then $9 \mid |G|$. Consequently no abelian group of order $12, 15, 21, 24, 33, 39, 48, 51$ or 75 has a strong complete mapping.*

Proof. Each fibre of χ has $|G|/3$ elements, so each of the four sets

$$\{\chi(t) = 0\}, \quad \{\chi(\mu(t)) = 0\}, \quad \{\chi(\mu(t) - t) = 0\}, \quad \{\chi(t + \mu(t)) = 0\}$$

has $|G|/3$ elements as well, because id, μ, $\mu - \mathrm{id}$ and $\mathrm{id} + \mu$ are all permutations of G and χ is a homomorphism. Now count how many of the four contain a given t, as a function of $(a, b) = (\chi(t), \chi(\mu(t))) \in \mathbb{Z}_3^2$: if $a = b = 0$ it lies in all four; if exactly one of a, b is 0 it lies in exactly one; and if both are nonzero then exactly one of $b = a$, $b = -a$ holds since $a \neq -a$ in $\mathbb{Z}_3$, so again exactly one. This is a nine-case identity over $\mathbb{Z}_3^2$. Summing over t and writing n_{00} for the number of t with $\chi(t) = \chi(\mu(t)) = 0$ gives $4 \cdot |G|/3 = |G| + 3n_{00}$, whence $|G|/3 = 3n_{00}$ and $9 \mid |G|$. For the consequence, each of the listed orders v satisfies $3 \mid v$ and $9 \nmid v$, so the 3-primary component of an abelian group of order v is $\mathbb{Z}_3$ and the projection onto it is a surjective homomorphism onto $\mathbb{Z}_3$. □

Remark 5.4. Proposition 5.3 is what closes the odd multiples of 3 that are not multiples of 9, and it is worth saying why the 2-obstruction cannot: at orders $33 = 3\cdot11$, $39 = 3\cdot13$ and $51 = 3\cdot17$ the unique abelian group has odd order, so $\mu = \mathrm{id}$ is already a complete mapping ($t \mapsto 2t$ being a bijection there) and the element sum of the group *does* vanish. What fails at those orders is the strong condition, and the reason is the 3-obstruction and not the 2-obstruction — nor, therefore, the Hall–Paige criterion of which the 2-obstruction is a special case. We record this because the misattribution is easy to make. Proposition 5.3 is also weaker than Evans's criterion [9, Theorem 15] for general abelian groups, which asks the Sylow 3-subgroup to be trivial or non-cyclic and would additionally rule out $\mathbb{Z}_9 \times \mathbb{Z}_7$; we state the form that is short to prove and exactly strong enough for the orders at issue — and indeed order 63 is settled above by the *different* group $\mathbb{Z}_3^2 \times \mathbb{Z}_7$.

Finally, one standing caveat. Corollary 5.2 lists finitely many groups, and the last step of Proposition 5.3 identifies the 3-primary component of an abelian group of one of the listed orders; both passages, from named groups to *every* abelian group of an order, use the structure theory of finite abelian groups, which is standard mathematics and is not part of the formal development. The caveat applies to the 26 orders treated by the two obstructions, and to order 8 of the next section, where $\mathbb{Z}_8$, $\mathbb{Z}_2 \times \mathbb{Z}_4$ and $\mathbb{Z}_2^3$ are taken to exhaust the abelian groups of that order. It does not apply to orders 7 and 11: those are prime, so every group of the order is cyclic, and the statements below are proved for an arbitrary abelian group of the order by transport along an additive isomorphism.

6. The three residual orders 7, 8 and 11

Exactly three orders of $P_1 \cup P_2$ are reached by neither obstruction: 7 and 11, where $\gcd(v, 6) = 1$ so strong complete mappings do exist, and 8, whose non-cyclic groups have vanishing element sum. These are settled by exhaustive enumeration.

Proposition 6.1 (The enumerations)**.** *Represent a candidate μ by its assignment list $[(g, \mu(g))]$. The three conditions of Definition 2.4 are pairwise conditions on that list — for $g \neq g'$, $\mu(g) \neq \mu(g')$, $g + \mu(g) \neq g' + \mu(g')$ and $\mu(g) - g \neq \mu(g') - g'$ — so a depth-first search that extends an assignment only by values compatible with all those already assigned is exhaustive: if it reports that a predicate Q holds at every leaf, then Q holds for every (strong) complete mapping of the group. Since μ is a (strong) complete mapping if and only if $\mu - \mu(0)$ is, and since condition (iii) of Theorem 3.2 is likewise invariant under adding a constant to μ, the search may start from the normalised assignment $\mu(0) = 0$, dividing the tree by $|G|$. Four searches are run in the kernel: at $\mathbb{Z}_7$ (238 child tests) and $\mathbb{Z}_{11}$ (27 214) with the affineness leaf test, and at $\mathbb{Z}_2 \times \mathbb{Z}_4$ (3 600) and $\mathbb{Z}_2^3$ (3 616) with the failure-of-(iii) leaf test. All four terminate with the verdict that their leaf test holds at every leaf.*

Proof sketch. Exhaustiveness is the only obligation, and it is a statement about lists rather than about groups: the predicate on assignment lists is Pairwise R for a decidable relation R, and splitting a list as $A +\!\!+ (p :: asg)$ splits Pairwise into the pairwise conditions on the parts and the cross terms, the middle factor being exactly the compatibility test the search performs. The invariance under $\mu \mapsto \mu - b$ is two short computations, the second using $B(x - b, d) = B(x, d) - B(b, d)$, which shifts every value of $t \mapsto B(t, q) + B(\mu(t), d)$ by the same amount. □

The counts are reproducible and, in part, published. An independent implementation, written before any of this was formalised, reproduces the unnormalised node counts exactly: 1 624 child tests at $\mathbb{Z}_7$, 299 244 at $\mathbb{Z}_{11}$, and 29 640, 28 744, 28 872 at $\mathbb{Z}_8$, $\mathbb{Z}_2 \times \mathbb{Z}_4$, $\mathbb{Z}_2^3$. It finds 28 strong complete mappings of $\mathbb{Z}_7$ and 88 of $\mathbb{Z}_{11}$, and 0, 384, 384 complete mappings at the three groups of order 8, none of them satisfying (iii). Both OEIS sequences below use the same $\mu(0) = 0$ normalisation, and under it the strong-complete-mapping counts at $\mathbb{Z}_5, \mathbb{Z}_7, \mathbb{Z}_9, \mathbb{Z}_{11}, \mathbb{Z}_{13}, \mathbb{Z}_{15}$ are $2, 4, 0, 8, 348, 0$, the terms $a(2), \ldots, a(7)$ of **A071607** [12] — six terms, all matching — and the complete-mapping counts at $\mathbb{Z}_5$, $\mathbb{Z}_7$, $\mathbb{Z}_{11}$ are 3, 19, 3441, the terms $a(2)$, $a(3)$, $a(5)$ of **A003111** [12].

Theorem 6.2 (Orders 7 and 11)**.** *Let G be a finite abelian group with $|G| \in \{7, 11\}$ and let μ be a strong complete mapping of G. Then μ is affine: there are $k \in \mathbb{N}$ and $b \in G$ with $\mu(t) = k \cdot t + b$ for all t. Consequently*

(1) *for every $L \geq 1$ and every pairing B on G with values in $\mathbb{Z}_L$, hypothesis (iii) of Theorem 3.2 fails; and*
(2) *for $G = \mathbb{Z}_7$ and $G = \mathbb{Z}_{11}$, μ does not satisfy Huang and Li's condition $(*)$.*

Thus MCDQLS(7) *and* MCDQLS(11) *lie beyond the reach of Huang and Li's construction, and of its generalisation in Theorem 3.2. More precisely, the strong complete mappings of $\mathbb{Z}_7$ (resp. $\mathbb{Z}_{11}$) are exactly the maps $t \mapsto kt + b$ with $k \notin \{0, 1, -1\}$: four slopes and seven shifts, so 28 of them, resp. eight slopes and eleven shifts, so 88.*

Proof sketch. Affineness at $\mathbb{Z}_7$ and $\mathbb{Z}_{11}$ is Proposition 6.1 with the leaf test "the assignment is $t \mapsto kt$ for some k": the two searches report that every leaf passes, which after undoing the normalisation says that every strong complete mapping is affine. That the affine maps of the stated slopes are indeed strong complete mappings is a 49-, resp. 121-case check, which gives the exact description and the counts 28 and 88. Since 7 and 11 are prime, every group of that order is cyclic, so the statement transports to an arbitrary G by conjugating along an additive isomorphism $G \cong \mathbb{Z}_v$; conjugation preserves the three injectivity conditions and preserves affineness. No classification of finite abelian groups is used here.

For (1), let $d \neq 0$ and put $q = -(k \cdot d)$. Bi-additivity gives

$$B(t, q) + B(\mu(t), d) = -k\, B(t, d) + k\, B(t, d) + B(b, d) = B(b, d),$$

constant in t, so (iii) fails — for every pairing, which is why no choice of character kernel rescues these two orders. For (2), the determinant of Definition 2.5 is $(t - s)(\mu(r) - \mu(s)) - (r - s)(\mu(t) - \mu(s))$, which vanishes identically for affine μ (three points of a line are collinear), and 0 is not a unit. □

Remark 6.3 (The affineness question elsewhere). The first assertion of Theorem 6.2 is a statement about strong complete mappings alone, and it is worth separating it from a superficially similar question in the literature. Bastide, Bishnoi, Groenland, Gijswijt and Joshi [11] ask the same affineness question for the permutations π of $\mathbb{Z}_n$ with $t([\pi]) = n - 2$, equivalently those all of whose cyclic shifts have cycle type $(1, n - 1)$. That is a strictly smaller class — every such π is a strong complete mapping, [11, Proposition 12, v3] — and they report that the smallest n admitting a non-affine member is $n = 23$. So it is a different question with a different answer: for strong complete mappings alone, non-affine examples already occur at 13, as Proposition 6.6(1) records. What is genuinely published in the vicinity is the enumeration — the normalised strong-complete-mapping counts 4 at $\mathbb{Z}_7$ and 8 at $\mathbb{Z}_{11}$ are terms of A071607 [12] — and not the consequence drawn from it, which is that Huang and Li's P_2 contains 7 and 11 for a reason their paper does not state.

Proposition 6.4 (Order 8)**.** *Let G be one of $\mathbb{Z}_8$, $\mathbb{Z}_2 \times \mathbb{Z}_4$, $\mathbb{Z}_2^3$ — that is, by the classification of finite abelian groups, an arbitrary abelian group of order 8 — carrying its canonical pairing. Then no complete mapping of G satisfies hypothesis (iii) of Theorem 3.2. Concretely: $\mathbb{Z}_8$ has no complete mapping at all, and every complete mapping of $\mathbb{Z}_2 \times \mathbb{Z}_4$ and of $\mathbb{Z}_2^3$ admits some $(d, q) \neq (0, 0)$ making $t \mapsto B(t, q) + B(\mu(t), d)$ constant. Since $8 \in P_1$, both* MCDQLS(8) *and idempotent* MCQLS(8) *are out of reach of the construction at that order, the complete-mapping negative covering both variants because a strong complete mapping is in particular complete.*

Proof sketch. For $\mathbb{Z}_8$ the element sum is $4 \neq 0$, so Proposition 5.1 applies. For the other two groups the statement is the two searches of Proposition 6.1, which find a bad (d, q) at every leaf. Each search has 48 leaves, so each of the two groups has $8 \cdot 48 = 384$ complete mappings; only the verdict, and not that count, is part of the proof. □

Remark 6.5 (A stated restriction). Proposition 6.4 is stated for the *canonical* pairing — the product of the cyclic pairings $B_m(x, y) = (L/m)\bar{x}\bar{y}$ with $L =$ lcm of the factor orders, so $L = 4$ and $B((a, b), (c, d)) = 2ac + bd$ on $\mathbb{Z}_2 \times \mathbb{Z}_4$, and $L = 2$ with the dot product on $\mathbb{Z}_2^3$ — and not for every pairing, unlike Theorem 6.2. The reason is structural: the order-8 complete mappings are not affine (the normalised ones of $\mathbb{Z}_2^3$ are additive with linear part of order 7 in $\mathrm{GL}(3, 2)$, and those of $\mathbb{Z}_2 \times \mathbb{Z}_4$ are not even additive), so the pairing-free argument is unavailable. A pairing-general version would

need surjectivity of $q \mapsto B(\cdot, q)$ onto $\mathrm{Hom}(G, \mathbb{Z}_L)$; that is a short piece of group theory which we have not carried out. Counting the complete mappings of small groups is classical territory, and the two counts 384 are certainly not new; they were recomputed here rather than looked up, and nothing above rests on a published value.

Proposition 6.6 (Controls on the enumeration)**.** *The search machinery of Proposition 6.1 reports a failure exactly where one exists. (1) At* $\mathbb{Z}_{13}$ *the affineness search reports a counterexample: only* 10 *of the* 348 *normalised strong complete mappings of* $\mathbb{Z}_{13}$ *are affine, so orders* 7 *and* 11 *are genuinely special and the affineness searches are not proving a triviality. (2) At* $\mathbb{Z}_7$ *with the third injectivity condition dropped the affineness search reports a counterexample:* 14 *of the* 19 *normalised complete mappings of* $\mathbb{Z}_7$ *are not affine, so the strong hypothesis is load-bearing. (3) At* $\mathbb{Z}_7$ *a complete mapping satisfying (iii) exists, so the failure-of-(iii) leaf test reports a counterexample — which recovers the source's own asymmetry,* $7 \in P_2$ *but* $7 \notin P_1$*. (4) At* $\mathbb{Z}_3^2$*, the group of the* MCDQLS(9) *witness, the same test reports a counterexample (*54 *of the* 72 *normalised strong complete mappings satisfy (iii)). (5) The map* $t \mapsto 2t$ *is a strong complete mapping of* $\mathbb{Z}_7$ *and of* $\mathbb{Z}_{11}$*, so the hypotheses of Theorem 6.2 are not vacuous. In (1)–(4) what is verified is the search's failure verdict; the ratios quoted alongside are measurements, in the sense of Section 9.*

Controls (3) and (4) are the pair that matter: together they say that the verdict at order 8 records a real absence rather than a test that cannot see.

7. The reach of the construction, determined

Theorem 7.1. *Every one of the* 35 *orders of* $P_1 \cup P_2$ *is either settled by a witness or out of reach of the construction of Theorem 3.2, and likewise for the* 13 *orders of* P_1*. Precisely, on the diagonal side:*

- 6 *orders —* $9, 20, 27, 32, 40, 63$ *— carry an* MCDQLS *witness (Theorem 4.1);*
- 17 *orders die by the* 2*-obstruction and* 9 *by the* 3*-obstruction (Corollary 5.2, Proposition 5.3), over every abelian group of the order, modulo the classification of finite abelian groups;*
- *the last* 3 *—* 7*,* 8*,* 11 *— die by the enumerations of Theorem 6.2 and Proposition 6.4, with orders* 7 *and* 11 *requiring no classification input and holding for every pairing, and order* 8 *for the canonical pairing (Remark 6.5).*

On the idempotent side, P_1 *minus the four orders of Theorem 4.2 is* $\{6, 8, 10, 14, 18, 26, 30, 38, 62\}$*, of which* 8 *is Proposition 6.4's and the other eight die by the* 2*-obstruction. No order of either list is left to a measurement outside the formal development.*

The three ingredients meet at the orders where several abelian groups of the same order are killed by different arguments. Order 12 is the clearest: of its two abelian groups, $\mathbb{Z}_4 \times \mathbb{Z}_3$ has element sum $(2, 0) \neq 0$ and dies by the 2-obstruction, while $\mathbb{Z}_2^2 \times \mathbb{Z}_3$ dies by the 3-obstruction — and that same group carries the idempotent MCQLS(12) of Theorem 4.2, since the idempotent variant needs only a complete mapping. Order 24 behaves the same way, with $\mathbb{Z}_8 \times \mathbb{Z}_3$ dying by the 2-obstruction and the other two groups carrying the two idempotent witnesses; order 48 has $\mathbb{Z}_{16} \times \mathbb{Z}_3$ dying by the 2-obstruction and its four other groups by the 3-obstruction; order 8 has $\mathbb{Z}_8$ dying by the 2-obstruction and its two other groups by enumeration.

Remark 7.2 (Where this route stops, and why). [1] closes with the pandiagonal variant, and there leaves MCPQLS(7), MCPQLS(11) and every MCPQLS(n) with $\gcd(n, 6) \neq 1$ undetermined. The move made here buys nothing there. The array (2) does have $2v$ orthonormal "generalised broken diagonals", the cell sets $\{(a, a + d)\}$ and $\{(a, c - a + d)\}$ for $d \in G$, orthonormal by (ii) and (iv); but pandiagonality asks for the broken diagonals of the *matrix*, $\{(i, (i + k) \bmod v)\}$, and shifting the index modulo v is a translation of G only when G is cyclic — for $G = \mathbb{Z}_3^2$ with the mixed-radix enumeration, $i \mapsto i + 1 \bmod 9$ is not a translation. This remark is an observation about the route and is not part of the formal development; nothing above depends on it.

8. Controls

Existence claims at the ceiling of an invariant, established from tables by finite verification, deserve controls in both directions. Proposition 2.3 brackets the invariant: at order 9 it refutes card = 82 outright, and refutes card = 8 for any QLS(9), so the claim card = 81 of Theorem 4.1 sits at the ceiling and is not vacuous. The next proposition checks the hypotheses of Theorem 3.2 individually.

Proposition 8.1 (Each hypothesis is a real restriction)**.** *(a) $\mu = -\mathrm{id}$ is a permutation of $\mathbb{Z}_3^2$ for which $t \mapsto t + \mu(t)$ is identically zero, so hypothesis (i) alone does not imply (ii). (b) The strong complete mapping of $\mathbb{Z}_3^2$ given by the index table $[0, 3, 6, 2, 5, 8, 1, 4, 7]$ satisfies (i), (ii) and (iv) and fails (iii), so (iii) is not implied by the other three — and it is not a rare failure either:* 162 *of the* 648 *strong complete mappings of $\mathbb{Z}_3^2$ fail it, a measurement in the sense of Section 9. (c) Perturbing a single entry of the order-*9 *witness table destroys injectivity, so the finite verification is testing the data rather than passing regardless. (d) Swapping two values of the mixed-radix enumeration of $\mathbb{Z}_3^2$ destroys hypothesis (v) for* every *constant c, so (v) constrains the enumeration and is not a consequence of bijectivity.*

Proposition 8.2 (Positive control at $v = 13$)**.** *Theorem 3.2, run at $G = \mathbb{Z}_{13}$ with the pairing $B(x, y) = xy$ — that is, at the source's own group with the source's own kernel ω^{xy} — yields an* MCDQLS(13).

Order 13 lies in neither P_1 nor P_2: [1] already proves that an MCDQLS(13) exists, which is exactly why it is worth re-deriving through the generalised machinery. It is the place where any drift between Theorem 3.2 and the construction of [1] would show. The mathematics of Proposition 8.2 is the source's; only the derivation is ours. For the record, the search finds 4 524 strong complete mappings of $\mathbb{Z}_{13}$, of which 4 394 satisfy (iii), and the resulting array verifies at 169/169 rays with both diagonals orthonormal.

9. Verification

Every definition, proposition and theorem stated above has been formally verified in Lean 4 (toolchain `v4.32.0`, *Mathlib* [13] at its `v4.32.0` tag), subject to the two qualifications recorded at the end of this section; the repository is private, repository reference to be added at submission. The development contains no `sorry` and declares no axiom of its own: every headline theorem depends on no axioms beyond `propext`, `Classical.choice` and `Quot.sound`, and in particular no statement is delegated to compiled evaluation — the finite checks are all kernel evaluations, so there is no trusted numeric or native-execution step anywhere. Definition 2.1 is transcribed from [1, §1] and Proposition 2.2 is the bridge that makes the transcription faithful rather than a weakening. The finite content is: the hypothesis checks per witness of Theorems 4.1 and 4.2, at orders up to 63; the element sums and divisibilities behind Corollary 5.2 and Proposition 5.3, over 37 groups; the four enumerations of Proposition 6.1 together with the exhaustiveness lemma that makes them proofs rather than searches; and the controls of Propositions 6.6 and 8.1. The complete verification costs a few CPU-minutes. The searches that *found* the witness tables, and the independent implementation that reproduced the enumeration counts before any of this was formalised, are described in the proof sketches of Theorem 4.3 and Proposition 6.1; they are how the data was obtained and are not part of any proof.

Two things stated above sit outside that verification, and both are flagged where they occur. The first is the structure theory of finite abelian groups, the standing caveat of Section 5: it is what carries Corollary 5.2, Proposition 5.3 and Proposition 6.4 from named groups to *every* abelian group of an order; it is used at the 26 orders settled by the two obstructions and at order 8, and orders 7 and 11 are exempt. The second is the counts. What the kernel decides is each search's verdict — that its leaf test holds at every leaf, or that it fails at some leaf — together with the exact characterisation of Theorem 6.2, from which the counts 28 and 88 there follow by arithmetic. The other numbers quoted above — the child tests of Proposition 6.1, the 384 and 48 of Proposition 6.4, the 162 of 648 of Proposition 8.1(b), the ratios of Proposition 6.6, and the floating-point ray counts and search costs quoted in the proof sketches — are *measurements* of the independent implementation. They are

recorded because they are reproducible, and because the counts over cyclic groups are independently published as [12]; no statement of this paper rests on any of them.

References

[1] Lin Huang and Yang Li (Department of Mathematics, Soochow University), *The Existence of Diagonal Quantum Latin Squares with Maximum Cardinality*, arXiv:2606.27758v1, submitted 26 June 2026.

[2] 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.

[3] Yajuan Zang, Meihui Zheng, Zihong Tian and Xiuling Shan, *A novel construction of quantum Latin square with maximum cardinality*, Discrete Math. **349** (2026), no. 9, 115126; doi:10.1016/j.disc.2026.115126.

[4] Yajuan Zang, Meihui Zheng, Zihong Tian and Xiuling Shan, *On the cardinalities of quantum Latin squares*, arXiv:2508.01972v1, 4 August 2025.

[5] Yuyuan Zhang and Haitao Cao, *Quantum Latin squares with maximal cardinality*, Discrete Math. **349** (2026), no. 3, 114863; doi:10.1016/j.disc.2025.114863.

[6] Yuyuan Zhang, Yiwen Zhang, Mingzhen Lv and Haitao Cao, *The maximal cardinality of quantum Latin squares and quantum Latin cubes*, J. Combin. Des. **34** (2026), no. 4, 169–183; doi:10.1002/jcd.70002.

[7] Ying Zhang, Xin Wang and Lijun Ji, *Quantum Latin squares with all possible cardinalities*, J. Combin. Des. **34** (2026), no. 8, 378–387; doi:10.1002/jcd.70021; arXiv:2507.05642.

[8] M. Hall and L. J. Paige, *Complete mappings of finite groups*, Pacific J. Math. **5** (1955), no. 4, 541–549; doi:10.2140/pjm.1955.5.541.

[9] A. B. Evans, *The existence of strong complete mappings*, Electron. J. Combin. **19** (2012), no. 1, Paper #P34.

[10] A. B. Evans, *Orthomorphism Graphs of Groups*, Lecture Notes in Mathematics, Springer, Berlin, 1992; doi:10.1007/BFb0092363.

[11] P. Bastide, A. Bishnoi, C. Groenland, D. Gijswijt and R. Joshi, *Circular sorting, strong complete mappings and wreath product constructions*, arXiv:2510.18529v3 (v1: 21 October 2025; v3: 17 June 2026).

[12] OEIS Foundation Inc., *The On-Line Encyclopedia of Integer Sequences*, https://oeis.org; entries A071607 (*number of strong complete mappings of the cyclic group* $\mathbb{Z}_{2n+1}$) and A003111 (*number of complete mappings of the cyclic group* $\mathbb{Z}_{2n+1}$), both of offset 0 and both normalised by $f(0) = 0$, consulted 30 August 2026.

[13] The mathlib Community, *The Lean mathematical library*, in: Certified Programs and Proofs (CPP 2020), ACM, 2020, pp. 367–381; doi:10.1145/3372885.3373824.